UNIVERZITET U BEOGRADU

FAKULTET ORGANIZACIONIH NAUKA

Dragan M. Korać

MODEL ZAŠTITE INFORMACIJA U SISTEMIMA ZA MENADŽMENT IDENTITETA I UPRAVLJANJE PRISTUPOM

doktorska disertacija

Beograd, 2018

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Dragan M. Korać

MODEL OF INFORMATION SECURITY IN SYSTEMS FOR MANAGEMENT IDENTITY AND ACCESS CONTROL

Doctoral Dissertation

Belgrade, 2018

Mentor:

dr Dejan Simić,
redovni profesor Fakulteta organizacionih nauka u Beogradu

Članovi komisije:

dr Dušan Starčević,
redovni profesor Fakulteta organizacionih nauka u Beogradu

dr Boško Nikolić
vanredni profesor Elektrotehničkog fakulteta u Beogradu

Datum odbrane: septembar, 2018.

Doktorsku disertaciju želim da posvetim svojim roditeljima,
a posebno majci jer znam koliko bi bila ponosna.

Posvećujem ga i mojoj porodici, djeci i supruzi
koji su strpljenjem i podrškom me vodili ka cilju,
kao i sestri i njenoj djeci.

Zahvaljujem i svima koji su savjetima ili na bilo koji drugi način
doprinijeli izradi ove doktorske disertacije,
a prije svih mentoru Prof. dr Dejanu Simić.

Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom

Rezime:

Predmet istraživanja u disertaciji su modeli zaštite informacija u sistemima menadžmenta identiteta i upravljanja pristupom (IAM), i unapređenje postojećih metoda i tehnika zaštite. Predmet je usmjeren u širem smislu riječi na menadžment identiteta, dok u užem smislu riječi na autentifikacione mehanizme koji su ključni u procesu menadžmenta identiteta. Cilj istraživanja je proučavanje dosadašnjih rezultata u ovoj oblasti, kao i razvoj i unapređenje postojećih modela zaštite u korisničko-orijentisanom okruženju IAM sistema. Problem analize modela zaštite informacija u sistemima za IAM nije nov. U poslednje dvije decenije, u ovoj oblasti postoji značajan broj radova i veliki broj autora se bavio ovom problematikom nudeći različite modele digitalnih identiteta i autentifikacionih mehanizama. Međutim, analizom dostupne literature utvrđeno je da takvi modeli imaju ograničenja, a da su vrijednosti takvih autentifikaciona rješenja deskriptivno izražene. Radi se o ograničenjima koji predstavljaju kritične dijelove modela zaštite informacija (model digitalnog identiteta i model za procjenu numeričke vrijednosti autentifikacionih rješenja). Ova ograničenja su bila motiv za razvoj Edukacionog modela digitalnog identiteta (EMDI) kao i Fishbone modela koji numerički vrijednuje postojeća autentifikaciona rješenja.

U poređenju sa svim drugim modelima identiteta, EMDI je uveo dva procesa planiranja i povratne informacije. Praktična primjena ovog modela je napravljena u Moodle platformi upotrebom plagina za filtriranje neaktivnih digitalnih identiteta kao implementacija podmodela. Razvijeni plagin je pokazao da je moguće da se popune praznine u problemima zaštite kao što je djelimično odsustvo kontrole administratora nad tokom procesa. Jedna od glavnih prednosti je mogućnost uspostavljanja bolje komunikacije između studenta i administratora. Dakle, disertacija ima direktan uticaj na popunjavanje praznina koje se odnose na zaštitu informacija u trenutnim istraživanjima i doprinosi boljem razumijevanju izazova digitalnih identiteta suočenih u e-learning okruženju. Na taj način je moguće da se poveća otpornost prema potencijalnim prijetnjama i rizicima kao što su kopiranje, krađa ili modifikovanje kredencijala.

S druge strane, u ovoj disertaciji je predložen i dizajniran Fishbone model, na osnovu koga se mogu implementirati bolji sistemi zaštite informacija od postojećih. Takođe, u disertaciji je urađena komparacija savremenih korisničkih metoda autentifikacije namjenjenih za mobilne uređaje prema izdiferenciranim ključnim korisničkim prioritetima kao što su zaštita, upotrebljivost, pristupačnost, cijena, kompleksnost, privatnost i pogodnost (SUAPCPC). Potrebno je istaknuti da glavna svrha nije bila direktna komparacija između metoda autentifikacije zasnovanih na SUAPCPC faktorima već analiza i daljnja upotreba rezultata za razvoj novog modela – Fishbone modela. Primjenom Fazi teorije i Fazi skupova u pogledu razvoja Fazi ekspertnog sistema (FES) izvršena je fazifikacija Fishbone modela u obliku univerzalnog autentifikacionog okvira - UAF. Na kraju, pomoću MatLAB urađena je implementacija Fishbone modela.

Dakle, najvažniji doprinos ove disertacije predstavlja prijedlog i dizajn Fishbone modela u obliku UAF koji omogućava numeričko vrednovanje nFA mehanizama. Na kraju, u disertaciji su dati prijedlozi o mogućim daljim poboljšanjima ovog modela.

Ključne riječi: *EMDI; zaštita; identitet; feedback; Fishbone model; SUAPCPC; UAF; FES.*

Naučne polje: Tehničke nauke

Uža naučna oblast: Informacione tehnologije i opperaciona istraživanja

UDK: 004.72.057.4

Model of information security in systems for identity and access management

Summary:

Subject of the research in this dissertation is a model of information security in identity and access management (IAM) systems, and the advancement of existing methods and security techniques. In a wider sense, the research is directed towards identity management, while in the narrower sense, it is directed towards authentication mechanisms which are key in process of the identity management. The aim of this research is to study previous results in this area, as well as development and advancement of existing models of security in user – oriented environment system of IAM. The problem of analyzing a model of information security is not a recent one. In the last two decades, there has been a significant number of papers in this area and a lot of authors have dealt with this issue by offering different models of digital identities and authentication mechanisms. However, literature analysis showed that such models have limitations, and values of such authentication solutions are descriptively expressed. It is about limitations that present a critical part of information security model (model of digital identity and model for evaluation of a numeric value of authentication solutions). These limitations were a motive for the development of the Education Model of Digital Identity (EMDI) as well as the Fishbone model which numerically evaluates the existing authentication solutions.

In comparison to all other models of identities, EMDI has introduced two processes: planning and feedback. The practical application of this model is made in Moodle platform using plugin for filtering inactive identities as an implementation of a submodel. The developed plugin has shown that it is possible to fill a gap in the security issue such as a partial absence of administrator control over process flow. One of the major advantages of the proposed model is the possibility of establishing a better communication between a student and an administrator. Therefore, this dissertation has a direct impact on filling security gaps in the current research and it contributes to a better understanding of the digital identity challenges faced by e-learning environment. In that way, it is possible to increase resistance to potential threats and risks such as copying, stealing or modifying credentials.

On the other side, in this dissertation the Fishbone model is proposed and designed, on the basis of which it can implement better security of information systems than existing ones. Moreover, given here is a comparison of the contemporary user authentication methods intended for mobile devices by differentiated key priorities such as security, usability, accessibility, pricing, complexity, privacy and convenience (SUAPCPC). It is necessary to highlights that the main purpose was not a direct comparison between authentication methods based on SUAPCPC factors but analysis and further utilization of results for development of new model – Fishbone model. For development of this model based on a crisp value, Fuzzy Expert System (FES) is used. Fuzzification of the Fishbone model is done in a form of universal authentication framework – UAF. Also, the implementation of the Fishbone model is done with the assistance of the MatLAB.

Therefore, the most important contribution of this dissertation is the proposal and design of the Fishbone model in a form of UAF that enables the numeric value of the nFA mechanisms. Finally, this dissertation gives proposals for possible further improvements of this model.

Key words: *EMDI; security; identity; feedback; Fishbone model; SUAPCPC; UAF; FES.*

Scientific field: Technical science

Specialized scientific field: Information technology and operational research

UDK: 004.72.057.4

SADRŽAJ

I UVOD

1.1. Ciljevi istraživanja

Razvoj Fishbone modela za numeričko vrednovanje metoda autentifikacije predstavlja glavni cilj ovog istraživanja. Opšti cilj istraživanja je usmjeren na razvijanje Edukacionog modela digitalnog identiteta – EMDI sa kojim se redukuju praznine koje omogućavaju razvijanje posebnog oblika kriminala koji se manifestuje u vidu zloupotreba, krađa i neovlašćenog objelodanjivanja identiteta. Da bi se u potpunosti ostvarili istraživački ciljevi, potrebno je da se omogući uvid u nedostatke u savremenim sistemima na osnovu kojih bi se uradilo poboljšanje u području menadžmenta identiteta i upravljanja pristupom – IAM. Za realizaciju glavnog cilja istraživanja potrebno je uraditi komparativni pristup metoda autentifikacija zasnovanih na korisničkim prioritetima kao što su zaštita, upotrebljivost, pristupačnost, kompleksnost, cijena, privatnost i pogodnost (SUAPCPC). Dakle, cilj istraživanja determiniše kombinovanje različitih metoda autentifikacija zasnovanih na SUAPCPC faktorima koji daju mogućnost razvoja novih autentifikacionih rješenja široko primjenjivih u različitim aplikacijama čime se postavljaju novi izazovi za napadače.

Pored navedenog, opšti cilj istraživanja treba da da i kritičku ulogu u životnom ciklusu digitalnog identiteta koji postaje imperativ za razumijevanje zaštite u sistemima za IAM. U tom pogledu, opšti cilj istraživanja je usmjeren na popunjavanje praznina u životnom ciklusu koji bi doprinijeli boljem očuvanju postojanosti digitalnih identiteta u sistemima za IAM. Time bi se osigurao maksimalni nivo zaštite upravljanja identitetima sa većom interoperabilnošću i komplementarnošću uz smanjenje mogućnosti stvaranja neaktivnih identiteta čime se omogućava i veća zaštite povjerljivih informacija. Na taj način generalno bi se postavili temelji u cjelovitijem razumijevanju problemskog područja i sinergijskog pristupa.

1.2. Polazne hipoteze

Za realizaciju predmentnog problema istraživanja postavljena je sljedeća osnovna (opšta) istraživačka hipoteza:

- *Razvojem novog jakog autentifikacionog mehanizma u korisničko-orjentisanom modelu menadžmenta identiteta zasnovanog na principu personalnog autentifikacionog uređaja, može se postići visok nivo zaštite identiteta.*

Iz osnovne istraživačke hipoteze mogu se izvesti sljedeće pojedinačne hipoteze:

- Proces razvoja mehanizma autentifikacije treba biti zasnovan na postojećim iskustvima i modelima.
- Personalni autentifikacioni uređaji podržavaju višestruke procese autentifikacije uključujući i biometrijske tehnologije.
- Analizom i prikazivanjem osnovnih mehanizama autentifikacije može se utvrditi potreba i efikasnost uvođenja jake autentifikacije.
- Procesom univerzalne jake autentifikacije može se omogućiti sigurnija zaštita identiteta.

1.3. Metode istraživanja

Za ostvarivanje postavljenih ciljeva doktorske disertacije, korišćene su sljedeće naučne metode:

- Analiza se koristi u postupku posmatranja metoda autentifikacija pri čemu se detaljno ulazi u strukturu problema, s ciljem uočavanja sličnosti i razlike.
- Sinteza se koristi u spajanju odabranih tehnologija i metoda.
- Apstrakcija i konkretizacija koriste se u postupku formiranja jake autentifikacije odnosno u procesu odabiru pojedinačnih metoda i tehnologija autentifikacije.
- Generalizacije i specijalizacije koriste se u postupku dizajniranja modela jake autentifikacije.
- Komparacija obezbjeđuje bazičnu procjenu trenutnih metoda autentifikacija primjenjenih u menadžmenta identiteta, radi formiranja sopstvenih prijedloga zaključaka.
- Deskriptivna metoda koristi se u postupku opisavanja tehnologija i metoda autentifikacije i logičkih arhitektura IAM.

1.4. Osnovni pojmovi zaštite informacija

Trend ubrzanog razvoja savremenih informatičkih tehnologija stvorio je uslove da bliska budućnost postane mnogo brže realnost. U tom kontekstu posmatranja, pojam zaštite informacija se izdiferencirao kao najvažnije globalno pitanje sa kojim se susreću sva društva i svi informacioni sistemi. Danas je gotovo nemoguće zamisliti neku oblast e-komunikacije (poslovne i društvene) bez njihove primjene. U tom pogledu, koncept zaštite informacija zahtijeva da mu se posveti posebna pažnja, naročito kada se radi o informacijama u kojima je pitanje zaštite od prvorazredne važnosti. Da bi se u potpunosti shvatio pojam zaštite informacija neophodno je prvenstveno razumjeti koncept pojma informacije.

1.4.1. Informacija

Informacija[1] potiče od latinske riječi "*in formare*" i izvorno je značila davanje oblika nečemu ali tokom svog razvoja izgubila je prvobitno značenje. Evoluirala je u interdisciplinarni pojam, pojam koji je relevantan za sve naučne discipline. Prema tome, kompleksnost pojma informacije kao planetarnog fenomena nije lako shvatiti niti jednostavno protumačiti. Sa informacionog aspekta, pojam informacije predstavlja pojam koji korisniku saopštava novost i time ga pokreće na mobilnost.

Istinski, značaj pojma informacije ne može biti prenaglašen pošto informacija predstavlja živi provodnik "*životnu snagu*" svakog sistema. Danas informacioni sistemi u svom funkcionisanju susreću se sa različitim vrstama informacija među kojima su najvažnije i najzastupljenije personalne ili lične informacije. Pod personalnom informacijom podrazumijevamo bilo koji dio informacije koji jedinstveno identifikuju pojedinca.

Primjeri personalnih informacija su kontaktne, identifikacione, biometrijske, demografske, profesionalne, školske, sportske, zdravstvene, inženjerske, finansijske informacije, onlajn aktivnosti (IP adresa, *cookies*, kredencijali za prijavu na sistem), i sl. Informacija, kao najvažniji resurs svake organizacije ili pojedinca čiji značaj i vrijednost je nemjerljiv, zahtijeva adekvatnu zaštitu.

[1]Više informacija o etimološkom i istorijskom značenju riječi informacija pogledati u Leksikonu stranih riječi i izraza - Vujaklija, M., Štampar Makarije, Beograd, 11 izdanje, 2012.

1.4.2. Zaštita

Pod pojmom zaštita (*engl. protection*) podrazumijeva se skup metoda, tehnika i aktivnosti koje imaju za cilj viši nivo sigurnosti. Zaštita zahtijeva opsežan i integrisan pristup, koji treba da podržava poslovne ciljeve ili misiju organizacije. Važnost zaštite informacija je u potrebi uspostavljanja i održavanja povjerenja u skladu sa zakonom i propisima između korisnika i davalaca tih servisa, štiteći pri tom njihov ugled. Kako bi se bolje razumio pojam zaštite potrebno je protumačiti pojam sigurnosti i sigurnosnog ciklusa (procesa). Sigurnost[2] (*engl. security*) potiče od latinske imenice *sēcūrĭtas, ātis f.* (bezbrižnost) i prideva *sēcūrus* (bezbrižan), a odnosi se na trenutnu primjenu. Pojam bezbjednost[3] (*engl. safety*) potiče od prefiksa bez (nepostojanje) i riječi bijeda, i predstavlja stanje korisnika u kojem je zaštićen od opasnosti, tj. odnosi se na apstraktni model zaštite. Prema Line-u *et al.*, [1] bezbjednost je definisana kao *"nemogućnost sistema da utiče na njegovo okruženje na nepoželjan način"* dok je sigurnost definisana kao "*nemogućnost okruženja da utiče na sistem na nepoželjen način"*. U kontakstu svega navedenog proističe da siguran sistem odgovara modelu koji je bezbjedan u odnosu na sva prava dok u suprotnom to nije slučaj. Dakle, siguran sistem je mnogo širi u odnosu na bezbjedan sistem ali pomenuti pojmovi posmatrani u kontekstu stanja sistema teže istom krajnjem cilju, kao što je garancija nesmetanog funkcionisanja sistema. Bivši direktor za obrazovanje Međunarodne asocijacije za bezbjednost računara – ICSA (engl. *International computer security association*) dr Mitch Kabay-a napisao je 1998. godine "*sigurnost je proces a ne stanje*".[4]

Sigurnost bilo kog informacionog sistema definiše se kroz zaštitne sfere ili prstenove koja ima za cilj stvaranje sigurnosnog mehanizma (*engl. security mechanism*). Uloga mehanizma zaštite je da detektuje, spriječi napad ili da sistem oporavi od napada. Na taj način održava se funkcionalnost sigurnosnog procesa. Sigurnosni proces je koncept koji opisuje osnovne faze koje sistem koristi za primjenjivanje i postizanje sigurnosnih ciljeva. Radi se o dinamičnom, kontinuiranom procesu koji je dizajniran da u sistemu identifikuje, procjenjuje, upravlja i kontroliše rizike. Započinje pitanjem, a odgovor neminovno dovodi do novih pitanja. Dakle, u osnovi kraj jednog sigurnosnog ciklusa neminovno dovodi do novog ciklusa. Ilustrativni prikaza sigurnosnog ciklusa je dat na slici 1.

[2] Više informacija o etimološkom i istorijskom porijeklu značenju riječi sigurnost pogledati na http://www.bezbednost.org/upload/document/medjunarodna_bezbednost-fragmenti.pdf
[3] Ibid.
[4] Ova izjava se pojavljuje u „Perils of Rushing to Market" u The Risk Digest, volume 19, izdanje 91, preuzeto sa online *http://catless.ncl.ac.uk/Risks/19.91.html*

Slika 1. Sigurnosni ciklus

Grafički, sigurnosni ciklus predstavlja cikličnu stazu koja se sastoji od 4 ponavljajuća čvora planiranje/procjena, zaštite, otkrivanja i odgovora.

- Planiranje/procjena (*engl. planning/assessment*) predstavlja polazno ili pripremno mjesto sigurnosnog ciklusa. Polazno mjesto se odnosi na pravila, procedure, pravne i druge upravljačke dužnosti kao i na tehničku procjenu stanja sigurnosti. Greške nastale u fazi planiranja direktno uzrokuju smanjenje nivoa sigurnosti određenog sistema i reflektuju se na sve naredne faze sigurnosnog ciklusa.
- Zaštita (*engl. protection*) tj. sprečavanje ili prevencija podrazumijeva primjenu protivmjera sa kojima bi se ugrožavanje sistema svelo na najmanju moguću mjeru. Ukoliko, proces zaštite zakaže primjenjuje se sljedeći korak otkrivanje.
- Otkrivanje ili detekcija (*engl. detection*) je kontinuirani proces otkrivanja novih prijetnji i ranjivosti trenutnih napada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost.
- Odgovor (*engl. response*) je proces oporavka, tj. saniranja posljedica napada, koji implicira formiranje povratne informacije *(engl. feedback).* Povratna informacija je najvažnije obilježje sigurnosnog ciklusa. Ona otkriva u kojoj mjeri je određeni sistem zaštićen. Sa povratnom informacijom sigurnosni ciklus se ne završava već se kontinuirano započinje novi ciklus.

Kissel [2] je definisao sljedeće pojmove:

- *prijetnja* (*engl. threat*) je "bilo koja okolnost ili događaj sa mogućim nepovoljnim uticajem na organizaciona djelovanja i imovinu, pojedince, druge organizacije ili

države kroz informacioni sistem putem neautorizovanog pristupa, destrukcije, otkrivanja ili modifikacije informacija, i/ili odbijanje servisa".

- *ranjivost* (*engl. vulnerability*) je "slabost u informacionom sistemu, procedurama sistema zaštite, internim kontrolama, ili implementacijama koje mogu biti iskorišćene od strane izvora prijetnji".
- *napad* (*engl. attack*) je "pokušaj da se stekne neautorizovani pristup prema servisnim sistemima, resursima, informacijama, ili pokušaj da se kompromituje integritet sistema".

1.5. Potreba za zaštitom informacija

Istorijski posmatrano, potreba za zaštitom informacija je stara koliko i sama ideja o čuvanju informacija. Potrebu za zaštitom informacija imaju oni koji posjeduju nešto što mogu da izgube. Potreba za zaštitom informacija proizlazi iz njene vrijednosti. Ubrzani razvoj tehnoloških i bežičnih mreža uslovio je povećanje novih i još organizovanih oblika prijetnji po informacionu sigurnost. Sa uporednim razvojem novih tehnologija nameće se potreba za učestalim preispitivanjem zaštite koja treba da ide u korak sa tehnološkim razvojem kako bi bila dovoljno upotrebljiva. Potreba za zaštitom informacija je posebno važna da se razumije od strane rukovodećih menadžera. Oni su jednako odgovorni kako za samu zaštitu informacija tako i za ukazivanje na potrebu i svjest o zaštiti informacija unutar organizacije.

Takođe, neophodno je istaći da potreba za zaštitom informacija se ogleda i u pogledu značaja zaštite kompanijskog brenda i ugleda. Radi prevlasti na tržištu danas brojne suprostavljene kompanije ciljano ili slučajno, direktno ugrožavaju konkurentske informacije u vidu neovlašćenog otkrivanja, modifikovanja ili sprečavanja pristupa odbijanjem usluge – DoS/DDoS (*engl. denial of service/distribution denial of service*) i sl. Kompanije primjenjuju najstrožije mjere zaštite kako bi onemogućili neovlašćen pristup osjetljivim informacijama. Na ovaj način se najdirektnije štiti moć i snaga koju kompanije posjeduju. Potrebno je napomenuti da efektivna zaštita informacija je implementirana, razumljiva, i odmjerena programskom politikom, procedurama i kontrolama koje konzistentno postižu saglasnost, kontrolu i zakonitost. Potreba za zaštitom informacija kao najvrijednijeg organizacionog resursa sadržani su u principima zaštite informacija.

1.6. Principi zaštite informacija

Principi zaštite informacija su nasljeđeni elementi u politici zaštite i razvojnim rješenjima koji definišu osnovne parametre potrebne za zaštitno okruženje. Potrebno je naglasiti da politika zaštite identifikuje pravila i procedure sa kojima se obezbijeđuje autorizovan pristup informacijama. Prema Peltier-u *et al.*, [3] glavni cilj i svrha zaštite informacija sadržani su unutar bazične zaštite trojstva (slika 2):

- Povjerljivost *(engl.Confidentiality),*
- Integritet *(engl. Integrity),*
- Raspoloživost *(engl. Availability)* – CIA[5].

Slika 2. Informaciono trojstvo

Akronim CIA naziv je nastao od engleskih početnih slova zaštite trojstva tj. od tri osnovna principa zaštite informacija povjerljivost *(engl. confidentiality),* integritet *(engl. integrity)* i raspoloživost *(engl. availability).* Pored bazične zaštite informacija postoji i dopunska zaštita informacija:

- identifikacija (*engl. identification*),
- autentifikacija (*engl. authentication*),
- autorizacija (*engl. authorization*),
- provjera ili revizija (*engl. auditing*),
- tajnost (*engl. secrecy*), i
- nemogućnosti poricanja informacija (*engl. non-repudiation*).

[5] Drugim permutacijama koncepta kao što su AIC su ponekad korišćeni da bi se izbjegla konfuzija sa najpoznatijom planetarnom obavještajnom agencijom.

Sva tri bazična navedena principa čine jezgro načela zaštite informacija. U menadžmentu identiteta svaka aktivnost se oslanja na jedan od tri navedena principa zaštite informacija. Bitno je napomenuti, da principi zaštite informacija nisu uvijek svi podjednako zastupljeni. Najočitiji praktični primjer zastupljenosti sva tri principa zaštite informacija je u obavještajnim i policijskim agencijama, i vojnim institucijama. S obzirom na značaj i važnost koju imaju principi zaštite informacija u informaciono-tehnološkom – IT sistemu posebno su opisani.

1.6.1. Povjerljivost

Prvi princip od CIA trojstva je povjerljivost. Istorijiski posmatrano, povjerljivost je najveću pažnju stekla primjenom u vojsci, a kasnije u obavještajnim i policijskim agencijama u kojima su izražene potrebe zaštite osjetljivih informacija ili resursa od potencijalnih napadača. Takođe, pored primjene u državnom sektoru princip povjerljivosti je od posebne važnosti i za poslove u privatnom sektoru, npr. u automobilskoj industriji. Sa povjerljivošću integrisanom u zaštitne mehanizme omogućava se značajna bezbjednosna usluga sa najvišim nivoom povjerenja odnosno najmanja mogućnost rizika da informacije budu izložene neovlašćenim subjektima. Ukoliko postoji prijetnja protiv principa povjerenja, neminovno je da i postoji mogućnost od neautorizovanog otkrivanja informacije. Princip povjerenja omogućava da informacije budu dostupne samo ovlašćenim subjektima ili sistemu kojima su i potrebne. Povjerljivost treba da bude primjenjena kroz sve aspekte sistema u kojima je moguća zaštita informacija od neovlašćenog pristupa, upotrebe, ili otkrivanja tokom obrade, pohranjivanja, i širenja.

Postoje brojni napadi usmjereni na narušavanje povjerljivosti kao što su presretanje mrežnog saobraćaja, krađe lozinki fajlova, socijalni inženjering, skeniranje portova, prisluškivanje, snifovanje i mnogi drugi. Narušavanje povljerljivosti nije ograničeno samo namjernim napadima, već i ljudskim greškama. Postoji mnogo mjesta na kojima je moguće izvršiti neovlašćeno otkrivanje povjerljivih informacija čiji uzrok je ljudska greška, previd ili nevičnost. Narušavanje povjerljivosti uzrokovano ljudskim faktorom može se desiti uslijed aktivnosti bilo kog korisnika, uključujući i administratora. Takođe, do narušavanja povjerljivosti može doći i usljed propusta u politici zaštite ili pogrešnoj konfiguraciji zaštitne kontrole. Sa druge strane, dva najčešća načina u praksi sa kojima se postiže povjerljivost je upotreba šifrovanja i steganografije. Šifrovanje je proces koji omogućava da se kod

otvorenog teksta učini nečitljivim odnosno nerazumljivim. Steganografija je proces stavljanja poruke unutar druge poruke na takav način da se ista sakrije od tuđih pogleda. Pored navedenih metoda, Whitman i Mattord [4] su naveli da se povjerljivost može obezbijediti i drugim brojnim mjerama kao što su klasifikacija informacija, pohranjivanje zaštitnih dokumenata, primjena jakih autentifikacionih procedura, i ekstenzivna personalna obuka.

1.6.2. Integritet

Drugi princip od CIA trojstva je integritet. Integritet je princip koji kod informacije zadržava istinitost i mogućnost namjerne modifikacije isključivo od strane autorizovanih subjekata. To ukazuje da napadač ne može neprimjećeno izmijeniti informaciju odnosno informacije mogu biti samo ažurirane ili dodate od strane onih kojima su i potrebna takva ažuriranja. U tom kontekstu, može se reći da zaštitni mehanizmi koji nude integritet time omogućavaju najviši nivo obezbjeđivanja informacije od neovlašćenog, nepredvidivog ili nenamjernog modifikovanja. Neautorizovana izmjena informacija uzrokuje gubljenje integriteta i pristup takvim informacijama treba onemogućiti sve do ponovne uspostave integriteta. Dopuštanje pristupa kompromitovanim informacijama može za posljedicu imati ugrožavanje pravilnog funkcionisanja cijelog sistema. Ove zlonamjerne promjene se mogu neopaženo desiti za vrijeme pohranjivanja informacija, u toku procesa ili širenja informacija, a da sistem pri tom ne ometano izvršava sve predviđene operacije. Integritet se ne posmatra samo u kontekstu informacije već programa i procesa.

Prema Maconachy-u *et al.*, [5] integritet treba da uključuje elemente kao što su tačnost, relevantnost i potpunost. Najjednostavniji primjer sistema u praksi u kojima je integritet od presudne važnosti je kontrola sistema vazdušnog saobraćaja. Drugi komercijalni primjeri sistema koji zahtijevaju visok nivo integriteta su zdravstveni, finansijski i proizvodno kontrolni sistemi. Kao i kod politike povjerljivosti, identifikacija i autentifikacija korisnika su ključni elementi politike integriteta što ukazuje da integritet zavisi od upravljanja pristupom. Mnoga mjesta neautorizovanih promjena osjetljivih informacija su uzrokovane ljudskom greškom, previdom i nevičnošću. Kao i sa povjerljivošću, narušavanje integriteta predstavlja konstantnu metu za zlonamjerne napadače. Prema Tipton-u i Kraus-u [6] postoje brojne prijetnje koje su usmjerene na narušavanje integriteta kao što su logičke bombe, neautorizovani pristupi, greške u kodiranju i aplikacijama, maliciozne modifikacije, namjerna zamjena, i sistem pozadinskih vrata (*engl. backdoor*).

Takođe, na narušavanje integriteta mogu uticati prijetnje kao što su hakerisanja, maskiranja, nezaštićeni preuzeti fajlovi, lokalne mreže, zlonamjerni programi (trojanski konj i virusi), i sl. Narušavanje integriteta kao i kod povjerljivosti, može nastupiti uslijed aktivnosti bilo kog korisnika (uključujući i administratora), i previda u politici zaštite ili pogrešnoj konfiguraciji zaštitne kontrole. Na primjer, ovlašćeni korisnik može modifikovati informacije i programe slučajno i namjerno ukoliko njegove aktivnosti na sistemu nisu pravilno kontrolisane. Prema Tipton-u i Kraus-u [7] tri su osnovna principa koja se koriste za uspostavljanje kontrole integriteta odobravanje pristupa na osnovu potrebno-da-zna, razdvajanja dužnosti, i rotacija obaveza. Integritet može biti obezbijeđen na mnogo načina od kojih su najznačajnija stroga upotreba upravljanje pristupom, rigorozna procedura autentifikacije, otkrivanje upada u sistem, šifrovanje informacija, ograničenje interfejsa, ulazi/provjeravanje funkcija i ekstenzivni personalni treninzi. Integritet i povjerljivost su međusobno zavisni jedno od drugog. Prema Tipton-u i Kraus-u [7] drugi koncepti, uslovi i pogledi integriteta uključuju tačnost, pravovremenost, autentičnost, potvrdnost, nemogućnost poricanja, odgovornost i nadležnosti, kompletnost, i opsežnost.

1.6.3. Raspoloživost ili dostupnost

Treći princip od CIA trojstva je raspoloživost. Raspoloživost je princip koji efikasno obezbijeđuje autorizovanim korisnicima pristup informacijama, objektima i resursima kada je to i zahtijevano. Drugim riječima, raspoloživost je usluga koja isključivo autorizovanim subjektima obezbijeđuje pravovremenu dostupnost informacijama i raspoloživost sistema. Ako zaštitni mehanizmi nude raspoloživost time omogućavaju najviši nivo bezbjednosti informacija, objekata i resursa. Raspoloživost se obično razmatra u dva aspekta:

- Sprečavanje DoS/DDoS napada.
- Gubitka procesne informacijske sposobnosti, koja može biti uzrokovana prirodnim katastrofama (npr. požari, poplave, oluje, zemljotresa), ili ljudskim destruktivnim aktivnosti (npr. rat, terorizam, i sl.).

Princip raspoloživosti podržava infrastrukturu koja uključuje mrežne servise, komunikacije i mehanizme upravljanja pristupom. Primjeri takvih usluga su sprečavanje odbijanja servisa – DoS/DDoS napada i sprečavanje infekcije virusima koji brišu ili oštećuju datoteku. Brojne su prijetnje po raspoloživost koje uključuju pogrešne uređaje, softverske greške i uticaj okruženja (toplota, atmosferske smetnje, prašina i sl.). Prema Tipton-u i Kraus-u [6] za održivu raspoloživost na sistemu potrebno je da kontrola bude na mjestu sa kojom se

obezbijeđuje autorizovan pristup i prihvatljiv nivo izvršenja, brzo rukovanje prekidom, redundantnost, održavanje pouzdanosti bekapa, isprečavanja gubljenja ili uništavanja informacija. Nadalje, u istom istraživanju isti autori navode da raspoloživost može biti obezbijeđena na nekoliko načina kao što su pravilno projektovanje posredničkog sistema isporuke, primjena efikasnog upravljanja pristupom, kontrolisano izvršavanje i mrežni saobraćaj, korišćenja vatrenog zida i rutera za sprečavanje DoS/DDoS napada, primjenjenu redundantnost za kritične sisteme, i održavanje i testiranje bekap sistema. Kao i kod inegriteta i povjerljivosti, narušavanje raspoloživosti proizlazi iz brojnih ciljanih napada. Mnogi su primjeri neautorizovane promjene osjetljivih informacija uzrokovani ljudskim faktorom, previdom ili nevičnošću. U događaje koji uzrokuju narušavanje raspoloživosti ubrajaju se greške slučajnog brisanja fajlova, promjene konfiguracija, i sl. Mnogi elementi informacionog trojstva su prvenstveno obezbijeđena sa odgovarajućim kontrolama zaštite informacija.

1.7. Kontrola zaštite informacija

Kontrola zaštite informacija je razvijena s ciljem bazične zaštite CIA trojstva. Da bi se uspješan koncept politike zaštite sproveo i stavio u funkciju neophodno je primijeniti tri ključna tipa kontrole zaštite informacija:

- fizičku kontrolu,
- tehničku kontrolu, i
- administrativnu kontrolu.

Ove tri kategorije kontrole mogu biti svrstane u jednu od preventivnih ili detekcijskih kontrola. Preventivna kontrola ima za cilj da izbjegne neželjene događaje, za razliku od detekcijske kontrole koja ima za cilj prepoznavanje neželjenih događaja koji su se već desili. Preventivna kontrola sprečava slobodu upotrebe kompjuterskih resursa i zbog toga može biti primijenjena samo u onom stepenu u kojem korisnik prihvata na volju. U detekcijsku kontrolu ubraja se provjera tragova (*engl. audit trails*), detekciju upada u sistem (*engl. intrusion detection methods*), i provjera sigurnosne sume (*engl. checksums*). Postoje i druge vrste kontrolnih kategorija koje su prije svega dodatak preventivnim i detekcijskim kontrolama, a ne spadaju ni u jednu ni u drugu kategoriju kontrola, kao što su:

- zaštitne ili zastrašivačke kontrole (*engl. deterrent control*) – imaju za cilj da u startu obeshrabre korisnika od pokušaja zlonamjernih aktivnosti kršenja informacionih sigurnosnih politika i procedura.
- korektivna kontrola (*engl. corrective control*) – ima za cilj da izvrši korekciju prava pristupa koja su u datim okolnostima bila pogrešno podešena. Izvršavanje korektivne kontrole može rezultirati izmjenama u postojećoj fizičkoj, tehničkoj i administrativnoj kontroli.
- kontrola oporavka (*engl. recovery control*) – ima za cilj da obezbijedi neophodnu pomoć za oporavak od problema pružajući time pomoć organizacijama da nadoknadi izgubljena materijalna sredstva. Primjer kontrole oporavka su bekapi, alternativni sajtovi i pohranjeni grupisani diskovi.

1.7.1. Fizička kontrola

Fizička kontrola koristi tehnologije kao što su magnetne kartice, radio frekvencijska identifikacija – RFID (*engl. radio frequency identification*), ili biometrijske zaštite s ciljem sprečavanja neautorizovanog pristupa pohranjenim informacijama ili mrežnim resursima. Fizička kontrola sastoji se od kontrole objekata kao što su grijanje, ventilacija i klimatizacija – HVAC jedinica (*engl. heating, ventilation and air condition*), električni generatori i protivpožarni sistemi. Fizička kontrola obuhvata zaključavanja vrata, stražarska obezbjeđenja, bedževe, alarme i slične mjere za kontrolu pristupa računarskom sistemu. Povrh toga, mjere zahtijevaju zaštitu računara i srodne opreme i njihovog sadržaja od prirodnih i ljudskih prijetnji. U prirodne prijetnje ubrajaju se sve atmosferske neprilike poput padavina (kiše, grada, leda i snijega) vjetra, oluja i ekstremnih temperatura, te geofizičkih neprilika kao što su vulkanske aktivnosti koji mogu izazvati niz neprilika poput požara i poplava. U prirodne neprilike takođe ubrajaju se i biološke prijetnje a to su razne bolesti koje mogu uzrokovati smanjenje broja sposobne radne snage. Prirodne prijetnje mogu uzrokovati veliku štetu i materijalne gubitke ali na njih se ne može uticati odnosno pomoću kontrole oporavka moguće je preduzeti mjere za uspostavljnje normalizacije funkcionisanja sistema. U ljudske aktivnosti koje mogu biti namjerne i slučajne, ubrajaju se krađa, neposlušnost, otkrivanje osjetljivih informacija, sabotaža, nenamjerno oštećenje imovine, zloupotreba položaja, i neovlašćen pristup informacijama ili resursima.

Fizička zaštita treba da obezbijedi zaštitu od neispravnih instalacija, požara, poplava, zagađivanja okoline, štetnih zračenja, neurednog napajanja električnom energijom,

nepovoljnih klimatskih i temperaturnih uslova za funkcionisanje sistema, elementarnih nepogoda, i sl. Fizička kontrola ima dvostruki cilj. Prvo, djeluje preventivno odnosno sprečava neautorizovanom osoblju pristup kompjuterskim resursima. Drugo, djeluje detekcijski tj. upozarava osoblje zaštitnog servisa da su mjere fizičke sigurnosti narušene. Prema Murphy -u [8] primjeri ovih kontrola su bekap fajlova i dokumentacija, fizičko ograđivanje, čuvari, bedž sistemi, dupli vratni sistem, brave i ključevi, rezervna elektro napajanja, biometrijska kontrola pristupa, odabir lokacije i protivpožarna zaštita, detekcija pokreta, osvjetljenja, detektor dima i vatre, nadgledani kablovski televizijski sistemi i senzori, i alarmi. Takođe, ova kontrola omogućava korišćenje kompjuterskih pogodnosti. Primjeri kompjuterskih pogodnosti su korišćenja lokacija kućnih kompjuterskih resursa, podrške korišćenju, kompjuterske hard kopije i unošenje podataka sa eksternih hard diskova.

1.7.2. Tehnička kontrola

Pod tehničkom zaštitom podrazumijeva se upotreba zaštite ugrađene u kompjuterski hardver, operativni ili aplikativni softver, komunikacijske protokole i srodne uređaje. Tehnička kontrola se koristi za ograničeni pristup mrežnim resursima i uređajima koji se koriste u organizacijama. Najčešće je to individualno korisničko ime i lozinka korišćena za pojedinačni pristup uređajima ili lista za kontrolu pristupa – ACL (*engl. access control list*) koje su dio mrežnog operativnog sistema. U literaturi [9], Harris i Maymí su naveli da termin tehnička kontrola se naziva i logičkom kontrolom. Preventivna tehnička kontrola se koristi da se spriječi, neautorizovanom osoblju ili programima, udaljeni pristup kompjuterskim resursima. Prema Hansche-u *et al.*, [10] primjeri ove kontrole su softverska kontrola pristupa, antivirusni softveri, biblioteka kontrolnih sistema, lozinka, smart kartica, enkripcija i *dial – up* kontrola pristupa, i sistem povratnih poziva.

Detekcijska tehnička kontrola upozorava osoblje o narušavanju ili pokušaju narušavanja preventivne tehničke kontrole. Primjeri ove kontrole uključuju provjeru tragova tj. zapise u dnevnicima (omogućava rekonstrukciju događaja i ispitivanje pojedinih događaja) i sisteme za detekciju napada. Sistemi za detekciju napada mogu biti posebno efektivni u otkrivanju slučajeva u kojima se napadač prerušava u autorizovanog korisnika ili kada je autorizovani korisnik uključen u neautorizovane aktivnosti.

1.7.3. Administrativna ili personalna kontrola

Administrativne ili personalne kontrole kao što sam naziv ukazuje bavi se osobljem s ciljem obezbijeđivanja informacionog trojstva informacija i programa. Sprovode se na mjestu pristupa i podrazumijevaju politiku organizacije koja opisuje njeno funkcionisanje. One predstavljaju vodič zaposlenima koji određuje način na koji njihovi zadaci treba da budu urađeni kao i resurse koji se koriste za tu realizaciju. Administrativna zaštita sastoji se od ograničenja u upravljanju, operativnih procedura (procedure kojima se provjeravaju potrebne dozvole za osobe koje imaju pristup kompjuterskim resursima), nadležnih procedura (procedure u kojima se određuju odgovornosti) i dodatnih administrativnih kontrola uspostavljenih da obezbijedi prihvatljiv nivo zaštite za kompjuterske resurse. Osim navedenog, administrativna kontrola uključuje procedure uspostavljene da osiguraju da sve osobe koje imaju pristup kompjuterskim resursima imaju i autorizovan pristup i određenu zaštitnu dozvolu. Administrativna kontrola takođe može biti posmatrana kao preventivna i detekcijska kontrola. Preventivna administrativna kontrola je personalno-orijentisana tehnika za kontrolisanje ljudskog ponašanja osiguravajući informaciono trojstvo kompjuterskih informacija i programa. Detektivska administrativna kontrola se koristi za određivanje koliko su ispunjene politike zaštite i procedure kao i za otkrivanje prevara. Prema Tudor-u [11] primjeri administrativne kontrole su:

- zaštitna svijest i tehnička obuka,
- razdvajanje dužnosti,
- procedure za odabir i otpuštanje kadrova,
- zaštitne politike i protokoli,
- supervizija (nadziranje),
- oporavak od katastrofa,
- oporavak od nepredviđenih situacija i hitnih planova, i
- korisnička registracija za kompjuterski pristup,
- zaštitni pregled i provjeru,
- procjenjivanje djelotvornosti ugrađenih sigurnosnih kontrola,
- dani odmora (dopust),
- pozadinska istraživanja, i
- rotaciju obaveza.

II OPIS PROBLEMA

2.1. Opis problema

Uzimajući u obzir današnju ulogu i značaj tehničkih mjera u zaštiti informacija, u ovom radu je predložena tema "*Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom*". Predložena tema treba da da konkretan odgovor na sadašnje i buduće informacione izazove. Međutim, da bi se došlo do adekvatnog odgovora neophodno je sagledati realne probleme koji se nalaze na tom putu. Kako je tema ovog rada širokog okvira, time je problem istraživanja u širem smislu riječi, usmjeren na menadžment identiteta, dok u užem smislu riječi na područja autentifikacija koji su ključni u menadžmentu identiteta. Dakle, bazični problem istraživanja svodi se na analiziranje postojećih metoda autentifikacija i razvoja novog metoda autentifikacija u korisničko-orijentisanoj arhitekturi. Prema Kiljan-u *et al.,* [12] autentifikacija kao primarna mjera zaštite je glavna istraživačka tema u polju zaštite informacija. Ovaj problem nameće potrebu za sistematičnim pristupom prema integralnom pristupu odabira korisničkih prioriteta u dizajnu i razvoju autentifikacionog rješenja u sistemima menadžmenta identiteta. Suština problema usmjerena je na informacije koje treba da budu zaštićene od unutrašnjih i eksternih napada. Ovaj problem može se posmatrati kroz prizmu razvoja i ekspanziju digitalnih tehnologija.

Sa posljednjim tehnološkim razvojem stvoreni su uslovi za brži razvoj i snažniju primjenu interneta. Smatra se nosiocem novog talasa digitalne revolucije u kojem je umreženo mnoštvo servisa koji međusobno komuniciraju. Posebno trendovi u korišćenju novih digitalnih tehnologija doveli su do stvaranja neslućenih mogućnosti u pogledu razvoja *e-learninga* i e-poslova u različitim područjima kao što je e-bankarstvo, e-trgovine, i sl. Internet predstavlja suštinski alat u *e-learning* okruženju koji obezbijeđuje korisničko-prijateljski interfejs prema korisniku. Dinamičan razvoj i rapidno širenje digitalnih tehnologija uslovili su kritičnu potrebu za dijeljenjem i pohranjivanjem informacija među složenijim organizacijama kao što su akademske institucije. Za pristup takvim resursima neophodno je da studentima budu dodjeljeni digitalni identiteti tj. studenti su obavezni da se digitalno identifikuju kako bi se znalo "*ko, kada i gdje*" pristupa resursima. U svakodnevnom *e-learning* okruženju digitalni identiteti imaju rastuću ulogu i kao takvi zahtijevaju odgovarajući pristup posebno u

aspektu upravljanja. Potreba za boljim upravljanjem digitalnih identiteta je glavni istraživački cilj koji ostaje neriješen u polje *e-learning* okruženja. Upravo ova činjenica opisuje sveobuhvatnu kompleksnost identiteta u *e-learning* okruženju koji zahtijeva da se posveti posebna pažnja prema pitanju zaštite. U svijetlu svih tih problema, problem zaštite digitalnih identiteta predstavlja fundamentalni istraživački problem u *e-learning* okruženju.

Dakle, u širem smislu riječi, prvi identifikujući problem u ovom radu se reflektuje kako popuniti praznine u životnom ciklusu digitalnog identiteta sa kojima bi se doprinijelo boljem očuvanju konzistentnosti digitalnih identiteta *u e-learning* okruženju. Pitanje zaštite digitalnih identiteta je postalo kritično pitanje za održivost bilo koje edukacione organizacije. Nesumnjivo, digitalne tehnologije u *e-learning* okruženju značajno su poboljšale studentski način učenja ali takođe su doprinijeli povećanom izlaganju personalnih informacija koje mogu voditi ka krađi identiteta [13]. Ovi problemi postaju mnogo kompleksniji u većim edukacionim sistemima kao što su Univerziteti. Sa druge strane, razvoj i širenje digitalnih tehnologija imaju veliki uticaj na studentsku percepciju digitalnih identiteta. Brzi tehnološki razvoj ima direktan uticaj na svijest i društvene promjene, ohrabrujući studente na upotrebu raspoloživih digitalnih identiteta čineći stvaranje identiteta jednostavnijim i jeftinijim (obično besplatnim), a istovremeno značajno doprinosi podsticaju u smislu njegove kratkoročnosti i nevažnosti. Posljedice takvog tehnološkog razvoja su da studenti često puta pribjegavaju istovremenom stvaranju višestrukih identiteta [14]. Na taj način dolazi do kontinuiranog povećanja broja digitalnih identiteta unutar jednog *e-learning* okruženja. Posljedice po korisnika su u poteškoći pamćenja brojnih kredencijala, dok za menadžment identiteta problem je u upravljanju i održavanju takvih kredencijala. Povećani broj identiteta uzrokuje situaciju u kojoj mnogi digitalni identiteti postaju neaktivni. Takva situacija predstavlja jedno od primarnih hakerskih mjesta za razbijanje sistema [15]. Ovo je najozbiljniji problem u *e-learning* okruženju jer studenti su onemogućeni da imaju potpunu kontrolu u pogledu upravljaja i zaštite njihovih digitalnih identiteta. Pored brojnih razvijenih tehnologija, studenti još uvijek imaju poteškoće o sticanju jasne slike o njihovom životnom ciklusu digitalnog identiteta [16]. Ovo istraživanje daje prijedlog rješenja u vidu novog Edukacionog modela digitalnog identiteta – EMDI sa kojim je moguće popuniti praznine u životnom ciklusu digitalnog identiteta, a time i doprinijeti boljem očuvanju kozistentnosti digitalnih identiteta u *e-learning okruženju.*

U užem smislu riječi, drugi identifikujući problem u ovom radu reflektuje se na autentifikaciona područja. "*E-doba*" je istaklo u prvi plan potrebu za kvalitetnijim dizajniranjem metoda zaštite u sistemima IAM. Bazični cilj dizajniranja autentifikacionog rješenja je usmjeren na korisničke prioritete kao što su zaštita, privatnost, povjerenje, upotrebljivost, pristupačnost, kompleksnost, cijena, i pogodnost (SUAPCPC). Prilikom dizajniranja autentifikacionog rješenja, korisnički prioriteti predstavljaju poseban problem u smislu njihovog analiziranja. Ovaj problem se manifestuje pri izradi autentifikacionog mehanizma gdje se zanemaruju činjenice da različiti korisnici imaju različite prioritete. Korisnički kriterijumi se razlikuju od aplikacije do aplikacije. Na primjer, neko hoće da ima zaštitu podataka kao prioritet (e-bankarstvo), dok drugi ne (pristup komercijalnim veb sajtovima). Ovo se dešava kada zaštitni faktor može spriječiti ili ograničiti regularnu primjenu drugih faktora, gdje na primjer neko hoće da ima cijenu kao prioritet (evidencija o prisutnosti zaposlenih na poslu). U kontekstu toga, očigledno je da korisnici u autentifikacionim pristupima nemaju kriterijume istog stepena značajnosti što dovodi do problema u vezi dodijeljivanja odgovarajućih težinskih koeficijenta (težina) ili pondera za kriterijume.

Prilikom dizajniranja višefaktorskog autentifikacionog – nFA/MFA rješenja pojavljuje se kompleksan problem oko izbora odgovarajućeg rješenja. Primjera radi, ako korisnik ne uspjeva iskoristiti nFA rješenje u kojem su ponuđene zaštitne mjere kao prioritet takvo rješenje je potpuno beskorisno za njega. Takođe, često se zanemaruje činjenica da različiti korisnici imaju različite fizičke i mentalne sposobnosti, potrebe, godine i umijeća. Fizičke i mentalne nesposobnosti u vidu oštećenja sluha, vizuelnog, fizičkog, kongitivnog oštećenja i disleksije mogu predstavljajati prepreku u procesima autentifikacija. Na primjer, brojni tokeni kao što su PIN – kodovi nisu prihvatljivi za korisnike sa smanjenom memorijom ili ljude disleksičare, ili za ljude koji imaju problem sa brojevima. Ako su brojevi prezentovani vizuelno oni će predstavljati problem za ljude sa oštećenim vidom, i sl. Tokom izrade autentifikacionog rješenja neophodno je voditi računa i o sociološko-ekonomskim interesima za razvoj pristupačnog nFA rješenja. Sve ovo ukazuje da korisnički prioriteti igraju veoma važnu ulogu u dizajniranju bilo kog nFA rješenja. To podrazumijeva da se pri dizajniranju određenog nFA rješenja u IAM treba voditi računa o svim korisničkim prioritetima.

Danas postoje u upotrebi brojna pojedinačna autentifikaciona rješenja sa kojim se ne postiže visok nivo zaštite identiteta. Svaki od pojedinačnih autentifikacionih rješenja

ima kako određene prednosti tako i značajne nedostatke koji mogu biti neatraktivni za većinu servis provajdera. Realno sagledavanje njihovih prednosti odnosno nedostataka predstavlja kompleksan problem koji posebno dolazi do izražaja pri dizajniranju nFA rješenja. Sa kombinovanjem pojedinačnih metoda autentifikacija dizajniraju se nFA rješenja, koji se oslanjaju na više od jednog faktora. Primarni cilj stvaranja nFA rješenja je uslovljen povećanjem nivoa zaštite. U važnim djelatnostima kao što je bankarstvo potrebna su jaka mobilna nFA rješenja koja nije moguće realizovati ako nisu sistematično i argumentovano sagledane pojedinačne metode autentifikacije. Pri upotrebi jake autentifikacije mnogo je faktora, prije svih korisničkih, koji utiču na obezbijeđivanje dodatne zaštite, i pri tom je potrebno naglasiti da većina poboljšanja u nFA neće riješiti nasljeđena pitanja koja se javljaju u pojedinačnim metodama autentifikacija. Pored već gore opisanih problema, prilikom dizajniranja nFA dodatni problem se pojavljuje u pogledu izbora pravilne procjene metode autentifikacije tj. koje pojedinačne metode autentifikacije mogu biti primjenjive za integraciju u novo nFA rješenje. Dakle, problem nFA rješenje je usmjeren na izbor pojedinačnih metoda čijim kombinovanjem se omogućava sinergijskim pristup. Na taj način integrišu se različite korisničke grupe sa različitim vještinama, dobima i sposobnostima, različitim pozadinskim kulturama kao i mogućnost pristupa sa različitih uređaja.

U poslednjih nekoliko godina sa ubraznim razvojem mobilnih uređaja (mobilni telefoni, *personal digital assistants (PDAs)*, i sl.), ovaj pristup se izdiferencirao kao posebna istraživačka tema u informacionim tehnologijama. Problem ovog autentifikacionog pristupa, u kojem je korisnik stavljen u centar pažnje, je usmjeren na centralizovani pristup informacija. Sa centralizovanjem informacija ”*sve u jednom*” na mobilnim uređajima poput PDA/mobilnih telefona može se narušititi integritet korisnika ukoliko isti uređaji dospiju u pogrešne ruke. Na taj način se dodatno usložnjava pitanje očuvanja postojanosti korisničkog identiteta i personalnih informacija. Prema tome, problem ovog autentifikacionog pristupa je usmjeren prema korisničkom faktoru upotrebljivosti. Upotreba mobilnih telefona u internet servisima zahtijeva kombinovanje i upotrebu različitih uređaja i tehnologija u procesu autentifikacije čije su arhitekture i komunikacioni kanali potpuno različiti. Takođe, problemi dolaze i sa potrebom da se posjeduju posljednje tehnologije koje mogu ostaviti ranjivost u metodama autentifikacija.

Trend rapidnog tehnološkog progresa mobilnih tehnologija uslovio je da su mobilni uređaji postali fenomen, neodvojivi dio ljudskog života. Ljudi su međusobno postali progresivno povezaniji, a u toj interakciji mobilni uređaji igraju značajnu ulogu. Oni danas predstavljaju esencijalne multifunkcionalne alate u svakodnevnom ljudskom životu čime su postali mnogo više od pukog sredstva za komunikaciju. Popularnost i atraktivnost mobilni uređaji su stekli zahvaljujući ogromnom razvoju u polju bežičnih mreža, softverskih i hardverskih konfiguracija. Povećana popularnost mobilnih uređaja ukazuju na trend kretanja tehnoloških granica. Kroz eksponencijalni tehnološki razvoj, mobilni uređaji omogućavaju nekoliko različitih načina za komunikaciju, a poboljšani su sa različitim funkcijama koje pružaju korisniku neslućene mogućnosti. Perfomanse mobilnih telefona u vidu moćnog procesora i malih dimenzija učinili su ga "*džepnim*" komjuterom prihvatljivim i primjenjivim u mnogim privatnim i poslovnim aplikacijama. Mnogi korisnici koriste pametne telefone za pohranjivanje personalnih informacija koje žele sačuvati od tuđih pogleda [17]. Tokom proteklih godina, brzi razvoj različitih mobilnih tehnologija je stvorio nove izazove u pogledu prema mobilnim autentifikacionim procesima. Ovaj pristup, ima rastuću važnost jer nova autentifikaciona rješenja su bila razvijena primjenom različitih tehnologija. Razvojem velikog broja različitih autentifikacionih rješenja posebno se uzdiže pitanje u pogledu izbora i procjene najboljeg rješenja.

Da bi se izvršio najbolji izbor i procjena bilo kog autentifikacionog rješenja, potrebno je izvršiti njegovo numeričko vrednovanje. Međutim, u literaturi je prisutno deskriptivno vrednovanje, na osnovu kojeg nije moguće izvršiti kvalitetan izbor i procjenu autentifikacionog rješenja. Ipak, da bi se došlo do numeričkog vrednovanja nekog autentifikacionog rješenja potrebno je izvršiti kvantifikaciju deskriptivnog vrednovanja. Dakle, problem je usmjeren na numeričko vrednovanje koji zahtijeva adekvatan pristup u pogledu opisivanja, pregleda i poređenja savremenih mobilnih metoda autentifikacija kao i korisničkih prioriteta – SUAPCPC faktori. Neki od ovih faktora su dobro – poznati, dok su drugi mnogo manje razumljivi. Razlog je što sveobuhvatni komparativni pristupi korisničkih prioriteta i savremenih mobilnih metoda nisu urađeni holistički u jednoj cjelini. Pored navedenog, problem nastaje kod korisničkih zahtijeva u kojima je neophodno da bude zastupljeno istovremeno više prioriteta u autentifikacionom rješenju. Kako ne postoji jedinstven metod autentifikacije zasnovan na SUAPCPC faktorima pribjegava se kreiranju nFA. Problem postaje još izraženiji kod odabira najpogodnijeg rješenja odnosno univerzalnog rješenja. U pogledu navedenog, proističe

da je trenutno jedan od najvećih problema suočenih u informacionom društvu stvaranje "*najpogodnijeg*" šablona za mobilne autentifikacije koji bi bio primjenjiv prema što je moguće većem broju korisnika [18]. Drugim riječima, problem je kako dizajnirati univerzalni autentifikacioni okvir (*engl. universal authentication framework – UAF*) za kvantifikovanje nFA u mobilnom okruženju odnosno dati odgovarajuće matematičke formule za dvo/tro faktorsku autentifikaciju (2FA/3FA) ili nFA. Takav UAF bio bi zasnovan na korisničkim prioritetima (SUAPCPC faktorima) koji imaju istu važnost. Kim *et al.,* [19] su istakli značaj i važnost stvaranja UAF u mobilnom okruženju.

Kao što je ranije pomenuto, problem za realizaciju UAF predstavlja lingvističko izražavanje pojedinačnih vrijednosti metoda autentifikacija. U literaturi, vrijednost mobilnih autentifikacionih rješenja je izražena sa različitim lingvističkim pojmovima kao što su jak, jače, slabo, slabije, vrlo nizak, nizak, srednje, visok, vrlo visok, i sl. Ovi pojmovi su deskriptivno korišćeni da ukažu u kom obimu određeni metod autentifikacije ispunjava specifičan skup korisničkih kriterijuma. Korišćeni pojmovi predstavljaju prepreku u stvaranju "*najpogodnijeg*" mobilnog rješenja za mobilne autentifikacije. Usljed nedostatka numeričke procjene mobilnih autentifikacionih rješenja, izbor "*najpogodnijeg*" mobilnog rješenja je prožeto sa nejasnoćama i neodređenostima. U svijetlu tih razmatranja, problem procjene mobilnih rješenja ne može biti generalizovan ili analiziran upotrebom binarne logike koja ima samo dvije istinske vrijednosti, istinu – 0, ili lažno – 1. Mobilna autentifikaciona rješenja su kompleksna područja gdje konvencionalni matematički modeli ne mogu dati zadovoljavajuće rezultate. Stoga, opisani problem zahtijeva upotrebu inteligentnih sistema koji mogu dati višestruku logiku sličnu ljudskom razmišljanju i interpretaciji.

U kontekstu svih gore pomenutih okolnosti, suštinski problem ovog rada svodi se na upotrebu novog metodološkog pristupa koji može biti korišćen kao odgovarajući matematički alat u potrazi za krisp vrijednostima mobilnih autentifikacionih rješenja. Na osnovu primjene te metodologije moguće je formirati UAF. Generalno, ovo istraživanje daje prijedlog rješenja problema deskriptivnog vrednovanja metoda autentifikacija u vidu dizajniranja *Fishbone* modela. Ovaj model numerički vrijednuje postojeća autentifikaciona rješenja zasnovana na korisničkim SUAPCPC faktorima, i na osnovu čijih vrijednosti je moguće dati prijedlog novog efikasnijeg modela zaštite informacija.

III MENADŽMENT IDENTITETA

Menadžment identiteta je gotovo neizostavna komponenta današnjih organizacija [20] koja čini integralni dio bilo kog menadžment identiteta i upravljanje pristupom (IAM). Sam naziv pojma ukazuje da koncept i pojam identiteta igra ključnu ulogu u menadžmentu identiteta. Sa razvojem inovativnih tehnologija, identiteti su postali dinamični i relativni ali to nije dovelo do prevazilaženja izazova u pogledu njihovog upravljanja. Taj izazov je prožet kroz različite procese njihovog životnog ciklusa kao što su procesi stvaranja i širenja identiteta, upotrebe i održavanja u vidu postupanja u skladu sa poslovnim pravilima čuvanja identiteta, sinhronizacije jednih sa drugima, kao i procesima ukidanja odnosno uklanjanja kada je to zahtijevano. Sa druge strane, trend razvoja modernih digitalnih tehnologija stvorio je uslove u kojima korisnici mogu brže, lakše i jeftinije stvarati digitalne identitete. Na taj način povećava se broj digitalnih identiteta po korisniku unutar istog sistema što može stvarati poteškoće kod korisnika u vidu pamćenja brojnih kredencijala. Povećanje broja digitalnih identiteta nerijetko može uzrokovati situacije u kojima mnogi digitalni identiteti postaju neaktivni. Ovo je posebno izraženo u složenijim sistemima što čini gotovo idealnim mjestima za njihovo kompromitovanje. Sve ovo ukazuje da nije lako upravljati velikim brojem različitih korisničkih naloga u različitim servisima i parcijalnim identitetima koji su pridruženi korisnicima. Tokom proteklih godina upravljanje identitetima je postala centralna tema u informacionim tehnologijama, politici i administraciji u javnom i privatnom sektoru [21]. Upravo, u cilju olakšanja i prevazilaženja svih tih navedenih problema sistemi menadžmenta identiteta su stvoreni.

Prema Gomi-u [16] menadžment identiteta je zasnovan na tehnologijama podržanim elektronskim interakcijama u kojima se zahtijeva identitet informacije. Prema Windley-u [22] menadžment identiteta se definiše kao proces kojim se postojeće tehnologije koriste za upravljanje informacijama o entitetu digitalnog identiteta kao i za upravljanje pristupa resursima. Procesi menadžmenta identiteta uključuju procedure njegovog životnog ciklusa, protokole za dokaze o identitetima i druge informacije koje se dijele među učesnicima. U mobilnom okruženju, menadžment identiteta se može koristiti za razvijanje servisa koji dosljedno prate korisnika u okruženju u kome se primjenjuju metode autentifikacije. Dakle, osnovna svrha upotrebe menadžmenta identiteta u mobilnom okruženju je definisanje okruženja i pravila za rukovanje parcijalnim

korisničkim identitetima. Prema Wood-u [23] menadžment identiteta ima dvije centralne komponente i to:

- Menadžment "*od*" identiteta – je proces izdavanja i korišćenja digitalnih identiteta i kredencijala za autentifikaciju.
- Menadžment "*po*" identitetu – kombinuje potvrđene korisničke identitete sa njihovom autorizacijom kako bi se odobrio pristup resursima.

Menadžment identiteta se posmatra kao suštinski elemenat mnogih servisa zaštite jer obezbijeđuje uvjerenje o korisničkoj legitimaciji. Da bi se u potpunosti shvatio koncept menadžmenta identiteta neophodno je prvo shvatiti koncept pojma identiteta i digitalnog identiteta.

3.1. Identitet i digitalni identitet

3.1.1. Identitet

Pojam identiteta danas predstavlja jedno od najvažnijih pitanja savremenog društva. U opštem smislu, termin identiteta ima šire značenje i upotrebu. Radi se o veoma komplikovanom konceptu sa mnogo nijansi u rasponu od teoretskog do praktičnog. U realnom svijetu identitet ukazuje na fizički entitet ili subjekat koji je jedinstven. Osnovna vrijednost identiteta je u njegovoj fleksibilnosti da u posmatranom području omogući utvrđivanje jedinstvenosti i određenosti entiteta u odnosu na druge entitete. Identitet se sastoji od karakteristika, atributa i preferenci koje mogu biti privremene ili trajne. Taj skup obilježja odnosno individualnih karakteristika predstavlja individualnost. Kombinacijom ovih atributa formira se jedinstvena slika pojedinca ili subjekta. Na osnovu navedenog, može se zaključiti da specifičnosti entiteta koje ga izdvajaju predstavljaju njegov identitet. Doživljaj identiteta je neminovno subjektivan sa tačke gledišta posmatrača (kao što je slučaj sa fizičkim identitetom). Prema tome, identitet nije samo ono što pojedinac želi da otkrije o sebi, već i šta drugi pripisuju, zaključuju, vjeruju i saznaju o njemu. Zapravo, većina personalnih identiteta je upravo tog tipa, što ne znači da su te informacije istinite, obmanjujuće, netačno predstavljene, i sl. To upućuje na činjenicu da identitet može da posjeduje više vlasnika, a da pri tom nije potrebno da odgovara stvarnosti. Identitet nije samo vlasnik od strane subjekta koji to opisuje, već i od drugih vlasnika koji prikupe saznanja o njemu. Najjednostavniji

primjer je ljekarski nalaz prikupljen od strane specijaliste i drugog doktorskog osoblja koji predstavljaju njihovo vlasništvo. Ti nalazi mogu se dati pacijentu samo na uvid bez mogućnosti prava i na najmanju izmjenu.

Obično se o identitetu govori u jednini, iako određeni korisnik može da ima višestruke identitete od kojih svaki prezentuje različite karaktere ili ličnosti. Radi toga, u literaturi se pojam višestrukih identiteta mogu pronaći pod nazivom "*ličnosti*". Koncept višestrukih identiteta je kolekcija karakteristika koja često karakteriše samo određene aspekte identiteta, primjera radi ulogu, poziciju ili status korisnika u datom društvenom, poslovnom ili nekom drugom kontekstu. Identiteti imaju tendenciju da izgledaju poput više različitih aspekata realnog identiteta ali pri tom i drugi subjekti imaju specifičan pogled koji odgovara samo podskupu tih atributa. Višestruki identiteti su specifično povezani sa pojedincem. Oni zapravo predstavljaju različite poglede na subjekat, npr. ko je i kakve atribute posjeduje. Višestruki identiteti su međusobno povezani na nekoliko informacionih elemenata koji su korišćeni u procesu pristupanja resursima npr. ime, adresa, datum rođenja, i sl. Najprostiji primjer subjekta sa dva različita identiteta je kada korisnik jedan identitet koristi u svojstvu društvenih mreža, a drugi u svojstvu zaposlenog radnika. Subjekat identiteta kao korisnika društvene mreže može da se sastoji iz imena korisničkog naloga kao identifikatora, poznavanja lozinke kao kredencijala, porodičnih imena, liste prijatelja i zapisa aktivnosti kao atributa. Sa druge strane, identitet subjekta kao zaposlenog može da se sastoji od broja zaposlenog kao identifikatora, službene legitimacije kao kredencijala, naziv posla, zaposlenja i službene lokacije kao atributa.

Identitet ima statičke, biološke, dinamične, društvene i psihološke komponente. Može biti kategorizovan na mnogo načina iz različitih perspektiva jer diskusije o identitetu obuhvataju širok spektar disciplina uključujući sociološku, psihološku, filozofsku kao i kompjutersku nauku. Prema tome, identitet dopušta multidisciplinaran pristup u procesu razmatranja samog pojma definicije. Definisanje pojma identiteta obično se dovodi u vezu sa definisanjem koncepta tradicionalnog pojma identiteta tj. ljudskog ili humanog identiteta sa različitim pogledima od javnog do privatnog. Naizgled definisanje pojma identiteta se čini veoma jednostavnim ali suštinski je veoma kompleksno pitanje. U literaturi postoji mnogo definicija u pogledu definisanja ovog pojma, pri čemu je u ovom radu prihvaćena defnicija koju je dao Windley [24] *"identitet je kolekcija podataka koji reprezentuju atribute, preferencije i osobine"*.

U kontekstu e-poslovanja, identitet predstavlja odliku moderne trgovine koji se rutinski zahtijeva u procesu transakcije. Brzi tehnološki razvoj implicira pitanja poput kakav je nečiji identitet u transakcionom kontekstu, konkretno šta ga čini i kako funkcioniše, koja je njegova pravna priroda, i sl. Odgovori na ova pitanja ukazuju da identitet pored česte upotrebe veoma rijetko je definisan naspram njegove funkcije i pravne uloge koje nisu jedinstveno određene. Primjer navedenog je Australija u kojoj se identitet pominje u veoma širokom opsegu federalnih i državnih zakona ali veoma rijetko je definisan. Kada je i definisan, definicije su obično obojene prirodnim zakonom. Primjer je s4 *Equal Opportunity Act 1995 (Vic)* koji definiše *'gender identity'* [25]. Kako se identitet pominje u veoma širokom opsegu tako je prihvaćeno postojanje mnoštva različitih identiteta od kojih posebno izdvajamo kontekstualni i kompanijski ili organizacijski identitet. Primjera radi, organizacijski identitet je identitet koji je sa instaliranjem softverskog rješenja definiše svaku poziciju unutar organizacije tako da se radniku po zaposlenju dodijeljuje postojeći identitet i on dolazi na poziciju za koju su već unaprijed definisana pravila i procedure. Organizacijski identitet pripada organizaciji, a korisniku je samo privremeno ustupljen dok radi na toj poziciji. Takav kreiran identitet je strogo definisan sa pravilima i procedurama životnog ciklusa identiteta.

U kontekstu istraživanja u oblasti edukacije, pojam identiteta predstavlja skup informacija koji opisuju pojedinca u određenom *e-learning* okruženju. Identitet kao pojam u edukacionom okruženju je često korišćen u konceptu profesionalnih identiteta. Postoji mnogo koncepata u vezi profesionalnih identiteta i njegovog razvoja. U radu [26] Dehing *et al.,* su razmatrali termin profesionalnih identiteta kao dio kompleksnih višestrukih koncepata razvoja personalnih identiteta koji takođe obuhvataju termine razvoja inženjerskih identiteta. Prema Capobianco-u *et al.,* [14] profesionalni inženjerski identiteti su sastavljeni od četiri podfaktora: akademskih identiteta, školskih identiteta, radnih identiteta i inženjerskih aspiracija. Ovo ukazauje da profesionalni inženjerski identiteti predstavljaju širi podskup profesionalnih identiteta tj. personalnih identiteta. U tom kontekstu, veoma važno je primijetiti dva aspekta identiteta, subjektivni nešto što smo mi (činjenice o nama i našim fizičkim karakteristikama) i objektivni (društveni ili reputacija) nešto što drugi imaju o nama. Ukupni identitet je suma subjektivnih i objektivnih identiteta. Identitet može biti potpun (kompletan) i parcijalan (djelimičan). Kod potpunog identiteta ujedinjeni su sveukupni personalni atributi, dok parcijalni identiteti čine podskup atributa kompletnog identiteta. Upravo,

zbog tih činjenica, parcijalni identitet ima praktični značaj za razliku od potpunog identiteta koji ima teorijski značaj.

3.1.1.1. Parcijalni identitet

Prema Pfitzman-u i Hansen-u [27] parcijalni identitet je definisan kao "*podskup korisnih atributa od cjelokupnog identiteta pri čemu potpuni identitet ujedinuje sve korisne atribute od svih identiteta te osobe*". Pošto parcijalni identitet čini podskup atributa kompletnog identiteta pojedincu se ostavlja mogućnost upotrebe različitih parcijalnih identiteta u različitim situacijama. U principu, svaki identitet ima svoj potpuni identitet koji se sastoji od skupa parcijalnih identiteta, a koji mogu imati različite oblike u različitim kontekstima. Takođe, višestruki identiteti uključuju ogromnu količinu personalnih informacija u vezi sa pojedincem. Svi podskupovi identiteta predstavljaju korisnika ili njegove parcijalne djelove. Neki od ovih parcijalnih identiteta jedinstveno identifikuju korisnika dok drugi ne. Parcijalni identiteti se tokom vremena povećavaju, a veoma rijetko brišu, i kao takvi su daleko dugovječniji od samog korisnika. Brojni primjeri parcijalnih identiteta su rodni list, sportski, školski ili zdravstveni karton, i sl. Prema Hansen-u *et al.*, [28] postoje određeni parcijalni identiteti za koje se može reći da nikad ne prestaju čak i nakon smrti pojedinca jer se njegov parcijalni identitet može prenijeti na drugu osobu npr. broj socijalnog osiguranja. Značaj parcijalnih identiteta je u tome veći što niko nije u mogućnosti ili nema potrebu da sakupi sve informacije o identitetu pojedinca. Koncept parcijalnih identiteta odnosi se na bilo koji podskup atributa koji se odnose na nekog pojedinca. Parcijalni identiteti mogu biti imenovani ili neimenovani zavisno da li se to može odnositi na pojedinačni istinski identitet ili ne [29].

3.1.2. Digitalni identitet

Ubrzani razvoj digitalnih tehnologija je stvorio različite pogodnosti u pogledu razvoja mnogih e-poslova. Danas, broj digitalnih materijala eksponencijalno raste i sve više materijala biće pohranjeno kao digitalni resurs na *World Wide Web* [30]. Nesumnjivo, informacione tehnologije snažno podržavaju i sve više prožimaju u svakodnevnim e-poslovima, primjera radi u e-trgovini, e-vladi, i sl. U svakom od ovih područja prikupljaju se brojne informacije koje se pohranjuju u svrhu višestruke upotrebe. U tom pogledu, može se reći da digitalni identiteti imaju rastuću važnost u svakodnevnom e-

okruženju i kao takav zahtijeva odgovarajući pristup. U posljednje vrijeme digitalne identitete nazivaju e-identiteti [31]. Prema Danner-u i Hein-u [32] "*e-identiteti obezbijeđuju način sa kojim je moguće odobriti personalne identitete, ne zahtijevajući fizičko prisustvo i verifikaciju papira - zasnovanog na dokumentima identiteta*".

Različitosti koje su prisutne u definisanju pojma identiteta takođe su prisutne i u pojmu definisanja digitalnog identiteta. Međutim, u okviru ove teme prihvaćen je pojam definicije digitalnog identiteta koju su dali Bosworth *et al.,* [33] "*Digitalni identitet je oblik identiteta koji nastaje digitalnom kodifikacijom identifikatora na način koji je pogodan za obradu i analizu u kompjuterskim sistemima*". Jøsang *et al.,* [34] su posebno naglasili da digitalni identiteti predstavljaju nekog ko je angažovan u onlajn aktivnostima. Dakle, pojam digitalnog identiteta se odnosi na aspekt digitalne tehnologije. Prema Aresta-u *et al.,* [35] digitalni identiteti obuhvataju prisustvo, učenje i vještine koje su razvijene kroz njihov personalni, akademski i profesionalni način.

Sve navedeno jasno ukazuje da je digitalni identitet usko povezan sa profesionalnim identitetima u istraživanjima u oblasti edukacije. Praktično, danas u digitalnom svijetu je nemoguće koristiti računare bez dodjeljenih digitalnih identiteta. Dugo vremena digitalni identiteti su smatrani ekvivalent korisničkog identiteta stvarnog života koji ukazuju na neke naše osnovne atribute:

- Ko smo mi: ime, prezime, državljanstvo, rođenje, i sl.
- Bavimo li se sportom?
- Šta nam se dopada: Naša omiljena knjiga, sportski klub, auto, hrana, piće, i sl.
- Koja je naša reputacija: Da li smo pošteni ili nečasni, i sl?

Digitalni identitet kao koncept ima široku primjenjivost ne samo u poslovnom području već i na internetu. Tendencija ere interneta je usmjerena na kretanje društvenih, poslovnih, zabavnih i drugih aktivnosti iz fizičkog u virtualni svijet. Internet je postao novo i najvažnije mjesto u interakciji između ljudi i organizacija u kojem važe sopstvena pravila. Mnoštvo personalnih informacija se svakodnevno pohranjuje na internetu i dostupna su trećim licima. Sve aktivnosti i tragovi koji ostaju u digitalnom svijetu po kojima nas drugi mogu pronaći i pročitati, kao i sve ono što će misliti o nama čini naš digitalni identitet.

Digitalni identitet je dio sveobuhvatnog identiteta tj. govori se o informacijama o identitetu koje su prevedene u parcijalne dijelove. Informacije o identitetu potrebno je stvarati, održavati, pohranjivati i razmijenjivati preko elektronskih mreža. Sa digitalnim identitetima nastoji se graditi slika o ličnom i profesionalnom životu. Slika stvorena u virtualnom svijetu direktno je u vezi sa stvarnim svijetom. Digitalni identitet je takođe u neposrednoj vezi sa onlajn reputacijom. U profesionalnom kontekstu izuzetno je važna pozicija i ugled koju osoba ima na internetu, jer sa dobrim ugledom moguće je i ostvariti krajnji cilj onoga čime se bavi tj. materijalizacija. Ljudi preferiraju da koriste informacije o stvarnom identitetu kako bi povećali mogućnosti za uspjehom a time i potvrdili korisničke vještine sa kojima mogu steći određenu reputaciju u specifičnom području.

Definisanje pojma reputacione vrijednosti je posebno pitanje, koje je usmjereno na pojedinačnu korisničku reputaciju i sveukupnu vrijednost reputacije zasnovane na korisničkom ponašanju u sistemu. Pod onlajn reputacijom podrazumijeva se javno održiva socijalna procjena pojedinca na osnovu njegovog ponašanja na vebu. Međutim, poznato je da, opšta vrijednost reputacije pojedinačnog korisnika ne može jasno prezentovati njegovu stvarnu reputaciju [36]. Primjer za ovo je da korisnik može imati dobru reputaciju kao zanatlija ali ne kao ekspert za berzu. Stvaranje ugleda na internetu je mukotrpan i dugotrajan proces koji se veoma lako "*u treptaju oka*" može narušiti sa nekom nesmotrenom aktivnošću. Aktivnost može biti izvedena od strane samog korisnika ili od strane drugih lica. Kako bi se ublažile ili smanjile mogućnosti narušavanja ugleda korisnika, digitalni identiteti zahtijevaju odgovarajući nivo zaštite:

- slabu zaštitu, npr. forumi, blogovi, onlajn trgovine i sl. (PIN i lozinke),
- jaku zaštitu, npr. e-pasoš, kreditna kartica i sl. (PKI, token, biometrija).

Današnji evolutivni razvoji usmjereni su u pravcu novog istinskog digitalnog svijeta uvijek sa imlikacijama po čovjeka. Digitalni identitet izgleda kao proširena lična karta ili pasoš, sadržan gotovo od istih informacija. Međutim, mnogo je svakodnevnih praktičnih primjera koji dokazuju da nije uvijek obavezna povezanost između stvarnog životnog i digitalnog identiteta. Najjednostavniji primjer je e-trgovina, pri čemu je najbitnije poznavati digitalnu reputaciju trgovca kao i potvrdu kontrole nad njegovim digitalnim identitetom. Mnogo manje je važno poznavati njegov stvarni život, nacionalni identitet, i slično tome. Prema tome, osnovni problem u e-komunikaciji je određivanje identiteta našeg sagovornika i tačnosti njegovih zahtjeva.

3.1.2.1. Koncept povezanosti digitalnog identiteta

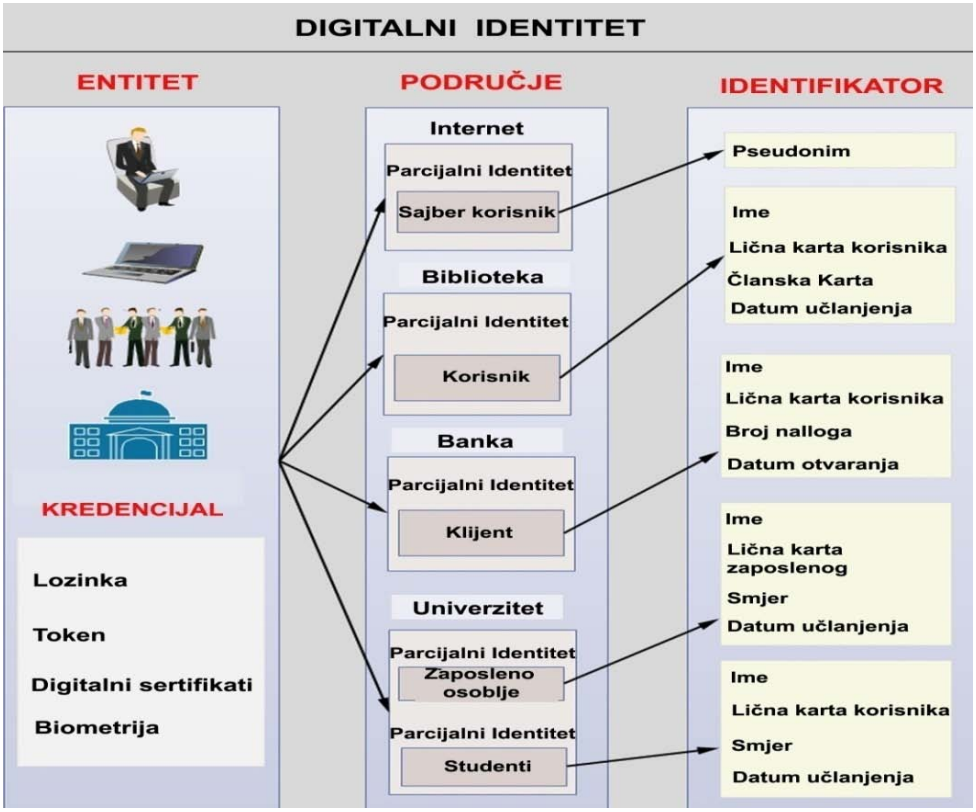
Digitalni identitet čini osnovu pomoću kojeg se entitet poziva prilikom pristupa resursima. Da bi povezao digitalne identitete sa entitetom (subjektom) posmatrač mora da vjeruje da se digitalno predstavljanje zaista odnosi na taj entitet. Sa druge strane, subjekat može posmatraču dati samo selektivni pristup svojim personalnim informacijama. Digitalni subjekat može biti pojedinac, grupa ljudi, organizacija, softverski program, hardverski uređaj ili neki drugi digitalni resurs. Digitalni identitet se sastoji iz skupa karakteristika odnosno atributa (identifikatora). Identifikatori su neophodni za identifikacione procese. Ovi identifikatori mogu imati različita svojstva kao što su privremena ili trajna, samoodabrana ili dodijeljena od strane administratora, i mogu biti pogodni za ljudsku ili samo za komjutersku interpretaciju.

Digitalni identitet karakteriše potencijalno neograničeni životni vijek, koji posjeduje konačan ali neograničen broj identifikacionih atributa. Entitet odnosno korisnik može imati višestruke digitalne identitete, pri čemu svaki digitalni identitet može posjedovati jedinstvene i nejedinstvene identifikatore unutar određenog područja. Područje digitalnog identiteta podrazumijeva područje u kojem je svaki digitalni identitet jedinstven. Razvoj digitalnih tehnologija u kojem su uspostavljeni specifični odnosi između identiteta odnosno korisnika kao i korisnika i tehnologija potencijalno mogu voditi prema problemima razumijevanja njihovih međusobnih odnosa što u krajnosti može rezultirati krađom identiteta.

Na osnovu svega gore navedenog, moguće je predstaviti osnovne elemente modela digitalnog identiteta:

- Entitet
- Područje
- Kredencijali
- Identifikatori

Osnovni elementi digitalnog identiteta kao i njihovi međusobni odnosi prikazani su na slici 3.



Slika 3. Osnovni elementi i odnosi elemenata digitalnog identiteta

3.1.3. Pregled modela digitalnog identiteta i prdruženih problema

U dostupnoj liteaturi, postoji mnogo radova koji se bave ekskluzivno sa digitalnim identitetima i njima pridruženim problemima. Problemi su holistički razmatrani kroz različite procese koji su pridruženi kroz životni ciklus digitalnih identiteta. Zavisno od autora postoje različiti modeli digitalnog identiteta čiji su životni ciklusi prezentovani u različitim oblicima – podijeljeni u nekoliko bazičnih faza. Primjera radi, prema Bosworth-u *et al.*, [33] životni ciklus digitalnog identiteta su podijelili na tri bazične faze (rođenje, život i smrt). Prema Elisi Bertino *et al.*, [37] životni ciklus digitalnog identiteta su podijelili na četiri bazične faze (stvaranje, upotreba, ažuriranje i opoziv), dok je Windley [15] životni ciklus digitalnog identiteta podijelio na pet bazičnih faza (stvaranje, širenje, upotreba, održavanje i ukidanje).

Međutim, sa druge strane postoji mnogo radova koji se bave pitanjima digitalnih identiteta i njegove arhitekture na apstraktnom nivou ili su oni tretirani u manje detalja unutar oblasti menadžmenta identiteta. Na primjer, u radu [38] Korać i Simić prezentuju savremeni pristup digitalnim identitetima u modelima menadžmenta identiteta. U radu [16] Gomi opisuje model životnog ciklusa za upravljanje identitetom informacija kroz

različita područja upotrebljavajući identitet prenosivih veza, dok u radu [39] Wang *et al.,* su se bavili personalnim prostornim podacima sistema upravljanja kao platformom za upravljanje personalnim podacima. U radu [40], Volonino *et al.,* su se bavili pitanjima kako upravljati životnim ciklusom elektronskih pohranjenih informacija. Takođe, u radu [41] Sabucedo *et al.,* su se bavili pitanjem kako upravljati personalnim informacijama od stanovnika i dokumentima koju oni posjeduju. Whitley *et al.,* [42] su se bavili identitetom informacija i identifikacijom kao odvojenim pitanjem u informacionim sistemima, dok Jøsang & Pope [43] i Koshutanski *et al.,* [44] istraživali modele menadžmenta identeta u kojem digitalni identiteti i povezani problemi su tretirani u manje detalja. Pfitzmann & Pfitzmann [45] su se bavili privatnošću i menadžmentom identiteta kroz život. Sullivan [46] je ispitivao prirodu i funkcije koncepta digitalnog identiteta.

Takođe, postoji mnogo radova kao što su [14, 47, 48] čiji je primarni fokus obuhvatao konstruisanje inženjerskih identiteta, tj. bavili su se sa konceptom formiranja identiteta u inženjeringu. U radu [49] Koole-u se bavio modelom *Web of Identity* (WoI) koji može da pojedinac upotrebi kao model svog identiteta i sa istim dešifruje druge identitete. Takođe, postoji više radova kao što su [50-53] koji su se bavili razvojem profesionalnih identiteta. Primjetno je da u svim prethodnim radovima, istraživački programi su jedinstveni u naglašavanju važnosti i uloge digitalnih identiteta. Takođe, može se primjetiti da su različiti autorski pristupi u predstavljanju i razmatranju životnog ciklusa digitalnih identiteta u suštini bave istim konceptima. Pored, različitih prezentacija životnog ciklusa digitalnih identiteta, u literaturi je prisutna određena konfuznost sistema menadžmenta identiteta koja je uslovljena pristupom načina opisa različitih modela. Isto tako, primjetna je nedovoljna interakcija učesnika u sistemu koja u krajnosti može rezultirati zloupotrebom digitalnih identiteta. U cilju potpunijeg razumijevanja digitalnih identiteta, smanjvanja i ublažavanja moguće zloupotrebe u narednoj podsekciji rada je dat prijedlog Edukacionog modela digitalnog identiteta – EMDI sa bazičnim modulima arhitekture.

3.1.4. Prijedlog EMDI

U ovom radu daje se prijedlog EMDI koji je nezavisan od konkretnih digitalnih tehnologija. Ovaj model bavi se sa reprezentovanjem identiteta u određenom edukacionom okruženju čija je implementacija data u obliku podmodela za filtriranje

neaktivnih digitalnih identiteta. Specifičnost EMDI je što ovaj model obezbijeđuje prezentaciju identiteta u virtuelnom kontekstu sa integrisanim pogledom i detaljnim opisom svih njegovih relavantnih karakteristika prezentovanih kroz njegove bazične module arhitekture. Virtuelni kontekst dopušta da model bude analiziran iz korisničke perspektive, tj. uloge entiteta, koji oblik identiteta se pojavljuje, i koja vrsta socijalne interakcije se dešava [54].

3.1.4.1. Bazični moduli arhitekture EMDI

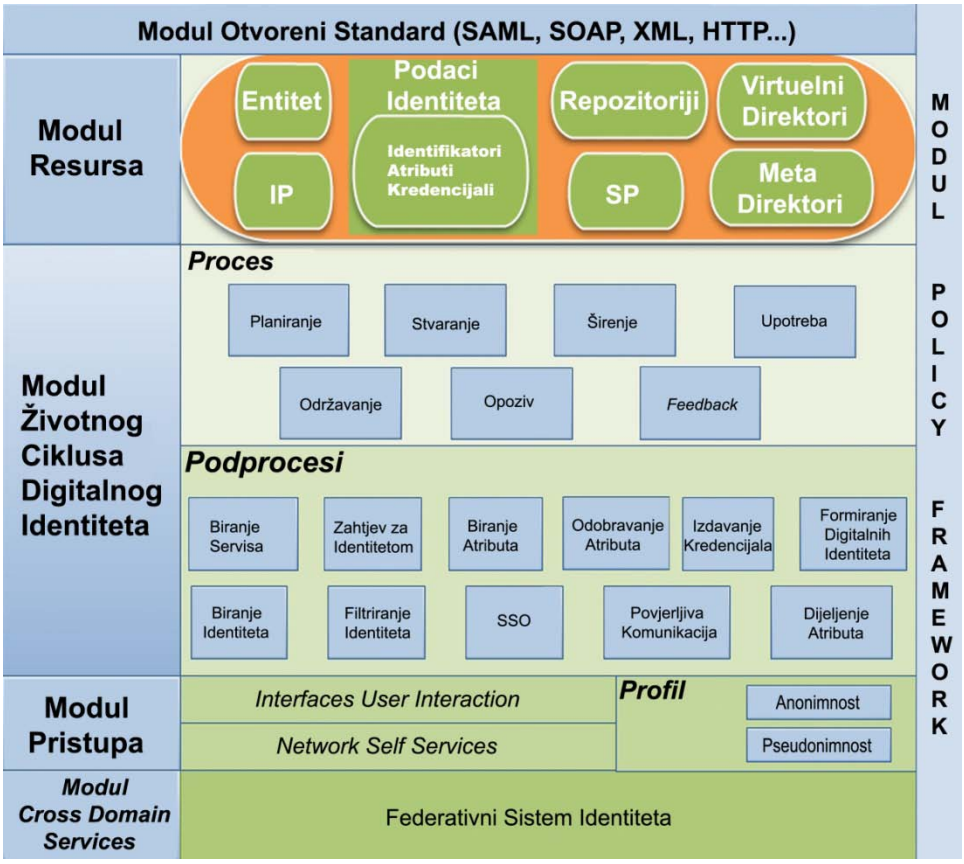
Arhitektura EMDI je prikazana na slici 4 pomoću bazičnih modula. Ova arhitektura obuhvata funkcionalne module korespondentne prema sistemima menadžmenta identiteta. Arhitektura predstavlja suštinsko obilježje EMDI prikazujući kompleksne izraze odnosa između učesnika u sistemu.

Bazične module arhitekture EMDI čine:

- *Modul Resursa,*
- *Modul Životnog cuklusa digitalnog identiteta,*
- *Modul Pristupa,*
- *Modul Cross Domain Services,*
- *Modul Policy Framework, i*
- *Modul Otvoreni standardi.*

Svaki modul sadrži bazičnu grupu komponenti odvojenu po njihovim funkcijama u EMDI. Ovi moduli su korišćeni kao obavezni u izgrađivanju blokova arhitekture EMDI. Centralni modul arhitekture EMDI koji ga izdvaja od svih drugih modela je životni ciklus digitalnog identiteta. Ovaj modul specifikuje obaveznu grupu procesa i podprocesa koji čine digitalni identitet bolje upravljivim u sistemima menadžmenta identiteta. Specifičnost ovog modula je proces planiranja i *feedback-a.* Modul životnog ciklusa je podržan od strane modula *Policy Framework* i *Open Standards.* Modul *Open Standard* je izgrađen na otvorenim standardima kao što su:

- *SAML – engl. Security Assertion Markup Language,*
- *SOAP - engl. Service Oriented Architecture Protocol,*
- *XML – engl. Extensible Language Markup,*
- *HTTP – engl. Hypertext Transfer Protocol, itd.*



Slika 4. Bazični moduli arhitekture EMDI

Važnost modula *Open Standard* u EMDI je u definisanju formata poruka između sistema učesnika, na primjer SAML standard (SAML *Response/Query*). Poseban značaj *Policy Framework* u EMDI je u tome što omogućava da se odrede dodatna pravila sa kojima se isključuje uticaj servis provajdera – SP-a u dijelu biranja identiteta. Modul resursa je modul koji služi da izgradi zaštitu zaštitnih servisa EMDI zasnovan na višim polugama (aplikativnim/veb servisima). Značaj i važnost ovog modula je da uspostavi kapacitete i ograničenja politika, odnosno modele povjerljivosti i privatnosti. Konačno, ovaj modul definiše elemente potrebne da se izgradi sistem federativnog identiteta. Moduli ovog resursa su Entiteti, SP-i, Identitet provajdera – IP-i, Podaci Identiteta, Repozitoriji, Virtuelne Direktoriji i Meta Direktoriji. Osim toga, ovaj modul omogućava da digitalni identitet bude otkriven od strane drugih učesnika. Modul pristupa može biti zasnovan na korisničkoj interakciji i interfejsu veb servisa. Korisnički profil pristupa može biti anoniman i pseudoniman. U modulu *Cross Domain Services* arhitekture EMDI predložen je Federativni Sistem Identiteta.

Kao što je označeno na slici 4, može se zaključiti da *User Interaction, Network Self Services interfaces, Profile (Anonymous or Pseudonymous), SAML, SOAP, XML i*

HTTP, mogu biti razmatrani kao dopunski moduli u arhitekturi EMDI. Iz tog razloga, u ovom radu savremeni pristup u izgradnji arhitekture EMDI ima holistički pristup koji je razmatran kroz pojedinačne determinante kao što su procesi i podprocesi. Procesi i podprocesi predstavljaju značajan izazov prema modelima menadžmenta identiteta koji pomažu da se definišu svi problemi po fazama tako da se oni mogu holistički rješavati a ne odvojeno. Kao što je gore pomenuto, ovi procesi i podprocesi su integrisani u modul životnog ciklusa digitalnog identiteta. Sljedeća sekcija rada detaljnije opisuje ovaj modul.

3.2. Životni ciklus identiteta

Naučnici koriste životni ciklus da povežu naizgled nepovezivo, a u ovom slučaju za analiziranje informacija tehnoloških problema [15]. Primjenjivost životnog ciklusa identiteta je izuzetno široka, bez obzira da li se radi o složenom sistemu (za velike poslovne subjekte) ili prostom sistemu (nalog na kućnom računaru). Shvatiti ulogu životnog ciklusa identiteta u parcijalnom sistemu i sistemu u cjelini je ključni za stvaranje strategije menadžmenta identiteta. Posebno je bitno naglasiti, da se menadžment identiteta bavi svim aspektima identiteta od stvaranja do ukidanja ukazujući time da to nije samo mjera o korisničkoj funkcionalnosti kao što je jednostruki upis i dijeljenje atributa.

Kako je prethodno navedeno, zavisno od autora životni ciklus digitalnog identita je prezentovan u različitim oblicima odnosno podijeljeni u nekoliko osnovnih faza. U takvim pristupima, primjetno je da su u životnom ciklusu digitalnog identiteta svi procesi odvojeno predstavljeni tj. ne postoji proces koji bi izvršio uzajamnu konekciju svih tih procesa. Zbog nemogućnosti povezivanja procesa pojavljuje se smanjena interakcija učesnika u sistemu. Nesumnjivo, nedovoljna interakcija učesnika u sistemu može ultimativno voditi ka konfliktima između aktivnih i neaktivnih digitalnih identiteta kao i zloupotrebi digitalnih identiteta. Konflikt između aktivnih i neaktivnih digitalnih identiteta podrazumijeva da od strane jednog korisnika postoji više digitalninih identiteta unutar istog sistema od kojih je najmanje jedan neaktivan. Zloupotreba se prvenstveno ogleda u mogućnosti kopiranja, modfikovanja ili krađe kredencijala što može da vodi ka potpunoj ili djelimičnoj krađi identiteta. U cilju

savladavanja svih navedenih izazova koji se javljaju u životnom ciklusu digitalnog identiteta, životni ciklus EMDI je dat u ovom radu.

3.2.1. Životni ciklus EMDI

Životni ciklus EMDI opisuje procese digitalnog identiteta (slika 5). Radi se o dinamičnom, kompleksnom, neprekidnom i kontinuiranom ciklusu. Grafički posmatrano, procesi EMDI predstavljaju cikličnu stazu koja se sastoji od ponavljanja čvorova odnosno osnovnih procesa. Razumijevanje osnovnih procesa je suštinsko za razumijevanje EMDI. Proces je skup jednog ili više podprocesa. Podproces je skup jedne ili više aktivnosti. Aktivnost je generički pojam za izvršenje bilo kog koraka u procesu. Za izvršenje procesa potrebni su određeni resursi i određeno vrijeme. Za razliku od drugih modela EMDI uvodi procese kao što su planiranje i povratna informacija *(feedback)* koji povezuju sve procese u sopstvenom životnom ciklusu.

Slika 5. Životni ciklus EMDI

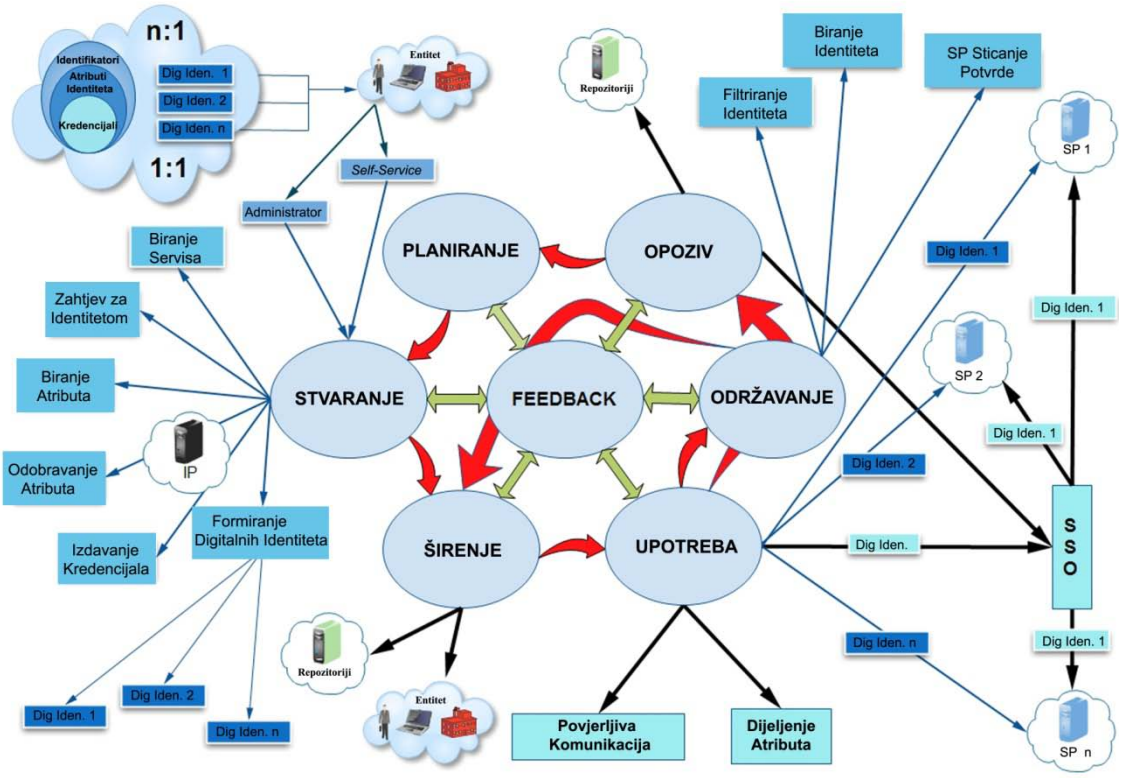
Osnovni procesi u životnom ciklusu EMDI su:

- Planiranje,
- Stvaranje,
- Širenje,
- Upotreba,
- Održavanje (ažuriranje),
- Opoziv, i
- *Feedback (povratna informacija).*

Pored procesa EMDI obuhvata i podprocese koji imaju za cilj da omoguće pružanje boljih usluga. Podprocesi EMDI su:

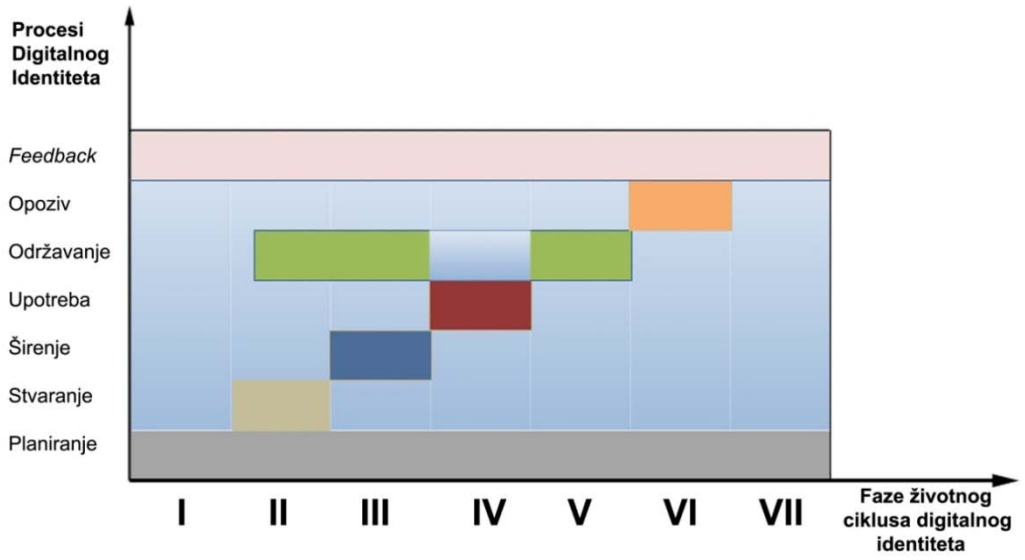
- Biranje Identiteta,
- Zahtjev za Identitetom,
- Biranje Atributa,
- Odobravanje Atributa,
- Izdavanje Kedencijala,
- Formiranje Digitalnog Identiteta,
- Biranje Identiteta,
- Filtriranje Identiteta,
- SSO,
- Povjerljiva Komunikacija,
- Dijeljenje Atributa.

U cilju potpunijeg sagledavanja svih procesa i podprocesa EMDI, njihov šematski prikaz je dat na slici 6.



Slika 6. Šematski prikaz procesa i podprocesa u životnom ciklusu EMDI.

U ovom radu, grafička prezentacija prisustva procesa EMDI u fazama životnog ciklusa digitalnog identiteta je data na slici 7. Kao što se može vidjeti na slici 7, procesi u životnom ciklusu EMDI imaju različitu prisutnost u fazama. Procesi planiranja i povratne informacije su prisutni u cjelokupnom životnom ciklusu EMDI. Proces održavanja je prisutan kroz tri faze životnog ciklusa EMDI u kome posebnu specifičnost čini njegovo "*zadiranje*" u fazu II. Ostali procesi su prisutni u domenu jedne faze. Proučavanje EMDI zahtijeva sagledavanje u detalje svakog od procesa koji čine životni ciklus digitalnog identiteta.



Slika 7. Grafička prezentacija prisustva procesa EMDI u fazama životnog ciklusa digitalnog identiteta.

3.2.1.1. Planiranje

U ovoj sekciji rada, uvedeni proces planiranja predstavlja prvi i osnovni proces odnosno polazno mjesto u životnom ciklusu EMDI. Radi se o kompleksnom, dinamičnom i predviđajućem procesu u kojem se definiše okvir za cjelokupan sistem funkcionisanja digitalnog identiteta. Značaj i važnost ovog procesa je u tome što su svi drugi procesi povezani sa ovim procesom. Uzimajući u obzir da se radi o predviđajućem procesu samim tim ovaj proces je povezan sa rizikom i neizvjesnošću. Stoga, može se zaključiti da se radi o kritičnom procesu jer praznine u ovom procesu direktno se reflektuju na sve druge procese.

Proces planiranja je mjesto gdje se prepoznaje korisnička potreba za digitalnim identitetom. Planovima se dolazi do poznatih ili predvidljivih korisničkih zahtjeva. Planiranje ne može biti urađeno samo na apstraktnom nivou već se mora proširiti na sve nivoe i sve dijelove sistema. Proces planiranja treba da bude fleksibilan i podložan uticajima odnosno spreman da po potrebi mijenja definisane ciljeve i mjere. Proces planiranja za svaku fazu EMDI je suštinski za izgradnju njegove arhitekture. Osnovni elementi ovog procesa su problemi, ciljevi i resursi. Planiranje se sprovodi kroz planove koji određuju politike i procedure tj. zadatke i sredstva za izvršavanje tih zadataka po vremenu i mjestu. Sa ovim procesom planiranja obezbjeđuju se uslovi potrebni za efektivniju i efikasniju upotrebu tehnologija. Na osnovu planiranja donose se odluke za upravljanje svih ostalih procesa i podprocesa kao što je izbor servisa, izbor atributa, i sl. U procesu planiranja u prvi plan posmatranja stavljaju se atributi identiteta koji istovremeno predstavljaju i ulazne elemente procesa u stvaranja digitalnog identiteta.

3.2.1.2. Stvaranje

Proces stvaranja je veoma složen i izazovan proces. Složenost se odnosi na automatizaciju svih procesa i podprocesa, dok izazovnost se ogleda u aktiviranju potpuno novog skupa pitanja koji zahtijevaju novu metodologiju. Posmatrano iz perspektive korisnika, proces stvaranja digitalnog identiteta predstavlja stvaranje zapisa o korisniku sa tačnim atributima. Prema tome, prikupljanje i registracija atributa identiteta organizovana je radi korisnika. Proces stvaranja identiteta dešava se kao posljedica korisničkih aktivnosti koje mogu biti urađene kroz aktivnosti administratora ili kao samoposlužujući servis. Njihova upotreba može biti zasnovana na višestrukim sistemima.

Dakle, entitet može kreirati višestruke digitalne identitete (n:1), pri čemu svaki digitalni identitet može posjedovati jedinstvene i nejedinstvene identifikatore unutar određenog područja. Neophodno je posebno istaći, da u procesu stvaranja identiteta broj upotrebljenih atributa treba da bude minimalan ali dovoljan da izvrši korisničku autentifikaciju. Sa minimiziranjem podataka odnosno atributa smanjuje se mogućnost krađe personalnih informacija kao djelimične ili potpune krađe identiteta. Takođe, prema [29] minimiziranje podataka predstavlja jedan od ključnih principa u zaštiti privatnosti. U radu [55] Paci *et al.,* su predložili pristup za kontrolisano oslobađanje atributa identiteta podržavajući selektivno i inkrementalno otkrivanje kredencijala.

Prema Elisi Bertino [37] proces stvaranja identiteta sastoji se iz tri podprocesa potvrđivanja i izdavanja atributa i formiranja identiteta. U odnosu na model Elise Bertino, proces stvaranja digitalnog identiteta u modelu EMDI je proširen sa tri nova podprocesa: biranje servisa, zahtjev za identitetom i izbor atributa. U procesu stvaranja EMDI postoje brojni rizici koji mogu ugroziti integritet korisnika. Rizik se ogleda u mogućnostima napadača da izvrši nelegalne aktivnosti u vidu kopiranja, krađe ili modifikovanja kredencijala. Kompromitovanjem kredencijala nečasni pojedinci mogu zloupotrebiti korisnika u smislu sticanja zaštićenih informacija i time steći puni pristup resursima. Često, krajnji cilj napadača je sticanje nezakonitog profita, tj. materijalizacija.

Primjer zloupotrebe identiteta je falsifikovanje pasoša, identifikacionih dokumenata, kreditne kartice, i sl. Sa druge strane, izazov za sisteme je da u svom funkcionisanju smanje ili ublaže navedene rizike. Rizici od ovakvih zloupotreba mogu imati ozbiljne posljedice poznavajući da kredencijali mogu biti korišćeni da se odredi pristupni nivo npr. zasnovan na grupnom članstvu (uloge u šemama *role based access control (RBAC)* ili mogući bilo koji drugi atribut u šemama *attribute-based access control (ABAC))* [56]. Stoga, zaključak je da su kredencijali u procesu stvaranja EMDI u svim svojim podprocesima ranjivi i kao takvi treba da budu zaštićeni od moguće zloupotrebe.

3.2.1.3. Širenje

Da bi se stvoreni digitalni identitet stavio u funkciju neophodno je izvršiti njegovo širenje ili distribuciju. Proces širenje u EMDI se obavlja prema entitetu i repozitoriju, najčešće putem mejla, e-mejla ili veb servisa. Zavisno od prirode sistema na kojem je identitet stvoren, zapisi digitalnog identiteta mogu zahtijevati distribuciju i do drugih sistema. Za jednostavne sisteme, širenje je jednostavno jer EMDI je stvoren i korišćen unutar jednog područja, a pohranjuje se na sistemskom fajlu ili u lokalnoj bazi podataka. Za kompleksnije sisteme može se obezbijediti neka vrsta dijeljenja direktorija, virtualnih ili meta direktorija gdje su identiteti stvoreni na jednom mjestu a korišćeni na višestrukim sistemima. Takođe, posredstvom virtualnih i meta direktorija omogućava se povezivanje sistema višestrukih direktorija. Pomoću ovih direktorija u EMDI se rješava ažuriranje digitalnih identiteta kada se isti identifikator koristi kod više SP-a. Na taj način se omogućava sinhronizacija sa postojećim atributima kako bi se

izbjegli mogući konflikti. Rizici koji se pojavljuju u fazi stvaranja EMDI se prožimaju i tokom ove faze. Ključni rizik u ovom procesu je usmjeren prema komunikacionim kanalima kojima se vrši proces distribucije. Prijedlog smanjenja ili ublažavanja takvog rizika moguće je postići upotrebom tehnika šifrovanja, dešifrovanja i steganografije.

3.2.1.4. Upotreba

Ova faza nastupa nakon stvaranja i distribucije digitalnog identiteta gdje se isti stavlja na raspolaganje korisniku. Kako su digitalni identiteti pridruženi sa procesima identifikacije, autentifikacije i autorizacije, proces upotrebe se može jednostavno posmatrati kao konsultovanje korisničkog digitalnog identiteta u tim procesima prema resursima. Stvoreni digitalni identitet upotrebljava se u različitim servisima unutar jednog ili više područja. Sa upotrebom digitalnih identiteta omogućava se višestruko poboljšanje servisa. Međutim, potrebno je istaći da digitalni identiteti treba da budu korišćeni na način koji smanjuje mogućnost zloupotrebe a korisniku pruža sigurnost i zaštitu privatnosti, te olakšava pristup zahtjevanom resursu.

Rizici u ovoj fazi se pojavljuju u vidu zloupotrebe digitalnih identiteta koji pored materijalizacije napadača, na najdirektniji način narušavaju korisničku privatnost i povjerenje, dok u slučaju otkrivanja internih kompanijskih informacija narušavaju kompanijski brend i ugled. Zloupotreba digitalnih identiteta ogleda se u korišćenju prava i privilegija od strane nečasnih pojedinaca koja inače pripadaju stvarnom korisniku identiteta. Svi rizici koji su identifikovani u prethodnim fazama takođe se prožimaju i kulminiraju u fazi upotrebe digitalnog identiteta.

Mnogo je načina zloupotrebe digitalnih identiteta, a prije svega to je upotreba raznih metoda i tehnika kao što su presretanje mrežnog saobraćaja, krađe lozinki fajlova, socijalni inženjering, skeniranja portova, prisluškivanja, snifovanja, fišinga i drugih napada. Da bi se smanjili ili ublažili rizici koji se pojavljuju u ovoj fazi, pored primjene tehnika šifrovanja i steganografije, neophodno je da bude uveden podproces SSO. Prema Elisi Bertino *et al.,* [37] najčešće korišćeni podprocesi (koji su prihvaćeni i u ovom radu) od strane servis identiteta su SSO, pouzdana komunikacija i dijeljenje atributa. SSO je veoma važan režim rada sistema menadžmenta identiteta čija je detaljna analiza opisana u narednom poglavlju rada.

3.2.1.5. Održavanje

Ova faza nastupa nakon upotrebe digitalnog identiteta odnosno kada postoji potrebe za njegovom reupotrebom. Važnost ovog procesa ogleda se u činjenicama da su mnogi kredencijali dinamični i promijenjivi tokom vremena, i da zaposleni mogu imati različit status unutar iste organizacije. Upravo u tim činjenicama leži izazov ovog procesa, kako i na koji način se nositi sa rizicima od mogućeg kopiranja, krađe ili modifikovanja kredencijala. Da bi se smanjili ili ublažili rizici povezani sa ovim procesom neophodno je da se uvedu dobre politike i procedure od strane menadžmenta identiteta. To podrazumijeva da je kvalitet procesa ažuriranja korisničkog profila direktno zavisan od IT-og odjeljenja. Nesumnjivo da čovjek predstavlja odlučujući faktor u životnom ciklusu EMDI. Međutim, u slučaju procesa ažuriranja pored čovjeka značajnu ulogu ima i tehnologija.

Dakle, ovaj proces ima za cilj stvaranje uslova za potrebe efektivnijeg i efikasnijeg rada. Pored pomenutih politika i procedura, u procesu ažuriranja digitalnog identiteta, životni ciklus EMDI obuhvata i tri podprocesa:

- *Filtriranja identiteta* je podproces koji omogućava kombinovanje podataka o uređajima i identitetima sa procedurama. Sa ovim podprocesom omogućava se klasifikovanje digitalnih identiteta u aktivne (upotrebljive) i neaktivne (neupotrebljive). Aktivni identiteti mogu biti klasifikovani kao direktni i indirektni. Direktni identiteti mogu biti upotrebljeni na uređaju za autentifikacione svrhe bez interakcije sa drugim uređajem, dok indirektni su isključivo zavisni od drugih uređaja.

- *Biranje identiteta* je podproces u kojem korisnik bira digitalni identitet iz prethodno klasifikovane liste. Ovaj podproces stvara preduslov da entitet koji sadrži više digitalnih identiteta (1:n) ima mogućnost slobodnog izbora.

- *Sticanjem potvrde od servis provajdera* je podproces kojim se potvrđuje da je izvršen proces ažuriranja odnosno digitalni identitet je stavljen korisniku na raspolaganje za upotrebu.

Ovaj proces djeluje korektivno u smislu praćenje validnosti kreiranog digitalnog identiteta, njihovih mogućih promjena u vidu podešavanja ili eventualnog stvaranja dodatnih. Može nastupiti od strane bilo kog učesnika u sistemu. Proces ažuriranja nema vremenskog ograničenja u smislu upotrebe, on je aktivan dok god postoji potreba za njim. Međutim, da bi identitet bio aktivan potrebno je njegovo redovno ažuriranje. Proces ažuriranja je neophodan za održavanje integriteta kredencijala, a uslovljen je karakteristikama kredencijala i različitim pravima i privilegijama koje korisnici mogu imati unutar organizacije. Uslovi koji aktiviraju ovaj proces mogu biti različiti kao što je vremensko ograničenje kredencijala (kredencijali u obliku digitalnih sertifikata ili lozinki), kredencijali mogu biti stvoreni u kasnijoj fazi, promjena mjesta prebivališta, i sl. Takođe, primjer promjene kredencijala koje mogu biti uzrokovane zbog osnovnog svojstva korisnika su zdravstveno stanje, suspenzija, gubljenja ili zaboravljanja lozinki sistema i promjene uloge u sistemu ili napuštanje organizacije.

Osim toga, podržavanje nove poslovne politike može usloviti odgovarajuću modifikaciju baze podataka sa dodavanjem novih polja ili izmjenom kompletnog sistema. Neophodno je naglasiti, da u EMDI proces ažuriranja pored "*zadiranja*" u proces stvaranja treba da dosljedno prati proces širenja, u suprotnom takvi digitalni identiteti su neupotrebljivi. U jednostavnim sistemima, postoje digitalni identiteti koji ne zahtijevaju proces održavanja, uglavnom se radi o digitalnim identitetima koji imaju kraći životni vijek postojanja odnosno nisu u funkciji reupotrebe. Inače, ovaj proces za organizacije predstavlja skupu investiciju.

3.2.1.6. Opoziv

Ova faza nastupa nakon upotrebe digitalnog identiteta za kojim osnovano ne postoji potreba za daljnom upotrebom ili u slučajevima njegovog kompromitovanja. Proces opoziva predstavlja opoziv kredencijala tj. ukidanja digitalnog identiteta. U ovoj fazi EMDI dolazi do potpunog uklanjanja digitalnog identiteta iz sistema kao i repozitorija. Ova faza zahtijeva posebnu pažnju jer proces gašenje predstavlja izazovan proces. Ovaj proces je jednako važan kao i sam proces stvaranja digitalnog identiteta. Posebna važnost procesa opoziva u EMDI je u obezbijeđivanju punovažnosti procesa autentifikacije i autorizacije. Rizici ovog procesa se javljaju u vidu neaktivnih digitalnih identiteta koji mogu dovesti do konfuzije, prevare ili krađe identiteta. Neaktivni digitalni identiteti predstavljaju vrata za neovlašćen hakerski pristup informacijama. U

suštini, oni čine zapostavljena ili napuštena mjesta tj. "*džepove*" u sistemu koji stvaraju pogodna i realna hakerska mjesta za razbijanje sistema. Takvi formirani "*džepovi*" u sistemu najčešće nisu nadgledani i neće skretati pažnju na sebe što hakerima ostavlja dovoljno prostora za manipulisanje.

Rizici u ovom procesu mogu nastupiti u slučajevima kada pojedinac napušta organizaciju, ako su kredencijali ukradeni, kompromitovani ili istekli (zastarijeli i/ili nevažeći). U cilju smanjivanja ili ublažavanja ranjivosti ovog procesa potrebno je da proces ukidanja bude pravovremeno sproveden u cijelom sistemu. Može se sprovoditi ručno i automatski. U principu, proces opoziva ne bi trebalo sprovoditi ručno jer se na taj način i mogu stvoriti opasni "*džepovi*". Proces ukidanja identiteta treba prepustiti specijalizovanim softverima i automatizovanim procedurama zasnovanim na tehničkim standardima. Primjer takvog standarda je *Online Certificate Status Protocol* (OCSP) [57].

3.2.1.7. Feedback

Povratna informacija je važan proces u životnom ciklusu EMDI. Povratna informacija kao i planiranje u EMDI obuhvata sve procese. Svi procesi su međusobno povezani putem povratne informacije. Način na koji se obezbjeđuje komunikacija sa drugim procesima je zasnovana na SAML standardu (SAML *Response/Query*). Ova faza se odvija u kontinuitetu, interaktivno između svih učesnika u sistemu, u vidu zahtjeva ili odgovora. Na taj način se ovaj proces prožima kroz cijeli informacioni tok omogućavajući da se u posmatranom trenutku vremena izvrši uvid u trenutni status digitalnog identiteta.

Feedback predstavlja važno obilježje životnog ciklusa digitalnog identiteta, što znači da dodjeljuje zadatke učesnicima u sistemu i prati njihovu realizaciju. Na primjer, korisnik u procesu registracije u komunikaciji sa SP-om obavezan je da kroz iterativne korake ispuni odgovarajuća pitanja. U slučaju pogrešnog popunjavanja pitanja, korisnik će biti primoran da izvrši pravilno ispunjenje svih pitanja kako bi pristupio resursu. Značaj i uloga povratne infomacije je višestruka:

- Za učesnike u sistemu ona predstavlja nezaobilazan alat u smislu interakcije korisnik – sistem. Prožima se kroz sve procese digitalnog identiteta djelujući

korektivno u vidu pravovremene modifikacije ili kontrole svih procesa. Na taj način se kroz analizu zahtjevanih i dobijenih rezultata unaprijeđuje razvoj organizacionih aktivnosti s ciljem boljeg opsluživanja korisnika. Dakle, povratna informacija predstavlja veoma važan korektivni faktor jer po potrebi utiče na proces planiranja.

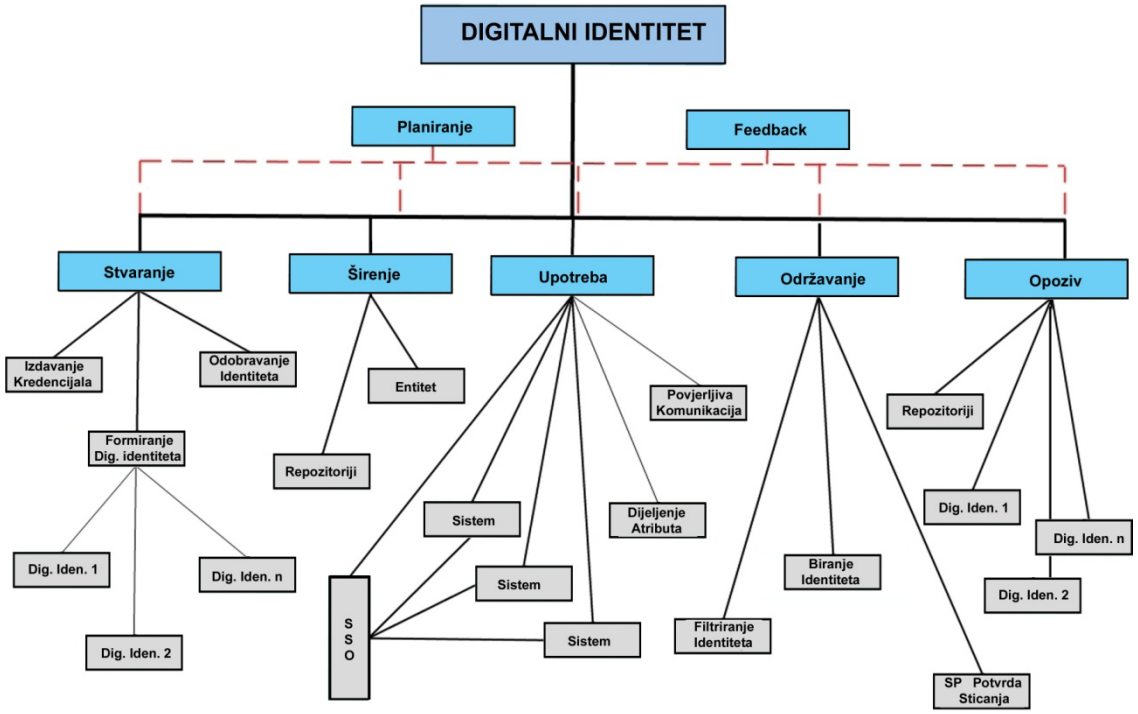
- Povratna informacija se može koristiti za identifikovanja praznina (nedostataka) tokom egzistiranja digitalnog identiteta. Na taj način direktno doprinosi poboljšanju učinkovitosti procesa održavanja.

- Sa povratnom informacijom unaprijeđuje se pravovremena korisnička aktivnost kao i povratna sesija. U tom kontekstu, EMDI zapravo generišu zahtjeve kroz iterativne procese. Kroz povratnu informaciju korisnik dobija kontinuiranu informaciju o izboru, prihvatanju kredencijala, njihovoj upotrebi, vremenskom trajanju poput PIN lozinke, digitalnih sertifikata, i sl., kao i postupanja u vezi sa sljedećim koracima poput informisanja u slučajevima suspenzije, promjene uloge u sistemu ili ukidanja korisničkog naloga.

- Konačno, sa ovim procesom nadgledaju se svi procesi u sistemu i posvećuje se više pažnje za mjesta (izolovana mjesta) koja bi mogla biti zloupotrebljena od strane hakera.

3.2.2. Hijararhijski dijagram procesa u životnom ciklusu EMDI

Hijararhijski dijagram procesa u životnom ciklusu EMDI je dat na slici 8. Za izgradnju dijagram procesa u životnom ciklusu EMDI neophodno je postići slaganje strukturnih dimenzija sa relevantnim parametrima kao što su procesi i podprocesi. Sa slike 8 je vidljivo da proces planiranje i *feedback-a* se prožimaju kroz sve procese. Dijagram procesa u životnom ciklusu EMDI veoma pregledno daje procese i podprocese kao i njihovu hijararhiju. Značaj procesne hijararhije je suštinski za složene procese u životnom ciklusu EMDI. Međutim, kako je prethodno navedeno sam dijagram procesa hijerarhije u životnom ciklusu digitalnog identiteta kao specifično obilježje EMDI ne može biti partikularno posmatran ili razmatran kao EMDI. Dakle, u ovom posmatranom modelu dijagram procesa hijerarhije isključivo ima komplementarni karakter u smislu boljeg razumijevanja procesa i podprocesa.

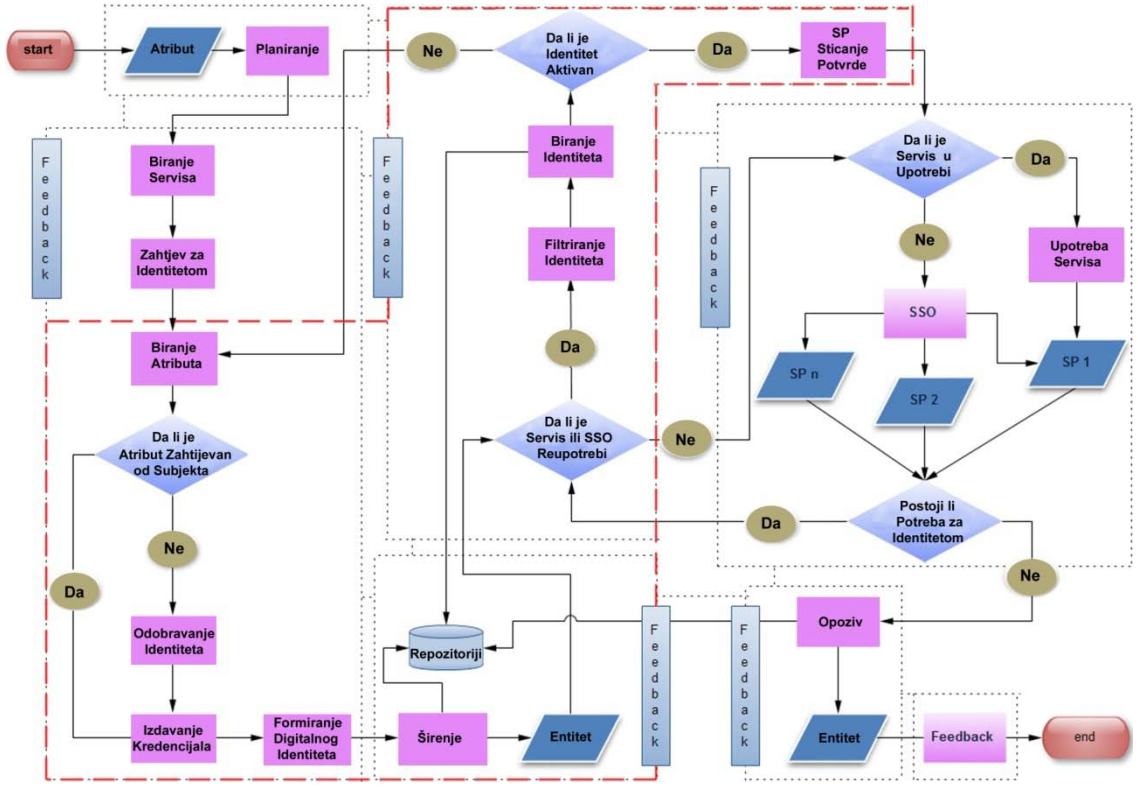


Slika. 8. Hijararhijski dijagram procesa u životnom ciklusu EMDI.

3.2.3. Dijagram toka podataka EMDI

Da bi se potpunije razumijeli procesi EMDI, dijagram toka podataka EMDI je dat na slici 9. Započinje sa procesom planiranja pri čemu atributi predstavljaju ulaz. Nakon procesa planiranja, slijedi korisničkim izbor željenog servisa. Da bi korisnik pristupio odabranom servisu neophodno je da podnese zahtjev za dobijanje digitalnog identiteta. Za realizaciju tog podprocesa potrebno je izabrati atribute. Pri izboru atributa vrši se sinhronizacija sa postojećim atributima da bi se izbjegli mogući konflikti. Ukoliko atributi nisu zahtijevani od subjekta prije izdavanja kredencijala potrebno je njihovo potvrđivanje koje često i zahtijeva određenu provjeru subjekta. Nakon tih podprocesa slijedi formiranje digitalnog identiteta koji se procesom širenja prenosi do korisnika i repozitorija. Ovaj podproces može uključivati aktivnosti koje podrazumijevaju "*oživljavanje*" identiteta (samo u slučajevima kada je proces ažuriranja aktiviran). Nakon završenog procesa prosleđivanja digitalni identitet je spreman za upotrebu. Ako se u EMDI proces upotrebe nije zasnovan na jednom sistemu tada se koristi podproces SSO sa kojim se omogućava višestruka upotreba sistema. Međutim, ukoliko ne postoji potreba za reupotrebom identiteta slijedi proces opoziva. U tom slučaju životni ciklus digitalnog identiteta je najkraći i ne zahtijeva primjenu procesa ažuriranja. U suprotnom, ako postoji potreba za njegovom reupotrebom u jednom sistemu ili u SSO okruženju, korisniku se daje mogućnost izbora identiteta odnosno korišćenje istog ili

drugog identiteta u iste svrhe. Za sprovođenje takvih aktivnosti potrebno je izvršiti filtriranje i odabir digitalnog identiteta. U suprotnom, ako postoji potreba za njegovom reupotrebom u jednom sistemu ili u SSO okruženju, korisniku se daje mogućnost izbora identiteta odnosno korišćenje istog ili drugog identiteta u iste svrhe.



Slika 9. Dijagram toka podataka digitalnog identiteta

Za sprovođenje takvih aktivnosti potrebno je izvršiti filtriranje i odabir identiteta. Po izboru digitalnog identiteta neophodno je izvršiti provjeru njegove aktivnosti. U suprotnom, ako postoji potreba za njegovom reupotrebom u jednom sistemu ili u SSO okruženju, korisniku se daje mogućnost izbora identiteta odnosno korišćenje istog ili drugog identiteta u iste svrhe. Za sprovođenje takvih aktivnosti potrebno je izvršiti filtriranje i odabir identiteta. Po izboru digitalnog identiteta neophodno je izvršiti provjeru njegove aktivnosti. Ukoliko je digitalni identitet aktivan tada slijedi sticanje potvrde o aktivnosti istog od strane SP-a, u suprotnom potrebno je ponovo izvršiti izbor biranja atributa i ponoviti određene podprocese koji se dešavaju i kod registracije novog digitalnog identiteta. Sa aktiviranjem identiteta obavezno slijedi njegova ponovna distribucija do korisnika i repozitorija. Nakon toga, digitalni identitet je spreman za njegovu reupotrebu. Nadalje, ako ne postoji više potreba za istim slijedi proces opoziva koji treba da se obavi u cjelokupnom sistemu uključujući i repozitorije. Međutim, ako postoji potreba za ponovnu upotrebu istog identiteta ili odabira drugog digitalnog

identiteta za iste svrhe neophodno je ponoviti cijeli ciklus. Broj ponavljanja ciklusa je neograničen ali konačan. Konačnost se ogleda u procesu opoziva koji je obavezan za sve digitalne identitete za koje osnovano ne postoji potreba daljnje upotrebe. Radni tok EMDI se završava sa procesom povratne informacije sa kojom se učesnici u sistemu informišu o gašenju digitalnog identiteta i o eventualnoj potrebi registrovanja novog digitalnog identiteta u slučaju kad se želi koristiti isti servis.

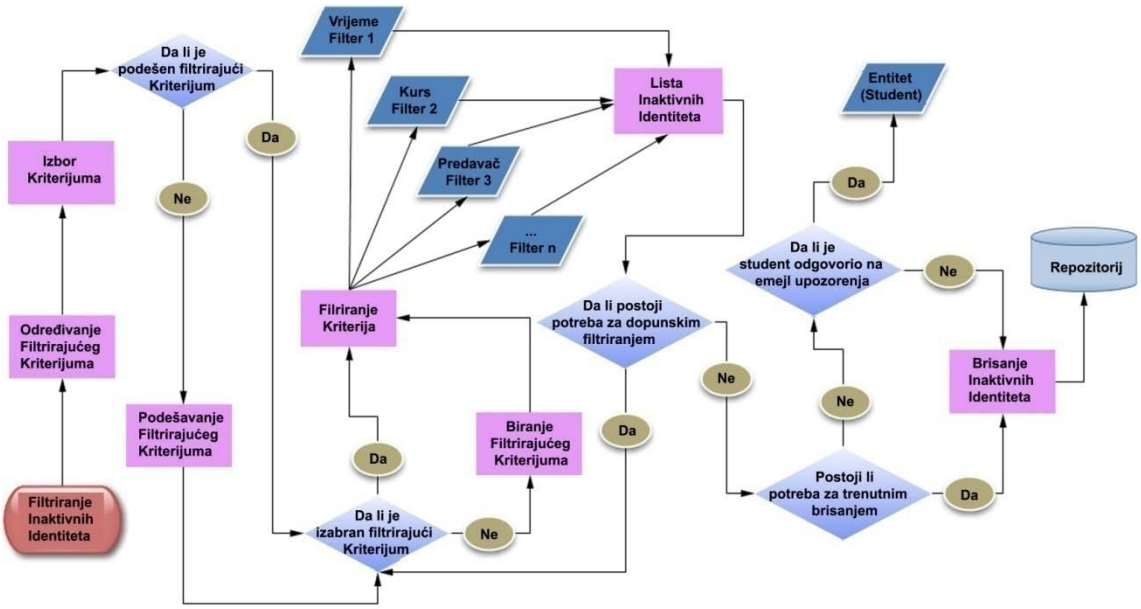
Kako proces održavanja takođe čini specifičnim ovaj model radi toga je u prilogu disertacije dat Algoritam 1. U kontekstu ovog istraživanja, uloga i važnost algoritma je da pokaže praktičnu izvodljivost datog algoritma.

3.2.4. Primjena EMDI u Moodle platformi: Podmodel za filteranje neaktivnih identiteta

Pri nastajanju neaktivnih identiteta, jedan od najčešćih problema je zaboravljena lozinka ili izgubljena lozinka, tj. nemogućnost postizanja konekcije između studenta i administratora. Zbog nemogućnosti da se postigne odnos između studenta i administratora takvi identiteti postoje u sistemu u punom svom kapacitetu ali kao neaktivni i predstavljaju zapostavljena mjesta za nenadgledani hakerski pristup. Prema tome, praznine u procesu komunikacije između studenta i administratora stvaraju neaktivne identitete. Sa druge strane postoje mnoge situacije u sistemu kao *Moodle* koji će automatski ili ručno obrisati takve identitete bez informisanja korisnika. Takođe, postoje situacije u kojima su identiteti aktivni po svom statusu, a ne bi trebao biti jer je suštinski maliciozan. Primjer za ovo je kada student završi kurs predavanja (programiranje, matematika, i sl.), ili napusti ili završi studije. Ipak, najčešća situacija u praksi je da student nije bio u stanju da pristupi *Moodle* sajtu jer je izgubio ili zaboravio svoju lozinku. U takvim situacijama, student nije voljan da se obriše njegov digitalni identitet. Prema tome, ovo jasno ukazuje da *Moodle* nema dovoljnu kontrolu nad procesnim tokom naspram sistema.

U ovom radu, predloženo rješenje za ove probleme je dato kroz primjenu EMDI odnosno njegov *feedback* proces. Proces *feedback-a* je primjenjen u *Moodle* platformi koristeći plagin za filtriranje neaktivnih modela kao podmodela. Plagin je zasnovan na interakciji između učesnika pri izmjenjivanju e-majl upozorenja u obliku

zahtjev/odgovor. Ovaj proces komunikacije je korišćen da uputi na situaciju u kojoj su student i administrator međusobno povezani tako da svaki od njih utiče na drugog, a da su pri tom njihove dinamike snažno povezane. Za bolje razumijevanje ovog plagina, dijagram toka je dat na slici 10, i biće opisan u više detalja.



Slika 10. Dijagram toka plagina filtera neaktivnih identiteta.

Proces filtriranja neaktivnih identiteta započinje procesom određivanja filtriranja kriterijuma. Da bi se bolje razumio predloženi model, tri primjera filtriranja kriterijuma su data na slici 10:

1. Vrijeme (administrator pravi filtriranje studenata po vremenu),
2. Kurs (administrator pravi filtriranje studenata po kursu kao što su baze podataka, matematika, i sl.),
3. Predavač (administrator pravi filtriranje studenata po predavačima koji su držali predavanja).

Potrebno je istaknuti da broj kriterijuma u praksi je moguće da se proširi na "*n filtriranje*". Nakon određivanja ključnih kriterijuma administrator pravi izbor kriterijuma za filtriranje neaktivnih identiteta. Da bi se pristupilo procesu filtriranja neaktivnih identiteta potrebno je da se podese izabrani kriterijumi. Na primjer, administrator može izvršiti proces filtriranja jednog od izabranih kriterijuma ili sve njih. Kada je proces filtriranja izabranog kriterijuma napravljen, i ako postoji potreba za dopunskim filtriranjem tada proces filtriranja je moguće da bude ponovljen. Nasuprot tome, ako ne postoji potreba za dopunskim filtriranjem tada administrator ima dvije

mogućnosti. Prvo, trenutno brisanje ili suspendovanje selektovanog neaktivnog identiteta i drugo, da pošalje e-mejl prema studentu kao zahtijev za reaktivaciju identiteta. Ako je student dao odgovor tada je identitet moguće da se obriše samo uz studentovo odobrenje. Nasuprot tome, izabrani neaktivni identitet će biti obrisan od strane administratora. U ovom modulu, postoje tri tipa uklanjanja identiteta iz repozitorija:

1. Fizičko brisanje – tabelarni red je potpuno obrisan.
2. Logičko brisanje – posebna vrijednost (0/1 ili netačno/tačno).
3. Suspenzija – identitet nije obrisan već je privremeno opozvan.

Suspenzija identiteta može biti takođe obezbijeđena na tri različita načina kao što je korišćenje foldera ili postavljanje fajlova, i ručno kroz status tabele. Predloženi plagin je dostupan na veb sajtu (https://commercial-doo.com/mdltest/).

3.3. Krađa identiteta

Krađa identiteta je moderni naziv za prastari fenomen koji je veoma često i danas u upotrebi. Poznat je kao jedan od oblika kriminala koji djeluje globalno i ne poznaje granice. Posebnu pažnju na sebe je skrenuo terorističkim napadom na Kule blizankinje 2001. godine u SAD. Najčešći motiv kradljivaca identiteta predstavljaju finasije (brz i lak izvor visokog profita). U najopštijem smislu krađu identiteta moguće je klasifikovati kao klasičnu i internet krađu. Pojam klasične krađe identiteta odnosi se na fizičku krađu primjera radi krađu ličnih stvari, vozačke dozvole, pasoša, i sl. Sa pojavom novih tehnologija, klasična krađa identiteta se razvila u mnogo opasniju sofisticiraniju internet krađu. Radi se o relativno novom stvorenom sociološkom fenomenu koji predstavlja mnogo razorniji, širi i kompleksniji problem nego što se uopšte u prvi mah i misli. Naime, njegova razorna moć ogleda se u tome što žrtva uopšte nije svjesna krađe sve dok ne bude prekasno. Jedan od najalarmantnijih aspekata krađe identiteta je činjenica da bilo ko može postati žrtva u bilo kom trenutku vremena. Žrtve i izvršioci krađe identiteta su različite dobi (u rasponu od novorođenčeta do pokojnika), pola, rase, društveno-ekonomskog statusa i zanimanja.

Krađa identiteta može imati ozbiljne posljedice za sve aspekte društva uključujući ekonomsku, finansijsku i nacionalnu bezbjednost. Vođeni tim saznanjima, brojne

razvijene države širom svijeta prepoznale su realnu opasnost od krađe identiteta i shvatile da se zakonodavstvom ne može riješiti ili spriječiti borba protiv krađe identiteta osim, ako sami ne usvoje mnogo efiksnija i naprednija preventivna rješenja. Jedan od pristupa koji se sprovodi u mnogim javnim i privatnim organizacijama je upotreba naprednih tehnologija. Praksa potvrđuje da propisanom primjenjenom takvih tehnologija postiže se bolja zaštita i verifikacija identiteta, a time i cjelokupna bezbjednost sistema. Prema Al-Khouri-u [58] krađa identiteta je aktivnost koja se dešava kada pojedinac personalne detalje preuzme ili ukrade od nekoga, pokušava da igra njegovu/njenu ulogu, ima pristup specifičnim informacijama ili servisima, izvrši finansijske transakcije, ili čak izvrši neko krivično djelo. Postoje mnoge vrste krađe identiteta, ali prevaranti najčešće ciljaju na personalne i poslovne identitete.

Personalna/poslovna krađa identiteta je proces neautorizovanog korišćenja personalnih/poslovnih informacija o identifikaciji sa namjerom izvršenja ili podsticanja na nelegalne aktivnosti kako bi se ostvario nezakonit profit. Pojam poslovni odnosi se na male organizacije, korporacije, finansijske, zdravstvene i vladine institucije. Takođe, personalna/poslovna krađa identiteta javlja se u slučajevima kada su personalne/poslovne informacije o identifikaciji zloupotrebljene u posrednom činjenju drugih kriminalnih djela. Najteži oblik krađe identiteta je kada napadač preuzme kompletan identitet žrtve. Radi se o slučajevima kada su ukradeni ključni dijelovi personalne/poslovne informacije o identifikaciji. U suštini, napadač sa lažnim identitetom uživa sva prava žrtve, a da pri tom žrtva nije ni svjesna toga. Žrtva ne može da sazna o krađi personalnog/poslovnog identiteta sve dok ne izvrši sumiranje računa (provjeri stanje računa) ili mnogo češći slučaj zaprimanjem upozoravajućeg izvještaja o prekoračenju računa od strane banke. Najjednostavniji primjer poslovne krađe identiteta je krađa elektronskog poslovnog računa.

Krađa identiteta je postala najbrže rastući kriminal u svijetu [59]. Bez sumnje, ekspanzija i povećanje sofisticiranih prijetnji krađe identiteta usvaja mnoge strategije informaciono-tehnoloških inicijativa kao što su e-vlada i e-poslovanje [60]. Brzi razvoj i pristupačnost informacionim tehnologijama su učinili lakšim i dostupnijim kriminal u obliku krađe identiteta. Trenutna istraživanja i studije ukazuju na napredak i širenje kompjuterskih tehnologija kao glavnog faktora koji dramatično uzrokuje krađu identiteta [61]. Činjenice nepobitno ukazuju da u posljednjoj deceniji krađa identiteta i nivo prevara su u konstantnom porastu širom svijeta (Amerika, Kanada, Kina,

Australija, Britanija, Japan i mnoge druge zemlje svijeta) sa gigantskim oštećenjima po žrtve i poslove. Brojni su primjeri koji to dokazuju.

Prema podacima američke agencije *Department of Justice*, u posljednjoj godini jedan od 14 amerikanaca je bio žrtva krađe identiteta [62]. Prema podacima američkog *Bureau of Justice Statistics* oko 18 miliona amerikanaca su bili žrtve krađe identiteta od čega je preko 7% starosti od 16 godina ili starije dobi [63]. Prema podacima CIFAS-a u 2014. godini u Velikoj Britaniji krađa identiteta je porasla za 25 % u odnosu na prethodnu godinu predstavljajući najveću prijetnju [64]. Krađa poslovnog identiteta je tipičan primjer krađe personalnih informacije preko 21,5 miliona ljudi u Americi koji su od 2000. godine konkurisali za poslove u saveznoj administraciji i kao takvi bili su predmet posebnih bezbjednosnih i drugih provjera [65]. Takođe, primjer krađe personalnih informacija je krađa koja je izvedena od strane kineskih hakera koji su ukrali personalne informacije više od 4 miliona američkih državnih službenika [66]. Ruski hakeri ukrali su preko 1.2 milijarde internet korisničkih imena i lozinki [67]. Kolika se važnost pridaje krađi identiteta najbolje ilustruju navodi kontra obavještajne američke službe bezbjednosti *Federalnog istražnog biroa* – FBI [68]. Prema riječima specijalnog agenta FBI u Njujorku *Dejvidu Vleaskes,* 5 februara 2013. godine uhapšena je grupa od 18 lica koji su optuženi za krađu podataka sa kreditnih kartica u Sjedinjenim američkim državama i za neovlašćeno prisvajanje sa tuđih računa preko 200 miliona dolara [69].

Kradljivci identiteta mogu veoma lako steći i zloupotrijebiti tuđe personalne informacije. Mnogo je načina na koji to čine od trivijalnih kao što je krađa ličnih stvari i pošte, kopanja po smeću, pa sve do upotrebe tehnološki sofisticiranih načina poput krađe elektronske pošte, onlajn aktivnosti. Zaprimanje tuđih informacija može se izvršiti i putem unutrašnjih izvora *(engl. inside sources).* Unutrašnji izvor je lice koje ima pristup tuđim personalnim informacijama koji ih može ustupiti iz neznanja ili sa namjerom. Prije svega, nezadovoljan ili nelojalan korisnik koji ima pristup osjetljivim personalnim informacijama, vođen različitim motivima, najčešće finansijskim može ustupiti takve informacije onima kojima su one potencijalno zanimljive ili korisne. Takođe, do personalnih informacija moguće je doći socijal inženjeringom, putem maloprodajnih transakcija, hakovanjem kompjuterskih sistema, fišing tehnikama, i na razne druge načine.

3.4. Budućnost digitalnog identiteta

Budućnost digitalnog identiteta igraće vrlo važnu ulogu u ličnom i profesionalnom životu svakog korisnika. Ubrzani evolutivni razvoj koji je omogućio planetarno veb povezivanje korisnika neće umanjiti prisustvo socijalne dimenzije pri razvoju novih fleksibilnih tehnologija za uklanjanje geografskih granica. Kao posljedice toga, korisnici će vjerovatno znatno više vremena provoditi na onlajnu nego što to čine danas. Na to upućuje i stil života koji jednostavno nameće takav tip aktivnosti kao što su poslovne, učenje, kupovina, igre, zabave, i sl. Značaj i važnost digitalnog identiteta u budućnosti će biti važniji nego ikad, jer će korisnici postati bliži jedni drugima zahvaljujući tehnološkim uređajima koji će zamagliti granicu između fizičkog i digitalnog svijeta.

Kako je personalni identitet postao važan dio ljudskog stanja, s tim i ograničavanje njegovih sposobnosti predstavlja strahovitu prijetnju za većinu ljudi. U tom kontekstu se strah od smrti tumači kao strah od gubitka identiteta. Da bi ljudi dobili identitet koji je značajan za njih spremni su na sve u životu poput promjene pola, učestvovanje u velikom bratu, i sl. Buduće tehnologije u vremenu ispred nas to vjerovatno neće promijeniti. Čak i sa pojavom budućih istinskih radikalnih tehnologija čovjek ih neće htjeti upotrijebiti ukoliko one uzrokuju neželjene izmjene njegovog identiteta. Nasuprot tome, ljudi će biti zainteresovani za tehnologije za koje smatraju da će osnažiti njihove identitete, proširiti društvenu mrežu i poboljšati ličnu reputaciju. To je u skladu sa rastom ljudskih izražajnih vrijednosti. Stoga, treba očekivati sve veći interes u tehnologijama i institucijama koje pomažu u upravljanju, manipulisanju i zaštiti identiteta. U isto vrijeme, rastu očekivanja i zahtjevi koji će mnoge ljude učiniti sumnjičavim u postojeće institucije, pronalazeći ih nesposobnim da odgovore njihovim potrebama. U tom pravcu biće potrebno povećati održavanje povjerenja u svim sferama života javnom, privatnom, i tehnološkom.

Tehnologije i politike koje utiču na lični identitet dopuštaju korisnicima da održavaju fleksibilnim društvene identitete. Tehnologije pojačavaju mnoge korisničke nedosljednosti u postupanju sa identitetima. U tom smislu, buduća javna politika će morati uzeti u obzir proširenja personalnih identiteta. Sa razvojem tehnoloških osnaženih identiteta korisnici će uporedo nastojati da povećaju zaštitu digitalne imovine i onlajn reputacije. Iako, trenutno postoji trend prema visokom stepenu otvorenosti

personalnih informacija, posebno među mlađim generacijama, prisutna je želja da se još uvijek održi kontrola nad ovakvim informacijama. Korisnici mogu mnogo toga da dijele iz svog života, ali vrlo oštro reaguju na pokušaje eksploatisanja ili manipulisanja sa informacijama bez njihovog odobrenja. Svakako, da je jedan od najvećih izazova u budućnosti digitalnog identiteta očuvanje zaštite višestrukih identiteta. Identitet sa takvim pristupom je još složeniji, jer svaki pojedinac može posjedovati više različitih identiteta, a time i uloga u kojima su identiteti različiti za svaku ulogu. U budućnosti, neminovno je postojanje bolje koordinacije informacija o identitetu među različitim servisima i među sistemima za pohranjivanje identiteta informacija. Identiteti posmatrani na osnovnom i biološkom nivou su jedinstveni, nepromjenljivi i otkrivaju brojne biometrijske indentifikatore kao što su otisak prsta, geometrija dlana, dužica, mrežnjača oka, i dr. Svi ovi indentifikatori odnose se prema pojedincu i nesumnjivo da je u budućnosti jedan od izazova razvijanje sistema i infrastrukture sposobne da povežu i zaštite ove višestruke indentifikatore.

Menadžment identiteta je ključni u pogledu budućnosti digitalnog identiteta i treba da bude dizajniran na jakom autentifikacionom mehanizmu u realnom i virtualnom kontekstu. U tom smislu, razvoj sistema menadžmenta identiteta treba da bude zasnovan na fleksibilnoj korisničko-orijentisanoj platformi koja će podržati sve mehanizme identiteta i protokole koji postoje i koji se pojavljuju. Takvi sistemi treba da budu sposobni da djeluju na različitim platformama, aplikacijama i servisno-orijentisanim arhitekturama. Pri tom korisnik treba da bude osposobljen da efikasno izvršava kontrolu nad svojim personalnim informacijama. U budućnosti, korisnik će imati snažniju kontrolu, u smislu ko raspolaže njihovim personalnim informacijam, u kom obimu i kako ih upotrebljava, minimizirajući time njihov rizik od moguće krađe identiteta i prevare. Njihov identitet i reputacija biće prepoznatljivi i prenosivi. Ako steknu dobru reputaciju na nekom sajtu oni će biti u mogućnosti da te pozitivne činjenice koristi i na bilo kom drugom sajtu. Za realizaciju ovakvih aktivnosti neophodno je, u budućnosti, razviti bezbjednije sisteme autentifikacije.

IV MENADŽMENT IDENTITETA I UPRAVLJANJE PRISTUPOM (IAM)

Menadžment identiteta i upravljanje pristupom - IAM je dio zaštite informacija koji se sastoji od menadžmenta identiteta i upravljanja pristupom. Nastao je kao odgovor na savremene bezbjednosne izazove koji su stavljeni pred organizacije odnosno sisteme. Svaki novi talas inovativnih tehnologija donosi organizacijama nove moćnije alate sa kojima je olakšana upotreba poslovnih informacija. Međutim, sa takvim tehnologijama dolaze i novi izazovi u pogledu upravljanja pristupom. Prije svega, radi se o izazovu centralizovanog pristupa informacija u sistemima, aplikacijama ili resursima. Često su IAM alati bili segmentno nadograđivani sa novim aplikacijama i hardverskim komponentama što je sveobuhvatno rezultiralo da IAM funkcije budu manje efikasne i efektivne. Danas, IAM rješenja omogućavaju čvrsto povezanu integraciju korisničkih identiteta sa politikama upravljanja pristupom preko različitih oblika aplikacija. Organizacije koje razvijaju i implementiraju IAM rješenja postaju značajno bezbjednije u podržavanju novih poslovnih inicijativa, i značajno mogu smanjiti cijenu upravljanja identitetima. Stoga, koncept menadžmenta identiteta i pristupa predstavlja disciplinu zaštite koja omogućava organizacijama bezbjedno upravljanje identitetima i pristupima u poslovnom okruženju.

4.1. Osnove IAM

Kada se govori o menadžmentu identiteta i upravljanja pristupom potrebno je dati najvažnije osnovne definicije termina u okviru ove teme. Od osnovnih definicija izdvojene su sljedeće [38]:

- Entitet ili subjekat (*engl. entity, subject*)
- identifikatori (*engl. identifiers*),
- kredencijali (*engl. credentials*),
- atributi identiteta (*engl. identity attributes*),
- područje digitalnog identiteta (*engl. domen of digital identity*),
- resurs (*engl. resource*),
- preferencija (*engl. preference*),

- svojstvo (*engl. trait*)
- sigurnosni autoritet (*engl. security authority*),

Entitet ili *subjekat* je osoba (pojedinac ili grupa ljudi), organizacija, ili sistem (softverski program, hardverski uređaj kao što je personalni računar, mobilni telefon ili mrežna oprema) koji zahtijeva pristup određenom resursnom mjestu. Entitet može imati jedan ili više identiteta od kojih svaki prezentuje različite karaktere.

Identifikatori su informacije koje jedinstveno predstavljaju određeni entitet. Mogu biti različiti nizovi brojeva, znakova i simbola ili bilo koji drugi karakterističan elemenat poput korisničkog imena, logujućeg identifikacionog broja, personalnog identifikacioniog broja – PIN, ili smart kartica. Skup identifikatora je mnogo veći od skupa identiteta, koji su opet veći od skupa ličnosti i organizacija.

Kredencijali su informacije korišćeni od strane entiteta u procesima identifikacije i autentifikacije. Oni predstavljaju dokaz da određeni entitet odgovara identitetu za koji se izdaje. Mogu biti bazirani na jednoj ili više informacija. Pojavljaju se u formi lozinke, digitalnih sertifikata, biometrijskih podataka, i dr.

Atributi identiteta su informacije entiteta koje nisu korišćene u procesima identifikacije, autentifikacije i autorizacije. Atributi čine osnovu personalnog identiteta tj. kvalitete ili karakteristike ličnosti. Primjeri atributa su ime, prezime, krvna grupa, ime zaposlenog, i sl. Biometrijski podaci mogu takođe biti primjeri atributa identiteta. Kako su biometrijski podaci jedan od oblika kredencijala neophodno je istaći da atribute identiteta i kredencijale ne bi trebalo smatrati strogo odvojenim.

Područje digitalnog identiteta je domen u kojem se određuje jedinstvenost nekog digitalnog identiteta.

Resurs ili objekat je pristupno mjesto pasivnog entiteta. Može biti fizički (objekti, kompjuterski uređaj, ili druga tehnička oprema), informacioni (intelektualna svojina, aplikacija i povjerljive informacije), i personalni (korisnici, zaposleni, i sl).

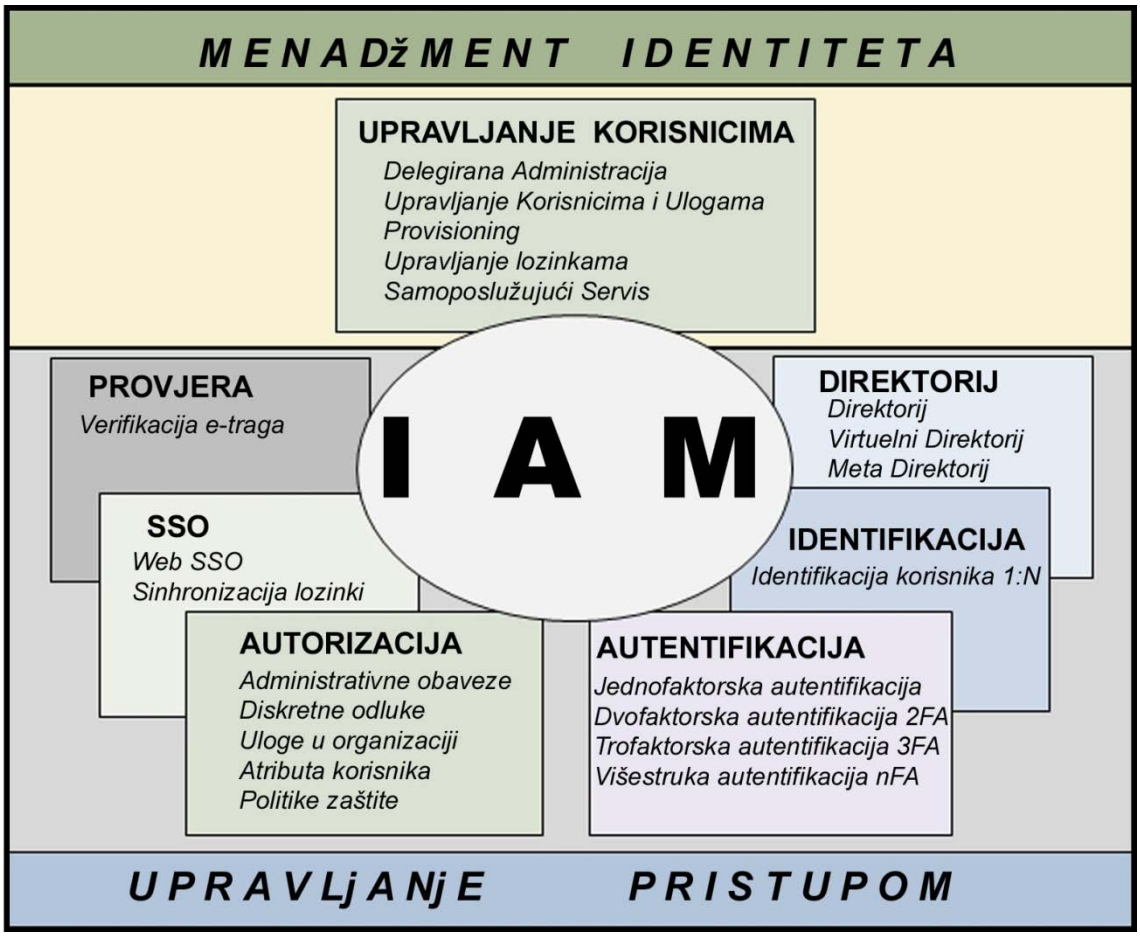
Preferencija predstavljaju personalne informacije koje preferira subjekat kao što su tip automobila, vrsta hrane, stil oblačenja, vrsta sporta, i sl.

Svojstva predstavljaju nasljedna svojstva entiteta kao što su boja kose, očiju, i sl.

Sigurnosni autoritet je autoritet koji vrši autentifikaciju kredencijala.

4.2. Osnovne komponente i funkcije IAM

Kao što je prethodno naglašeno IAM se sastoji iz dvije glavne komponente menadžmenta identiteta i upravljanja pristupom čije su funkcije potpuno odvojene. Kako je menadžment identiteta opisan u prethodnom poglavlju III, tako je komponenta upravljanje pristupom centralna tema ovog poglavlja. Komponenta upravljanja pristupom predstavlja najvažniju komponentu IAM sistema, u kojem je dio za autentifikaciju suštinski dio koji ga izdvaja od svih drugih komponenti. Na slici 11 su prikazane osnovne komponente IAM.



Slika 11. Osnovne komponente IAM

Upravljanje pristupom obuhvata sljedeće osnovne komponente i funkcije IAM za bilo koji servis [70]:

- Identifikaciju,
- Autentifikaciju, i
- Autorizaciju,
- Jednostruka prijava – SSO,
- Revizija,
- Direktorij.

Osnovni cilj svake organizacije je, da pored zaštite svojih resursa, obezbijede pristup i zahtjevani nivo pristupa za korisnke pri izvršavanju njihovih zadataka. Upravljanje pristupom se u najopštijem smislu može shvatiti kao usluga koja omogućava pristup na takav način da svakog korisnika drži odgovornim za njegove aktivnosti. Matematički posmatrano, radi se o matričnom pristupu u čijim se vrstama nalaze operacije sistema, a u kolonama korisnici. Stoga, važnost komponente upravljanja pristupom ogleda se u određivanju prava pristupa i uslova pristupa resursima. Za upravljanje pristupom najčešće važe sljedeća opšta paravila:

- Upravljanje pristupom je obavezna i neizostavna komponenta.
- Svi autorizovani korisnici bi trebalo da budu ovlašćeni kako bi mogli pristupiti određenom resursu.
- Korisnici sistema ne smiju zloupotrebljavati tuđa prava pristupa.

Osnovne komponente upravljanja pristupom detaljnije su opisane u narednim sekcijama ove disertacije.

4.2.1. Identifikacija

Identifikacija je prvi i osnovni korak u procesu jedinstvenog identifikovanja korisnika odnosno njegovog predstavljanja računaru. Suštinski, identifikacija predstavlja pripremni korak za autentifikaciju korisnika, tj. prethodi procesu autentifikacije. U informacionim sistemima postoji potreba korisničkog identifikovanja pri čemu se ne identifikuje trag aktivnosti subjekta već njegovog identiteta. Dakle, računar ne razlikuje korisnike ali je u stanju da razlikuje njihove korisničke naloge. Da bi korisnik mogao pristupiti korisničkom nalogu neophodno je da ima jedinstven identifikator u procesu identifikacije. Ovaj proces je zasnovan na principu upoređivanja prezentovanih

karakteristika sa svim prethodno pohranjenim u bazi podataka (1:N) – ko si ti? Stoga za identifikaciju kaže se da je proces koji pravi provjeru postojanja prezentovanog korisničkog identiteta prilikom pristupanja resursu, tj. daje odgovar na pitanje da li postoji takva osoba i o kojoj se osobi radi. U literaturi značaj procesa identifikacije je često zapostavljen, a neki autori poput [71, 72] ukazuju na identifikaciju kao dio procesa autentifikacije. Svakako, ovaj pristup u procesu identifikacije je krajnje zbunjujući. Posebna važnost procesa identifikacije ogleda se u aspektu bezbjednosti jer predstavlja procesni filter za upotrebu svih ostalih procesa u IAM. Jedinstvena identifikacija korisnika je najkritičniji trenutak u procesima pristupanja resursima, da li je određena osoba baš ta osoba i za koju se i predstavlja. Pozitivna identifikacija svakog korisničkog sistema je ključna u osiguravanju efektivnije politike i svih narednih procesa. Greške koje se jave u ovom procesu narušiće vrijednost cijelog IAM sistema.

4.2.2. Autentifikacija

Proces autentifikacije može biti veoma složen i logički nastupa po završetku procesa identifikacije. Suštinski, autentifikacija predstavlja pripremni korak za autorizaciju korisnika, tj. prethodi procesu autorizacije. Autentifikacija je faza raspoznavanja koja obično sugeriše na snažniji oblik identifikacije. Međutim, radi se o potpuno dva odvojena procesa koja idu u paru. Proces autentifikacije se odvija tako da subjekat pokušava potvrditi identitet uz dostavljanje kredencijala koji treba da egzaktno odgovaraju naznačenom identitetu. Na osnovu tih kredencijala vrši se upoređivanje u sistemu sa prethodno pohranjenim identitetima u bazi podataka (1:1). Stoga, za autentifikaciju se kaže da je proces u kojem se pomoću kredencijala utvrđuje identitet vlasnika, odnosno potvrđuje da se zaista radi o korisniku koji se kao takav i predstavlja. Nivo zaštite koji se obezbjeđuje procesom autentifikacije je promjenjiv i zavisi od postavljenih bezbjednosnih zahtjeva. Greške koje se jave na ovom nivou takođe će narušiti vrijednost cijelog IAM sistema.

Procesi autentifikacije obuhvataju nekoliko naučnih oblasti obično podijeljenih u tri glavna područja odnosno tri autentifikaciona faktora [73]:

1. Autentifikacioni faktor zasnovan na ”*nečemu što znaš*” (PIN, lozinka, i dr.),
2. Autentifikacioni faktor zasnovan na ”*nešto što imaš*” (mobilni uređaj, smart kartica, memorijske kartice, USB drajveri, i dr.),

3. Autentifikacioni faktor zasnovan na ”*nešto što jesi*” (otisak prsta, lice, govor, dinamika kucanja, i dr.).

Autentifikacioni faktori u procesu autentifikacije mogu se koristiti zasebno ili međusobnim kombinovanjem. Zavisno od broja upotrebljenih faktora i načina na koji se koriste razlikujemo pojedinačnu i višestruku autentifikaciju.

4.2.2.1. Jednofaktorska(pojedinačna) autentifikacija

Jednofaktorska autentifikacija je najjednostavnija autentifikacija korisnika zasnovana na upotrebi samo jednog od bilo koja tri osnovna autentifikaciona faktora. S obzirom da se pojedinačnom autentifikacijom obezbjeđuje najniži nivo zaštite ona se obično primijenjuje za jednostavnije sisteme koji imaju manje bezbjednosne zahtjeve. Svaki tip autentifikacionog faktora je približno isti u smislu obezbjeđivanja nivoa zaštite. Ipak, neophodno je istaći da svaki tip sigurnosti je viši u odnosu na prethodni. Na primjer, tip tri je najteži oblik za ”razbijanje” u poređenju sa druga dva faktora. Međutim, kako ne postoji apsolutna zaštita svaki od navedena tri faktora mogu biti razbijena. Savladavanje nedostataka jednofaktorske autentifikacije postiže se primjenom višestruke i jake autentifikacije.

4.2.2.2. Višestruka i jaka autentifikacija

U literaturi za termin višestuka i jaka autentifikacija prisutna su različita mišljenja bez jedinstvenog stava po pitanju univerzalne definicije. U kontekstu autentifikacije, ovaj rad ima istu konotaciju pojmova višestruka i jaka. Višestruka autentifikacija je definisana kao složena autentifikacija koja podrazumijeva upotrebu najmanje dva/tri osnovna autentifikaciona faktora.

Višestruka autentifikacija potvrđuje pregled traga korisničkih aktivnosti zahtijevajući ubjedljiv dokaz identiteta prije nego što se odobri pristup osjetljivim informacijama i resursima. U autentifikacionom pristupu procesom jake autentifikacije ostvaruje sinergijski pristup. Pri integrisanju različitih faktora kroz višestruku autentifikaciju svaki od pojedinačnih faktora zadržava svoj izvorni oblik dodajući jedan novi nivo zaštite. Moć takvog autentifikacionog mehanizma onemogućava napadaču pristup osjetljivim informacijama ukoliko nije prošao sve nivoe odnosno prikupio sve potrebne

kredencijale. Stoga, može se zaključiti da višefaktorska autentifikacija je fundamentalno oružje u borbi protiv krađe korisničkih informacija. Ukoliko su u procesu višefaktorske autentifikacije upotrebljena dva/tri autentifikaciona faktora govorimo o dvofaktorskoj (2FA)/trofaktorskoj (3FA), tj.višefaktorskoj autentifikaciji (nFA).

Koncept dvofaktorska autentifikacija posmatran u odnosu na pojedinačnu autentifikaciju je dvodimenzionalan jer daje još jednu novu dimenziju obično drugi identifikator (nešto što korisnik ima). Na taj način dvofaktorska autentifikacija nadograđuje jednofaktorsku autentifikaciju dodajući dodatni sloj autentifikacije obezbjeđujući time viši nivo zaštite. Teoretski posmatrano, u dvofaktorskoj autentifikaciji mogu biti upotrebljena dva ista faktora. Međutim, praktični koncept dvofaktorske autentifikacije se mora zasnivati na upotrebi različitih autentifikacionih faktora kako bi se postigao zadovoljavajući nivo zaštite. Sa druge strane, koncept trofaktorska autentifikacija posmatran u odnosu na dvofaktorsku autentifikaciju je trodimenzionalni jer daje još jednu novu dimenziju treći identifikator (npr. biometriju). Snaga trofaktorske autentifikacije ogleda se u tome što napadač ne može pristupiti sistemu ukoliko ne prikupi sva tri autentifikaciona faktora. Trofaktorska autentifikacija nadograđuje dvofaktorsku autentifikaciju omogućavajući novi sloj autentifikacije obezbjeđujući time najviši nivo zaštite. Kao i kod dvofaktorske autentifikacije tako i kod trofaktorske autentifikacije praktični koncept se mora zasnivati na upotrebi različitih autentifikacionih faktora kako bi se postigao zadovoljavajući nivo zaštite. Međutim, neophodno je istaći da primjenom trofaktorske autentifikacije nije moguće postići apsolutnu zaštitu. Napadač može uspješno prikupiti sve relevantne autentifikacione elemente i time ugroziti sistem zaštite.

4.2.3. Autorizacija

Proces autorizacije logički slijedi po završetku procesa autentifikacije i ukazuje na to ko je autorizovan da izvrši specifične operacije. Uloga i važnost autorizacije kao finalnog procesa odnosi se na dozvole i ograničenja autentifikovanih korisnika. Subjekat koji je identifikovan i autentifikovan ne znači da je automatski i autorizovan. Za subjekat se kaže da je autorizovan ukoliko su dopuštene njegove specifične aktivnosti, u suprotnom ako specifične aktivnosti nisu dopuštene subjekt nije ni autorizovan. Dakle, autorizacija je proces primjenjivanja politika zaštite u kojem se određuje šta korisniku može biti dopušteno da radi. Sa politikom zaštite određuje se šta je dozvoljeno i koja su

ograničenja. Na taj način korisnicima se odobravaju aktivnosti i pristupi određenim osjetljivim resursima uz dodjelu principa najmanje privilegije i razdvajanja obaveza.

Princip najmanjih privilegija podrazumijeva da se entitetu odobri najmanja količina privilegija potrebna za izvršenje određenog zadatka. Princip razdvajanja obaveza podrazumijeva razdvajanje kritičnih funkcija u procesima (koracima) među različitim pojedincima kako bi spriječili pojedince u narušavanju kritičnih procesa. Primjer autorizacionih ovlašćenja uključuje pristup fajlovima i folderima, vrijeme pristupa, količinu dostupnog prostora na hard disku i sl. Za različite korisnike mogu se dodijeliti različite uloge u sistemu. To jasno ukazuje da je proces autorizacije usko povezan sa korisničkim *provisioning-om*. Autentifikacija i autorizacija se provode od strane organizacije i/ili SP-a. Postoje dvije komponente autorizacije i to:

1. Osnovna provjera – provjera ovlašćenja dodjeljena od strane sistem administratora nad sistemskim resursima, i
2. Dodatna provjera – provjera ovlašćenja od strane sistema ili aplikacija u korisničkom pokušaju da pristupi ili ažurira sistemske resurse.

U većini slučajeva, proces autorizacije zasniva se na sistemskoj matričnoj procjeni upravljanja pristupom koji upoređuje subjekt, objekt i namijenjene aktivnosti. Treba imati na umu da proces autorizacije i pristupa nekom resursu u izuzetnim slučajevima moguće je definisati bez korišćenja procesa autentifikacije. To se dešava kada su ovlašćenja data anonimnom korisniku jer on ne prolazi kroz proces autentifikacije. Ovakav selektivni pristup dodjeljivanja ovlašćenja je vrlo ograničen i kao takvog treba ga i koristiti. Na ovaj način mogu se dodijeliti ovlašćenja za subjekte koji su logovani na mrežama ali su im onemogućeni pristupi fajlovima, kopiranju, štampanju, i sl.

Autorizacija dodjeljivanja prava pristupa kompjuterskim resursima zasnovana je na bazi sljedećih opštih modela upravljanja pristupom [74]:

- Administrativne obaveze – MAC (*engl. Mandatory access control*)
- Diskretne odluke – DAC (*engl. Discrection access control*)
- Uloge u organizaciji – RBAC (*engl. Role-based access control*),
- Atributa korisnika – ABAC (*engl. Attribute-based access control*),
- Politike zaštite – PBAC (*engl. Policy-based access control*).

4.2.4. Jednostruka prijava – SSO (*engl. Single Sign-On*)

Koncept SSO dopušta korisniku da sa jednim logovanjem obezbijedi autorizovan pristup svim servisima i aplikacijama koji čine dio okruženja njegovog identiteta. Na ovaj način se eliminišu dosadna korisnička zamaranja "*stani pa kreni*" i kontinuirana ispitivanja korisničkog strpljenja uzrokovanim višestrukim logovanjima. Takođe, druge prednosti SSO su u pogledu poboljšanja integriteta pojedinačnih kredencijala i lozinki čime se unapređuje korisnička i administratorska produktivnost. Korisnička produktivnost ogleda se u samom načinu eliminisanja pamćenja višestrukih lozinki i opasnosti koje dolaze sa lozinkom.

Korisnici u SSO okruženju imaju potrebu da pamte samo jednu lozinku. Sa vremenskim istekom lozinke korisnici prave izmjenu prema centralnom sistemu menadžmenta identita i izmjene se automatski šalju svim decentralizovanim sistemima koji su registrovani u jezgru menadžmenta identiteta. Na taj način vrši se sinhronizacija lozinki i značajno se pojednostavljuje rad krajnjem korisniku. Administratorska produktivnost proizlazi iz korisničke produktivnosti jer sa smanjenim brojem korisničkih logovanja i administratori imaju manji broj identiteta i naloga za upravljanje. Sa administratorskim instaliranjem korisničkog naloga korisniku se odobrava pristup svim decentralizovanim sistemima. Ukoliko, je korisnički nalog ukinut od strane sistem administratora time je korisniku odbijen pristup svim decentralizovanim sistemima.

Pored upravljanja lozinkama i sesijama prednost SSO je u direktorijskoj nezavisnosti. Na taj način procesi korisničkog pristupa postaju jeftiniji, jednostavniji, efikasniji i fleksibilniji uz mogućnost pravljenja određenih izmjena profila tokom vremena. Nasuprot pozitivnim stranama koncept SSO ima i nedostatke. Glavni nedostatak SSO rješenja je da napadač po sticanju korisničkih kredencijala, zbog centralizovanog pristupa može pristupiti svim decentralizovanim sistemima bez kontinuirane autentifikacije. Sa kompromitovanjem lozinke SSO sistema uvodi se ranjivost u cijeli sistem. Takođe, ranjivost SSO sistema je usmjerena i prema sistem administraciji i procesima upravljanja nalogom u vidu obrade korisnika koji više nije autorizovan. Za uspješnu zaštitu ključnih kredencijala pri implementaciji bilo kog SSO rješenja neophodno je obezbijediti posebne mjere zaštite.

Zavisno od pogleda u kojem su izraženi korisnički zahtjevi u tom pravcu se razvijaju pojedina SSO rješenja (npr. *Web SSO* rješenje). Primjer *Web SSO* rješenja je *Microsoft Passport*. Dok se u pojedinim organizacijama okreću korisničkim zahtjevima u cilju smanjenja troškova i većoj bezbjednosti time se na vebu ti zahtjevi stavljaju u drugi plan, ističući prvenstveno važnosti korisničkih usluga. Najpoznatiji protokol kojim se implementira SSO funkcionalnost je Kerberos, koji se između ostalog koristi i kao autentifikacioni protokol kod *windows* i drugih operativnih sistema. Potrebno je istaknuti da je SSO veoma važan režim rada sistema za upravljanje identitetima.

4.2.5. Provjera ili revizija (*engl. auditing*)

Provjera ili revizija je važan kontrolni mehanizam IAM sistema koji čini sastavni dio standardnih bezbjednosnih operacija. Provjera doprinosi detekciji svih neautorizovanih pristupa sistemu kao i prevarantskih aktivnosti, obezbjeđujući da korisnički pristup bude postavljen od strane menadžmenta u skladu sa politikom zaštite i propisima. Dakle, pod revizijom podrazumijevamo proces prikupljanja, arhiviranja i analizu pregleda, ispitivanja i zapisivanja korisničkih naloga i procesa u aktivnostima izvedenih unutar bezbjednosne arhitekture. Osnovna namjena je da u sistemu bude zabilježen e-trag prilikom pristupa korisnika. Provjera stvara pregledni trag koji se uredno na računaru pohranjuje u bezbjednosnu log datoteku. Log datoteka bezbjednosno relevantnih događaja je dobro konfigurisana i redovno pregledana.

Pregledni tragovi mogu biti korišćeni za rekonstrukciju događaja i za verifikovanje narušenosti politike zaštite ili autorizacije. Sa procesom provjere moguće je utvrditi odgovornost pojedninca na onlajn aktivnostima. Prilikom upoređivanja sadržaja iz preglednih tragova sa procesom autorizacije i autentifikovanih korisničkih naloga, odgovornim pojedincem se može smatrati onaj koji je povezan sa tim korisničkim nalogom putem kog su i izvršene onlajn aktivnosti. U tom kontekstu IAM revizija predstavlja sredstvo prikupljanja informacija s IAM sistema koje su uključene u životni ciklus identiteta. Isticanje značaja procesa provjera nisu na prvi pogled prepoznate u IAM sistemu ali svakako da daju posebnu unutrašnju vrijednost za zaštitu i usklađenost sistema. Većina zakona i propisa zahtijevaju brojne provjere logovanja, što predstavlja izazov za sve organizacije.

4.2.6. Direktorij (*engl. directory*)

Za pohranjivanje personalnih korisničkih informacija koristi se direktorij koji obuhvata tri područja [70]:

- Direktorij,
- Virtualni direktorij,
- Meta direktorij.

Direktorij je najkritičnija komponenta svakog IAM rješenja jer predstavlja jezgro sistema menadžmenta identiteta. Suštinski, direktorij predstavlja "*imenik*" sa višestrukom ulogom. Centralna uloga direktorija je pohranjivanje i čuvanje personalnih korisničkih informacija. Povrh toga, direktorij igra ključnu ulogu u autentifikaciji korisnika, i na osnovu zahtjeva omogućava servisnu isporuku. Direktorij se koristi za centralizovano upravljanje o korisničkim podacima, grupama, serverima, štampačima, i sl. Dakle, direktorijski serveri se koriste za pohranjivanje informacija i servera koji mogu duplirati elemente podatka potrebnim za poboljšanje dostupnosti i skalabilnosti. Aplikativni pristup podacima koristi standardne protokole kao što je LDAP (*engl. light-weight directory access control*) ili X.500. Pristup direktoriju i svim informacijama ograničava se primjenom bezbjednosne politike koja je takođe pohranjena unutar direktorija.

Virtuelni direktoriji su direktoriji koji nisu smješteni u istu fizičku strukturu kao veb domaći direktoriji. Oni mogu biti na potpuno različitim lokacijama u fizičkom direktoriju strukture, primjera radi na drugom hard disku ili udaljenom kompjuteru. Virtualni direktorij dopušta pohranjivanje na jednom mjestu bez premještanja osjetljivih informacija tako da informacije o identitetu veoma brzo i efikasno se mogu integrisati s poslovnim aplikacijama. Značaj i važnost virtualnih direktorija ogleda se u fleksibilnom pristupu sa zahtjevima za integraciju informacija iz različitih direktorija. Umjesto fizičke pohrane informacija na jednom mjestu, virtualni direktoriji pohranjuju informacije prema zahtjevu. Osim toga, poseban značaj virtualnih direktorija je što oni zadržavaju informacije na izvornim lokacijama čime se omogućava izbjegavanje neželjenih sukoba unutar podsistema koji nastoje zadržati pravo vlasništva nad korisničkim informacijama. Informacije o korisniku se isključivo koriste na određeni zahtjev korisnika te u svim ostalim slučajevima ostaju pohranjene u direktoriju gdje su i prvobitno nastale.

Meta direktoriji je direktoriji sa meta informacijama. SP-i mogu dijeliti identitete – povezane podatke na meta nivou. Za primjenu meta direktorija potrebno je ostvariti integrisanje svih SP-a specifičnih identiteta prema meta – identifikatoru povezanog sa kredencijalima. Ovaj direktorij omogućava prikupljanje informacija iz različitih direktorija čime se obezbijeđuje pojedinačni pregled informacija. Sa korisničkog aspekta, ovaj pristup može se posmatrati kao sinhronizovanje lozinki preko višestrukih SP-a. Dakle, lozinke su automatski razmjenjene sa svim drugim SP-a. Ova arhitektura može biti korišćena u velikim sistemima gdje su svi servisi povezani prema meta direktoriju. Ovaj direktoriji omogućava jednostavnost uporebe korisničkih informacija jer administracija je urađena od strane pojedinačnog autoriteta. Drugim rječima, prednosti korišćenja meta ditektorija je u jednoj referentnoj tački koja obezbijeđuje apstraktne granice između aplikacija i stvarne primjene. Na taj način se smanjuju višestruki direktoriji, a s tim i administrativni zadaci.

4.3. Učesnici i zahtjevi u IAM

Razmatranje učesnika u IAM-u je ključno u razumijevanju IAM arhitekture. U tom kontekstu posmatranja razlikujemo nekoliko učesnika u menadžmentu identiteta koji mogu imati jednu ili više uloga koje su potpuno odvojene [70], i to:

- Subjekt (korisnik, pojedinac ili entitet),
- Provajder identiteta – IP,
- Servis provajder – SP,
- Kontrolni učesnici, i
- Personalni autentifikacioni uređaj – PDA.

4.3.1. Subjekt

Subjekt ili korisnik je učesnik, obično pojedinac koji zahtijeva uslugu od SP-a. Subjekat posjeduje atribute identiteta u formi digitalnog zapisa koji se koriste u procesima autentifikacije od strane SP-a. Subjekti su vlasnici identiteta koji treba da posjeduju najmanje jedan identitet da bi mogli učestvovati u procesu autentifikacije. Mogu posjedovati i više identiteta pri čemu servisi ne dijele autentifikacije. Subjekti

dostavljaju direktno ili indirektno sve neophodne atribute identiteta za formiranje svakog od njihovih identiteta. Atributi identiteta mogu biti u formi podataka navedenog prilikom registracije, pretraživanja ili sticanjem historija. Povezani zapisi mogu biti kombinovani sa atributima identiteta, na primjer korisnik obezbijedi kućni i poštanski broj na osnovu kojih je direktorij u stanju pronaći punu adresu. Subjekti prema potrebi mogu da modifikuju ili koriguju svoje atribute identiteta.

4.3.2. Identitet provajder

Identitet provajder – IP obezbjeđuje autentifikaciju servisa prihvatajući ili odbijajući korisnički identitet. Na taj način IP obezbjeđuju identitete za subjekte potvrđujući korisničku vrijednost (baziran na biranim autentifikacionim mehanizmima). Davalac identiteta je organizacija ili kompanija koja upravlja sa identitetom svojih korisnika. Identitet provajder može izdati sertifikate koji potvrđuju vezu između navedenih atributa biometrijskih obrazaca i dokumenata. Sertifikati mogu biti digitalni ili izdati u obliku papira ili plastike. Upotrebom ovih sertifikata moguće je otkriti integritet i autentičnost informacije o korisniku (primjeri su Gugl, *Microsoft* i Fejsbuk). IP je odgovaran za provođenje primarne autentifikacije entiteta koji se odnosi na uspostavljanje veze između entiteta i identiteta. Primarna autentifikacija je zasnovana ne nekom od autentifikacionih faktora.

IP može dati određene korisničke podatke davaocima resursa nakon izvršene autentifikacije. U procesu autentifikacije jedan identitet može biti pridružen jednom ili nekolicini IP-a. IP je snažno u vezi sa SP-om kojem obezbjeđuje kredencijale za autentifikaciju korisnika. Kredencijali izdati od strane IP-a mogu sadržavati atribute izdate od strane bilo kog IP-a. Proces osiguranja identiteta dopušta pridruživanje i drugih subjekata sa određenim stepenom povjerenja. IP može obezbijediti autentifikaciju za višestruke SP-e. IP postoji uglavnom u autoritativnim javnim institucijama kao što su vlada, i vladine agencije (CIPS za izdavanje vozačkih dozvola, ličnih karti, i sl.).

4.3.3. Servis provajderi

Uloga SP-a je da korisnicima na osnovu podnijetog validnog zahtjeva obezbijede određeni servis ili pristup prema resursima. SP-i predstavljaju svrhu formiranja i

postojanja digitalnog identiteta. Korisnici kroz SP-e stiču sve funkcije. Najvažniji zahtjev za SP-e je određivanje u kom obimu oni imaju povjerenje u korisničke kredencijala i atribute koje sadrže. Zavisno od prirode pruženog servisa od strane SP-a određeni nivo povjerenja treba biti primjenjen. Proces verifikovanja može biti veoma kompleksan zadatak i kao takav zahtijeva saglasnost sa propisima i zakonima usmjerenim na sprečavanje krađe personalnih informacija.

4.3.4. Kontrolni učesnici

Kontrolni učesnici su u pravilu agencije za sprovođenje zakona i kontrolnih tijela koji mogu zahtijevati pristup prema informacijama o identitetu. Na primjer, sesijsko logovanje uključuje upotrebu informacija o identitetu i drugih podataka u svrhe kao što je forenzička istraga. Ključni zahtjev ovih učesnika je provjerljivost i podrška za forenzičke istrage. Osim toga, kontrolna tijela mogu obavljati pregled informacija o identitetu.

4.3.5. Personalni autentifikacioni uređaji

Personalni autentifikacioni uređaji – PAD (*engl. personal authentication devices*) su hardverski uređaji koji mogu da sadrže pametnu karticu i senzore koji posjeduju različite identifikatore i kredencijale (na primjer mobilni uređaji). Unutar konteksta kompjuterske zaštite, ovaj termin je prvi put bio upotrebljen 1985. godine od strane Wonga *et al.*, [75]. U skorije vrijeme inkarnacija istog koncepta može se pronaći u obliku personalnih povjerljivih uređaja definisana u radu [76]. Dakle, suštinski koncept je isti, samo što su zahvaljujući rapidnom tehnološkom razvoju uređaji značajno napredovali pri tom mijenjajući radikalno svoje perfomanse. Posmatrano sa korisničke strane primjenom PAD-a se mogu osnažiti korisnička iskustva i olakšati automatizacija kao i sistemska podrška menadžmenta identiteta. PAD uređaj ima brojne prednosti u procesima autentifikacije. Prvenstveno, ovaj uređaj otklanjanja slabosti i neugodnosti koji nastaju prilikom upotrebe metode zasnovane na autentifikacionom faktoru korisnika “nešto što zna”. Pored toga, prednosti PAD uređaja su u pogledu obezbijeđivanja korisničko – prijateljske i korisničko – orijentisane primjene, i podržavanja nFA [70] kao i biometrijskih tehnologija. Međutim, fundamentalna prednost PAD u odnosu na proste računare koji koriste opšti operativni sistem kao što je *Windows* ili *Linux* je što PAD ima moćno izolovane procese [70]. To podrazumijeva da

ugrožavanjem aplikacije koja je u trenutnoj upotrebi ne kompromituje ostale neaktivne aplikacije u PAD uređaju.

Ova prednost postaje manje važne za mobilne telefone pošto proizvođači kontinuirano i ubrzano uvode nove fleksibilnije i multifunkcionalnije telefone. S novim pametnim mobilnim tehnologijama uvode se i mnoge ranjivosti. Na primjer, razvijanje različitih oblika virusa za mobilne telefone čak i virusa za radio frekvencijsku identifikaciju – RFID. Ovakvi nedostaci mogu da ugrožavaju i procese nFA zasnovane na biometriji. Dakle, primjena zaštite u PAD uređajima je veoma osjetljiv proces. Posljednih godina sa tehnološkim razvojem pristupačnost ovih uređaja postaje sve veća. Kanali autentifikacije koji mogu biti primijenjeni u PAD-u mogu se grupisati u dvije glavne kategorije [70]:

- pojedinačni kanal autentifikacije, i
- dupli kanal autentifikacije.

Danas je upotreba duplih kanala autentifikacije sve zastupljenija posebno u bankarskom sektoru koji zahtijeva veći nivo zaštite. Radi se o dva potpuno različita tipa kanala u kojem je jedan od kanala autentifikacije zasnovan na upotrebi mobilnih mreža, uglavnom GSM (*engl. Global Sytem for Mobile Communications)*. Upotrebom GSM moguće je ublažiti mnoge zaštitne ranjivosti kao što su fišing napadi ili čovjek – u – sredini (*engl. man – in – middle, MITM*). Takođe, postoje i druge prednosti upotrebe ovog metoda kao što su smanjenje cijene troškova sa povećanom korisničkom upotrebljivošću, što čini ovaj metod veoma atraktivnim u bankarskom poslu.

4.4. Arhitektura IAM

Arhitektura IAM igra veoma važnu ulogu u sprečavanju krađe identiteta. Različite IAM arhitekture imaju različite bezbjednosne aplikacije. Postoji mnogo radova koji su bavećи se arhitekturama menadžmenta identiteta dali određeni klasifikacioni pristup. Prema Palfrey-u i Gasser-u [77] postoje tri tradicionalne arhitekture menadžmenta identiteta centralizovana, federativna i korisničko orijentisana. U drugim radovima moguće je pronaći klasifikacione pristupe u kojima autori pored tradicionalnih arhitektura tretiraju i druge arhitekture kao što je Jøsang [43] izolovanu arhitekturu, Alpár *et al.*, [78] *network-based* arhitekturu i *claim-based,* dok u radovima Zwattendorfer *et al.*, [79],

Gopalakrishnan-u [80] *cloud identity* arhitekturu. Takođe, u radu Zwattendorfer-a *et al.*, [81] daju pregled arhitekture identiteta oblaka u menadžmentu identiteta. Imajući u vidu fokus ovog rada u nastavku je dat kratki opis četiri osnovne tradicionalne arhitekture.

4.4.1. Izolovana Arhitektura

Spada u najjednostavnije arhitekture koja simplifikuje menadžment SP-a. Ovaj model zahtijeva da svaki korisnik posjeduje identifikator za pristup svakom izolovanom servisu. U ovom modelu ne postoji kooperacija između učesnika u svrhu korisničke autentifikacije. SP vjeruje samom sebi i igra ulogu IP-a. Istorijski posmatrano, internet SP-a djeluje u izolovanom sistemu menadžmenta identiteta. Glavni sistem menadžmenta identiteta trenutno razvijen na internetu je nazvan Silo model. Trenutna praksa za onlajn SP-e je da djeluju kao kredencijali provajdera i identifikatori provajdera prema svojim korisnicima. Korisnik dobija odvojeno jedinstvene identifikatore od svakog SP/IP kada je u sesiji sa istima. Osim toga, svaki korisnik ima odvojene kredencijale pridružene sa svakim od njegovih identifikatora. Ovaj pristup može obezbijediti jednostavan IAM sa tačke gledišta od SP-a, ali je problematično za korisnike jer sa brojnim povećanjem identifikatora značajno se otežava njihovo upravljanje. Posljednih godina, eksponencijalni rast onlajn servisa uzrokuje korisničku prenatrpanost i zamorenost sa kredencijalima i identifikatorima što predstavlja značajnu barijeru za njihovu širu upotrebu. Dakle, realni problem je u povećanju broja lozinki, korisnička zaboravnost, kao i otežanom upravljanju sa istima što očigledno može voditi visokoj cijeni administrativnog održavanja. Sve ovo može da rezultira da korisnici ne dostignu puni svoj potencijal u upotrebi servisa. Upravo iz tih razloga su razvijene i primjenjene nove arhitekture menadžmenta identiteta. Silo model nije interoperabilan i manjkav je u mnogim aspektima kao što je visoka cijena održavanja servisa, korisnička preopterećenost sa brojnim identitetima i lozinkama, itd. [70]. To je razlog zašto se pojavljuju i drugi modeli menadžmenta identiteta koji su veoma cijenjeni u organizacionim sistemima.

4.4.2. Centralizovana Arhitektura

Centralizovana arhitektura je relativno jednostavna arhitektura menadžmenta identiteta koja centralizuje digitalne identitete. Prosto rečeno, u centralizovanoj arhitekturi digitalni identiteti su pohranjeni u centralnoj bazi podataka u kojoj korisnik nema

nikakvu korisničku kontrolu. U ovoj arhitekturi postoji jedan IP korišćen za sve identitete servis provajdera. SP je obavezan da obezbijedi svaki identitet prema IP-u. Ova arhitektura odvaja ulogu SP-a i IP-a koji mogu biti nezavisni entiteti. Odvojeni identiteti služe kao ekskluzivni korisnički kredencijali koji snadbijevaju sve SP-e. Dakle, u ovom okruženju korisnici mogu imati pristup svim SP-a koristeći isti skup identifikatora i kredencijala. Centralizovani sertifikati – CA (*engl. centrlized certificate*) mogu biti implementirani sa Javnim ključevima infrastrukture – PKI (*engl. public key infrastructure*) ili Jednostavnim javnim ključevima infrastrukture – SPKI (*engl. simple public key infrastructure)* [82].

Ova arhitektura je veoma efikasna u područjima u kojima korisnici mogu biti identifikovani kontrolisanjem e-mejl adrese. Iako, ovakva arhitektura izgleda skalabilna, problem je usredsređen na zaštiti privatnosti informacija, što uzrokuje mnoge poteškoće u pojmovima njenog društvenog prihvatanja [83]. U centralizovanoj IAM arhitekturi Mikrosoftov Pasoš je centralizovan sistem potpuno kontrolisan od strane Mikrosofta i u bliskoj je vezi sa drugim Mikrosoftovim proizvodima. Međutim, ova arhitektura ima suštinske nedostatke, kao što su jedinstvena tačka centralizacije digitalnih identiteta u IP-u čime se i stvara krug nepovjerenja. Upravo, to predstavlja osnovni razlog neuspješnosti mikrosoftovog pasoša.

4.4.3. Federativna Arhitektura

U federativnom modelu, digitalni identiteti su distribuirani širom različitih IP-a koji čine krug povjerenja – CoT (*engl. circle of trust*). Skup SP-a u federativnoj arhitekturi slijedi dogovor o međusobnoj zaštiti i autentifikaciji dopuštajući SSO efekat. Ova arhitektura kombinuje SSO i autorizacione alate koristeći brojne zajedničke SP tehnologije i standarde. Sa ovim postupcima čini se lakšim prepoznavanje i pravo pristupa korisničkih identiteta od drugih SP-a. Suštinska razlika između sistema federativnog identiteta i centralizovanog upravljanja identitetima je da ne postoje pojedinačni entiteti koji djeluju u sistemu upravljanja identitetima. U ovom modelu isti identifikatori i kredencijali su korišćeni za svaki SP. Mogućnost da sistem radi čak ako SP i IP nisu iz istog bezbjednosnog domena čini glavnu prednost ovog federativnog područja. Takođe, prednost ove arhitekture je što ona omogućava balans između održavanja kontrole prava privatnosti i kontrole identiteta uz istovremeno omogućavanje lakšeg i bržeg korisničkog pristupa resursima.

Ova arhitektura omogoćava snažnu krajnje korisničku kontrolu nad identitetom informacija koje su dijeljene unutar federativnog područja. Sa druge strane, nedostatak ove arhitekture je korisničko oskudijevanje po pitanju privatnosti i narušavanja anonimnosti. Takođe, nedostatak je skalabilnost korisnika jer pri autentifikaciji korisnici imaju pristup mrežama iz različitih područja prema njihovim povezanim IP. Stoga, problem lozinki prenosi se i preko višestrukih federativnih područja.

4.4.4. Korisničko-Orijentisana Arhitektura

Ne postoji jedinstvena definicija ali u ovom radu je usvojena prema [70]: *"korisničko - orijentisani menadžment identiteta je razumljiv u značenju arhitektura digitalnog identiteta gdje pojedinac krajnji korisnik ima suštinsku nezavisnu kontrolu nad širenjem i upotrebom svojih identifikatora i personalnih informacija"*. Dakle, korisničko-orijentisana arhitektura korisniku uvijek ostavlja u vlasništvu njegove personalne informacije. Na taj način korisniku se omogućava puna kontrola nad njegovim identitetima. Upravo, ideja da korisnik veb servisa treba da ima punu kontrolu nad svojim informacijama o identitetu predstavlja jedan od fundamentalnih principa korisničko – orijentisane arhitekture. Svrha ove arhitekture je da informiše korisnika o prikupljenim informacijama i garantuje saglasnost za bilo koji tip manipulisanja prikupljenim informacijama. Pored toga, korisničko-orijentisana arhitektura omogućava korisniku sticanje anonimnog pristupa jer korisnici zadržavaju punu kontrolu nad svojim digitalnim identitetima. Anonimnost treba da bude garantovana na aplikativnom i mrežnom nivou. Puna anonimnost i nemogućnost nepovezivanja mogu voditi ka povećanoj zloupotrebi anonimnih korisnika. U tom slučaju, alternativa je upotreba pseudonima npr. u e-trgovini. Može se zaključiti, da gore pomenuti tradicionalni modeli imaju specifične karakteristike kao što su privatnost, povjerenje, korisnička kontrola, skalabilnost i dr. koje im daju prednosti odnosno nedostatke u međusobnom poređenju. Upravo, korisničko-orijentisana arhitektura je i uvedena kako bi se riješila neka od gore pomenutih pitanja.

Mnoge tehnološke diskusije i rješenja su fokusirani na SP-e, a rijetko na korisničku perspektivu. Paradigma korisničko-orijentisanog identiteta je stvarna evolucija jer se IT arhitektura kreće u pravcu korisnika sa sljedećim prednostima [70]:

- Osposobljavanje korisnika da ima potpunu kontrolu nad svojom privatnošću,

- Upotrebljivost, korisnici upotrebljavaju iste identitete za svaku sesiju identiteta,
- Konzistentna korisnička iskustva, zahvalna za jednolikost identiteta interfejsa,
- Ograničavanje napada na identitete, kao što je fišing,
- Ograničavanje u dosezanju poremećaja, kao što je spam,
- Pregledanju politika na obe strane, IP-i i SP-i (veb strane), kada je potrebno,
- Velike skalabilne prednosti, pošto IP ne treba nikakvo prethodno saznanje o SP-u.
- Osiguravaju bolje uslove zaštite pri izmjeni podataka,
- Razdvajaju digitalne identitete od aplikacija,
- Pluralizam operacija i tehnologija.

4.5. Uloga i odgovornost IAM

Uloga i odgovornost IAM je višestruko značajna u današnjem digitalnom svijetu, posebno ako se imaju na umu sve prijetnje kojima su izloženi učesnici u IAM-u. Kao što su prethodno već definisani mnogi pojmovi menadžmenta identiteta, važno je pomenuti da subjekat kroz različite komunikacijske kanale pruža svom sagovorniku određeni skup informacija o sebi koji su tokom vremena promjenjivi. Upravo u tom kontekstu posmatranja proizlazi i ključna uloga IAM, da *pravi* korisnik u *pravo* vrijeme pristupi *pravom* resursu za *prave* razloge (4P). Ovo je posebno značajno za bezbjedno poslovanje velikih sistema koje je veoma teško i fizički predstaviti. U e-poslovanju, od organizacija se zahtijeva spremnost i sposobnost da se na veoma brz, jednostavan, jeftin i transparentan način odobri autentifikacioni pristup korisniku. Pristup, pored toga što treba da bude samoposlužujući zasnovan na korisničkom imenu i lozinki, treba i da bude praćen drugim pravima pristupa koja treba da budu praktična za interno i eksterno upravljanje. Eksterni pristup obično dolazi od nezaposlenih, kao što su kupci, prodavci, preduzetnici, poslovni partneri ili dobavljači. Održavanje sigurnosti i integriteta svih unutrašnjih sistema predstavlja izazov za organizacije, dok one omogućavaju eksterni pristup aplikacijama u svom unutrašnjem povjerljivom okruženju. Dakle, izazov je usmjeren na organizacije koje autentifikuju korisnike izvan svog područja. Da bi organizacije kapitalizovale na poslovnom potencijalu koje pruža poslovanje izvan granica, organizacije treba da budu u stanju da imaju povjerenje u e-identitete sa kojim se preko interneta pristupa njihovim veb aplikacijama.

Pored svega navedenog, u ovom radu su izdiferencirane odgovornosti koje IAM ima u organizacijama, kao što je:

- odgovornost u boljem upravljanju digitalnim identitetima,
- odgovornost u autorizaciji korisničkog pristupa, tj. omogućava autorizovanim korisnicima da pristupe određenim servisima, aplikacijama i informacijama obezbjeđujući time zaštitu od neovlašćenog pristupa,
- odgovornost u transparentnom, učinkovitom i fleksibilnijem funkcionisanju cijelog sistema uz obezbjeđivanje cjelovite bezbjednosne arhitekture,
- odgovornost u redukovanju nepotrebnih kadrova, administrativnih troškova, vremena i resursa,
- odgovornost u optimizaciji poslovnih procesa čime se poboljšavaju servisni nivoi,
- odgovornost u izgradnji većeg povjerenja po pitanju identiteta,
- odgovornost u pravovremnom pristupu resursima,
- odgovornost u smanjenju rizika od moguće krađe informacija, i sl.

V METODE AUTENTIFIKACIJE

5.1. Uvod u metode autentifikacije

Kako su informacione tehnologije (IT) evoluirale tokom godina, time su postojeće metode autentifikacije značajno poboljšane i unapređene u cilju prilagođavanja narastajućim prijetnjama i ranjivostima sistema. Potreba za metodama autentifikacija, kao jedan od najvažnijih koraka u bezbjednosti informacionih sistema, proizilazi iz činjenice da svaki sistem ili organizacija u svom funkcionisanju jednostavno treba da razlikuju korisnike. U cilju bolje zaštite informacionih sistema razvijen je veliki broj raznovrsnih metoda autentifikacija koje omogućavaju verifikovanje korisnika u sistemu. Metod autentifikacije je vrlo složen metod i obuhvata nekoliko naučnih područja kao što je to opisano u prethodnom poglavlju ove disertacije. Upotreba metoda autentifikacija se zasniva na korišćenju pojedinačnih autentifikacionih faktora ili njihovom kombinovanju. Potrebno je naglasiti da nijedna metoda autentifikacije nije idealna i ne omogućava apsolutnu zaštitu. Mnoge organizacije se oslanjaju na standardnu metodu autentifikacije (korisničko ime i lozinku) unutar svog okruženja zaštite, dok druge nastoje implementirati jake metode autentifikacije. U poslednje vrijeme, napredak mobilnih tehnologija je učinio mogućim upotrebu gotovo svih metoda autentifikacija koje su doskoro smatrane isključivom privilegijom za upotrebu PC/laptop tehnologija. U nastavku poglavlja opisane su opšte metode autentifikacija.

5.2. Autentifikacija korišćenjem lozinke

Lozinka ili pasvord spada u opšte tradicionalne metode autentifikacije zasnovane na autentifikacionom faktoru korisnika "nešto što zna". Čini je niz karaktera koji treba da budu različiti za svakog korisnika i visoko zaštićeni. Postupak autentifikacije metodom lozinke zasniva se na dokazivanju korisničkog identiteta. Sam proces dokazivanja korisničkog identiteta sastoji se u upoređivanju lozinke sa postojećim šablonom na osnovu čega se vrši njeno verifikovanje ili odbacivanje. Da bi se ostvarila autentifikacija putem ove metode potrebno je podijeliti znanje o tajnosti lozinke između korisnika i sistema. Sam proces dijeljenja lozinke odvija se prilikom otvaranja korisničkog naloga na sistemu neposredno pri odabiru lozinke. U literaturi se može

pronaći da se za lozinku koristi opšti termin *passcodes* koji uključuje PIN, tekstualne i druge grafičke lozinke [84]. Lozinka spada u najpopularniju i najčešće korišćenu metodu i pored toga što pruža najniži nivo zaštite. Popularnost je u tome što korisnik ”nešto što zna” je daleko prihvatljivije za samog korisnika u poređenju sa ostala dva autentifikaciona faktora “nešto što ima” i “nešto što jeste”. U prilog tome idu i činjenice da kao lozinka mogu poslužiti mnogi identifikatori poput PIN-a, broj za ATM (*engl.automated teller machine*) karticu, datum rođenja, vozačka dozvola, i sl. Razlikujemo dva osnovna tipa lozinki statičke (fiksne) i dinamičke (jednokratne). U statičke lozinke ubrajamo tekstualne (PIN), vizuelne i grafičke. Dinamičke lozinke su lozinke koje genrišu token uređaji i detaljnije će biti opisane u token metodi.

Lozinka je metod autentifikacije zasnovan na ljudskim sposobnostima da zapamte određenu jedinstvenu kombinaciju alfabeta ili numeričkih znakova (alfanumerički lozinka) ili da selektuje predodređenu sliku na vizuelnom displeju (grafička lozinka). Uzimajući u obzir ograničene ljudske sposobnosti pamćenja ovaj metod autentifikacije se svrstava u najnebezbjednije mehanizme u poređenju sa svim ostalim metodama autentifikacija. Svakako, da veća upotreba lozinki i sposobnost ljudskog pamćenja su ograničavajući faktori koji često korisnika iz praktičnih razloga naginju na upotrebu prostih lozinki. Oko 81% korisnika bira prostije lozinke koje su mnogo osjetljivije na napade riječnikom [85]. Takođe, korisnici koji imaju više naloga pribjegavaju korišćenju iste lozinke za višestruke naloge. Neophodno je istaći da jake lozinke primoravaju korisnika na zapisivanje poput ljepljivog podsjetnika koji lijepe na vidnim mjestima, a iste mogu biti kompromitovane ili izložene drugim metodama napada poput napad grubom silom.

Takođe, primjena ovog metoda u mobilnim autentifikacijama spada u nezgrapnu metodu. Brojni su dobro poznati nedostaci ovog mobilnog metoda autentifikacije u kojem prednjači teška pamtljvost i laka pogodljivost [86], česta upotrebljivost korišćenih lozinki [87], inficiranost malicioznim programima mobilnih uređaja ili surfujuće rame [84], poteškoće pri unošenju precizne lozinke na malom ekranu osjetljivom na dodir, pogrešan unos lozinke može rezultirati zaključavanjem naloga koji zahtijeva da bude resetovan oslanjajući se na alternative, te unošenje brojeva i alfanumeričkih simbola što zahtijeva promjenu tastature [88]. Takođe, ovaj metod ima slabosti u pogledu pohranjivanja kredencijala, čak i u slučajevima kada su kredencijali zaštićeni putem enkripcije ili nekog drugog oblika prikrivanja.

Nasuprot nedostacima, posljednjih nekoliko godina zbog svoje jednostavnosti tekstualne lozinke su bile najčešće korišćeni korisnički metod autentifikacije [89]. Prednosti ovog metoda koja ga izdvaja u odnosu na sve druge metode autentifikacije su cijena (besplatni), praktičnost i pogodnost. Praktičnost lozinke ogleda se u jednostavnoj primjeni i održavanju. Mnogo su pogodnije za resetovanje kompromitovanih lozinki nego npr. u slučajevima obezbjeđivanja i konfigurisanja novih pametnih kartica. Sa resetovanjem kompromitovanih lozinki značajno se smanjuje rad sistema administratora u izdavanju novih lozinki. U slučaju kompromitovanja lozinke su zamjenljive i lake za resetovanje.

Kvalitetan odabir i česta izmjena lozinki značajno doprinosi odvraćanju od napada na lozinke. U psihologiji je poznata činjenica da čovjek sa svojim kognitivnim sposobnostima izuzetno sporo i nepouzdano obrađuje i pamti nasumične nizove alfanumeričkih znakova i simbola. Mnogo lakše pamte nizove alfanumeričkih znakova i simbola ukoliko ih oni mogu asocirati na neko poznato značenje ili događaj. Neki sistemi koriste lozinke koje se isključivo sastoje od brojeva kao što su kreditne i SIM (*engl. subscriber identity module*) kartice.

Da se ne bi ionako nizak nivo zaštite metod autentifikacije lozinkom urušio, a time i opšta bezbjednost sistema degradirala, u ovom radu su date smjernice koje je potrebno koristiti pri izboru i upravljanju sa lozinkama:

- preferirati odabir kompleksnih, kvalitetnih i nasumičnih lozinki,
- lozinke treba da budu duže (minimum 8 karaktera) i raznolike sa upotrebom kombinacijom malih i velikih slova, alfanumeričkih znakova i simbola,
- lozinke ne bi trebalo da sadrže trivijalne riječi, nazive i sl.
- potrebno je izbjegavati upotrebu istih lozinki, njihovog dijeljenja sa drugim korisnicima, i ne ostavljati ih na vidnim mjestima,
- postupak unošenja lozinki u sistem treba činiti na diskretan način,
- prilikom udaljavanja od računara korisnici su obavezni da se odjave sa naloga,
- redovno primjenjivati promjenu lozinki,
- potrebno je izbjegavati pohranjivanje lozinki u izvornom obliku kao otvoren tekst, već to raditi u nekoj formi šifrata,
- koristiti programske alate za provjeru odabira kvaliteta korisničkih lozinki,
- redovno brisati poštu u kojoj je pohranjen sadržaj ili fajl lozinke,

- podestiti sisteme na ograničen broj neuspješnih logovanja,
- precizne provjere logovanja treba da u svojim procesima održavanja sadrže informacije o svakom pokušaju logovanja, datum, vrijeme, korisnički ID i pristupno mjesto.
- serveri u kojima su pohranjene lozinke treba da imaju ograničen fizički i logički pristup sa visokim nivom zaštite.

Danas postoje različite aplikacije za automatsko stvaranje jake lozinke. Primjer je generator za stvaranje jake lozinke [90]. S druge strane, zbog značaja i vrijednost koju imaju lozinke, brojni programi su razvijeni za njihovo otkrivanje i kompromitovanje. Postoje tri opšta tipa napada koji se koriste prema lozinkama:

- Napadi prisluškivanjem, poznatiji kao napad čovjek u sredini – MITM (*engl. man – in – the – middle*),
- Napadi društvenim inženjeringom,
- Napadi pogađanjem:
  - *napadi rječnikom (engl. dictionary attacks),* izvršavaju se putem softverskih alata koji sadrže stotine ili hiljade riječi koji su najčešće birane kao lozinke. Napadač obično uhvati sažetu lozinku ili fajl od lozinke, i alat tada vrši poređenje svake riječi koja je prethodno unijeta sa presretnutom riječi sve dok se ne izvrši njeno otkrivanje. Napad rječnikom zasniva se na upotrebi unaprijed proizvedenog rječnika pretpostavljenih lozinki. Ovaj oblik napada je veoma uspješan u slučajevima korisničkog odabira slabih lozinki (kraće dužine). Korišćenjem metode zaslanjivanja (*engl. salt*) vrši se dodavanjem nasumičnog niza znakova ispred lozinke prije nego što se izvede njen sažetak čime se otežava njeno otkrivanje.
  - *napadi grubom silom ili iscrpljivanjem (engl. bruto force),* izvršava se putem softverskih alata tako da napadač pokušava isprobati sve moguće kombinacije svakog izabranog karaktera ili niza karaktera sve dok lozinku ne otkrije. Ukoliko žrtva koristi dužu i kompleksniju lozinku ovaj tip napada je veoma spor i zamoran pa se zato i često naziva *iscrpljujući* napad. Za razliku od napada rječnikom koji koristi dugu listu riječi, napad grubom silom je vremenski orijentisan u procesu otkrivanja lozinke. Zahvaljujući velikoj procesnoj moći današnjih računara uspješnost napada grubom silom je u značajnom porastu.

Programi napadi rječnikom i grubom silom ne koriste se samo od strane napadača, već ih koriste i sistem administratori u rekonstrukciji zaboravljenih lozinki ili testiranju postojećih lozinki. Međutim, ovaj pristup testiranja lozinki ima i lošu stranu bezbjednosne politike. Ukoliko korisnik može da otkrije zaboravljenu lozinku samim tim i napadač može to isto učiniti obzirom da koriste iste programske alate. Prema [91] deset najpopularnijih softverskih alata za otkrivanje lozinki su *brutus, rainbowcrack, wfuzz, cain and abel, john the ripper, thc hydra, medusa, ophcrack, crackfinder, l0phtcrack i aircrack-ng.*

5.2.1. Autentifikacija korišćenjem personalnog identifikacionog broja – PIN

Personalni identifikacioni broj – PIN je broj koji je najčešće korišćen u mobilnom metodu autentifikacije u postupku zaključavanja mobilnih uređaja. Predstavlja prvi i osnovni sloj zaštite personalnih informacija pohranjenih na SIM kartici mobilnog uređaja. Opšta varijanta se sastoji najčešće iz 4-digitalna koda ili 4 cifre koja se unose putem tastature. Dužina od 4-digitalna koda spada u proste lozinke koje predstavljaju lak plijen za napade grubom silom i napade rječnkom, ali u mobilnom metodu autentifikacije su gotovo neupotrebljivi. Naime, nekoliko pogrešnih pokušaja pristupa na mobilnom uređaju uzrokovaće automatsko zaključavanje kartice čineći je potpuno beskorisnom. Prema *Clarke-u* and *Furnell-u* [92] trenutna upotreba autentifikacije zasnovana na PIN-u je problematična i oni navode da su ispitanička mišljenja u pogledu budućih zaštitnih opcija interesantna, u kojem su korisnici sa 83% voljni da prihvate neki oblik biometrijske autentifikacije na svojim uređajima.

5.2.2. Autentifikacija korišćenjem vizuelne lozinke

Metod autentifikacije vizuelne lozinke zasniva se na autentifikaciji korisničke lozinke u formi slike. Ovaj metod nudi korisniku niz slika za odabir. Korisnik mnogo lakše pamti sliku nego niz alfanumeričkih karaktera i simbola. Vizuelne i grafičke lozinke u poređenju sa tekstualnim lozinkama imaju određene prednosti i nedostatke. Prednosti su u smislu lakšeg pamćenja lozinke jer su nezavisne o jeziku govora, a računari veoma teško raspoznaju slikovne podatke čime je otežano automatsko otkrivanje. Prednosti ovog metoda u mobilnom autentifikacionom pristupu u odnosu na PIN i tekstualne lozinke je što ne prisiljavaju korisnika da ukucava lozinku na maloj tastaturi mobilnog uređaja. Sa druge strane, nedostaci ovog metoda su u upravljanju sa slikama koji se

manifestuju u nemogućnosti skrivanja slika jer se one upravo i oslanjaju na korisničkom prepoznavanju, te načinu i prostoru pohranjivanja u sistemu i njihovom generisanju pri svakom autentifikovanju. Napadač vizuelnim pristupom korisničkog ekrana može otkriti lozinku. Postoje određene metode koje ublažavaju te ranjivosti u vidu kombinovanja slika i njihovih pozicija. Za razliku od vizuelnih, većina sistema ne prikazuje tekstualne lozinke prilikom unosa. Na primjer *Unix/Linux* sistemi ne prikazuju ništa dok se na veb formama prikazuju samo zvijezdice umjesto stvarnih znakova.

5.2.3. Autentifikacija korišćenjem grafičke lozinke

Autentifikacija korišćenjem grafičke lozinke zasniva se na korišćenju slika koje korisnik samostalno nacrta. Za razliku od vizualne lozinke u kojoj se korisniku nudi niz slika za odabir, kod grafičke lozinke korisnik mora nacrtati određenu sliku koja predstavlja njegovu lozinku. Osnovna karakteristika ovog metoda autentifikacije je da se površina na kojoj se crta slika dijeli u određena polja koja čine matricu. Osnovni princip ovog matričnog pristupa je usmjeren na prepoznavanju polja u kojem korisnik crta, a ne na sliku. Prema tome, suštinu grafičke lozinke čini niz korisničkih prolaza kroz određena polja na površini za crtanje. Time se korisniku olakšava da slika koju crta ne treba da bude identična, čak ni slična izvornoj da bi se mogao autentifikovati.

Vrlo važan elemenat u ovom procesu autentifikacije je upotreba jednosmjernih funkcija za procese pohranjivanja zapisa lozinki. Jednosmjerne funkcije sažimaju korisnički zapis koji se potom upoređuje sa šablonom i ukoliko se poklapaju korisnik je autentifikovan. Metod autentifikacije je poptpuno sličan tekstualnim lozinkama, s tim što se ovakav dobijeni niz znakova (crtanjem slike) mnogo lakše pamti. Složenost grafičke lozinke direktno je u zavisnosti od izabranog broja polja u matrici. Što je matrica većeg reda to je i sama složenost lozinke veća.

Različite grafičke lozinke su predložene kao dio mobilnog autentifikacionog rješenja za savladavanje nedostataka prethodno pomenutih tekstualnih lozinki [93]. Povrh toga, upotreba grafičke lozinke čini mnoge korisnike mnogo zadovoljnijim [94]. Mana ovog metoda autentifikacije se manifestuje kroz korisničke nacrtane znakove koji imaju predvidljiv karakter i koji su simetrični, što čini pogodnim za njeno otkrivanje napad rječnikom.

5.3. Autentifikacija korišćenjem tokena

Token je fizički mali uređaj veličine kućnih ključeva, i predstavlja drugi autentifikacioni faktor nešto što korisnik ima. Zasniva se na korišćenju posebnog uređaja koji generiše *pass-code* poznat pod nazivom dinamična lozinka. Uključuju se direktno u kompjuterske uređaje i time eliminišu dodatne hardvere. Na samom token uređaju nalazi se programska podrška i svi podaci koji su potrebni za korisničku autentifikaciju. Token može biti bilo koji hardver ili softver koji se koristi u autentifikacione i autorizacione svrhe. U poređenju sa lozinkom, token metod spada u bezbjednije autentifikacione mehanizme. Međutim, sama upotreba tokena ne obezbijeđuje viši nivo zaštite u procesima autentifikacije. Ovaj metod se gotovo uvijek koristi u kombinaciji sa drugim metodama autentifikacije koji su dio višestrukog autentifikacionog mehanizma. Najveća primjena tokena je u poslovnom okruženju.

Token za generisanje lozinki je program koji pokreće procesor u izvršavanju *one time pasword* – OTP algoritma sa ciljem generisanja PIN-a promjenjivog u vremenu. Osnovni koncept dinamičkih lozinki je da odobri lični identitet na osnovu jedinstvenog generatora ključa ili lozinke. Dinamičnu lozinku čini skup nasumičnih karaktera izloženih na malom ekranu tokena. Mogu biti jednom i samo jednom korišćeni za dokaz korisničkog identiteta. Za svaki pojedinačni pristup zahtijeva se generisanje nove lozinke. Nakon upotrebe, lozinka je potpuno beskorisna jer nije više prihvatljiva za proces autentifikacije. Na taj način onemogućava se uzastopna upotreba iste lozinke dva ili više puta. Ovo svojstvo dinamičke lozinke omogućava diskreditaciju napadača koji posjeduje takvu lozinku. Time se i uveliko smanjuju ranjivosti sistema od strane napadača i tehnika poput snifovanja mrežnog saobraćaja.

Proces autentifikacije zasnovan na tokenu započinje nakon što korisnik priključi USB uređaj u računar. Sa identifikovanjem USB uređaja, računar zahtijeva od korisnika brzo unošenje lozinke (drugi autentifikacioni faktor) za sticanje pristupa računarskom sistemu. Zavisno od nivoa bezbjednosti koji se želi postići, poslije očitavanja USB uređaja u nekim slučajevima se traži dodatna autentifikacija putem lozinke (prvi autentifikacioni faktor). Za svaki zahtijevani pristup resursima, zaštitni softver ili hardver na osnovu dinamičkih lozinki stvorenih od strane token uređaja izračunavaju nasumični niz. Ukoliko se dva broja podudaraju zaštitni sistem odobrava pojedinačni

pristup. Karakteristično za tokene uređaje je da generišu novu lozinku svakih n sekundi na primjer 30 ili 60 sekundi. Osim lozinke, USB token ima sposobnost da pohranjuju biometrijske informacije i digitalne sertifikate koji mogu biti korišćeni u okruženju infrastrukture javnog ključa. Token uređaji u vidu upotrebe dinamičkih lozinki predstavljaju alternativu fiksnim lozinkama koje nude slabu zaštitu u kontroli pristupa računarskih resursa.

Za metodu autentifikacije dinamičkom lozinkom, sistemi upravljanja pristupom sadrže baze podataka sa tipom tokena u koji su pohranjeni jedinstveno određeni ili kriptografski ključevi za svakog korisnika. Ukoliko je korisnički token izgubljen ili ukraden, korisnik ne može pristupiti sistemu i potrebno je da kontaktira sistem administratora koji jednostavno obriše informacije na prethodnom tokenu i korisniku da novi token sa novim podacima. Na taj način se sprečava neautorizovana upotreba tokena. Takođe, većina sistema koristi PIN za aktiviranje tokena čime se dodaje dodatni sloj zaštite, a neki tokeni izdaju i određena upozorenja.

Token uređaji su pogodni za nošenje, jednostavni za upotrebu, teški za dupliranje i veoma otporni. Pored navedenih prednosti token uređaje karakterišu lozinke sa čestim internim promjenama i relativno kratkim vremenskim periodom života. Lozinke generisane token uređajem su daleko bezbjednije zbog vremenske osjetljivosti i sinhronizovane prirode u procesu autentifikacije. Time se suštinski doprinosi njenoj tajnosti i eventualnoj mogućnosti otkrivanja. Nasumični, nepredvidljivi i jedinstveni niz generisanih brojeva značajno otežavaju njeno otkrivanje od strane sajber napadača. Takođe, jednokratnost generisanih lozinki je višestruko korisno svojstvo koje ne zahtijeva od korisnika da je pamti ili memoriše, te čini je potpuno beskorisnom nakon upotrebe. Ukoliko se koristi u kombinaciji sa drugim prenosivim uređajima token ima određene prednosti kao i slabosti. Prednosti su perfektna zaštita zbog vremenske sesije na uređaju, a slabost je pružena zaštita koja može imati veoma nizak nivo. Ako token nije u blizini uređaja, sesije mogu biti prekinute čime se onemogućava napadačima pristup osjetljivim informacijama. Hardverski autentifikacioni tokeni imaju značajne prednosti u odnosu na druge metode autentifikacije u vidu zadovoljavajućih ograničenih obuka, nisku stopu greške i visoka svojstva memorisanja.

Nasuprot prednostima, mane ovog metoda su visoka ranjivost prema krađi, oštećenjima ili gubljenju, te visoka uključenost bežične infrastrukture za slanje lozinki prema

tokenima. Takođe, ovaj metod autentifikacije zahtijeva određena investiciona ulaganja, kao što su nabavka, zamjena tokena (vijek trajanja token uređaja je obično 4-5 godina) i troškovi održavanja cjelokupnog sistema. Posebno to ima na značaju kada jedan korisnik ima više naloga i u većini slučajeva dodjeljuje se hardverski token za svaki nalog. Povrh toga, u slučaju oštećenja, krađe ili gubljenja tokena oganizacije poput banaka su dužne korisnicima obezbijediti nove, što čini veoma skup korak u odnosu na zamjenu npr. ATM kartice ili resetovanja lozinke. Pored toga, organizacije su dužne obezbijediti podršku korisnicima u vidu kontinuirane obuke upotrebe token uređaja.

U mobilnom metodu autentifikacije token predstavlja sam mobilni uređaj. Glavni razlog za upotrebu mobilnih uređaja poput mobilnog telefona kao autentifikacionog tokena su hardverska i softverska infrastruktura koja dopušta automatizaciju procesa autentifikacije. Ovaj metod obezbijeđuje viši nivo zaštite u poređenju prema prethodnim metodama. Mobilni uređaji imaju nekoliko prednosti koje mogu biti eksploatisane u metodama autentifikacije. Prednosti su u značajnom smanjenju cijene proizvoda i održavanja token uređaja koji mogu biti teret za korisnike i organizacije. Takođe, korisnici mobilnih uređaja svakodnevno vode brigu o samim uređajima. Pored navedenog, mobilni uređaji koriste višestruke komunikacione kanale i tako dodatno povećavaju nivoe zaštite u područjima autentifikacija. Jedan od tih komunikacionih kanala je izgrađen u standardu za mobilnu telefoniju GSM što mobilni telefon čini dobrim zaštitnim mehanizmom. Na taj način napadač da bi uspio u svojim namjerama potrebno je da ima potpunu kontrolu svih komunikacionih kanala. Nasuprot prednostima, nedostatak ovog metoda su visoka ranjivost prema krađi i potencijalnom pozajmljivanju, oštećenju, inficiranju, kompromitovanju ili gubljenju. Takođe, mane su u tehničkim ograničenjima u procesnoj sposobnosti i moći, memoriji i veličini ekrana, metodi unosa podataka, različitim displej rezolucijama i kontrastima, vijeku baterije kao i mrežnim perfomansama.

U mobilnom metodu autentifikacije token predstavlja bilo koji fizički uređaj (uključujući i mobilne uređaje) koji obezbijeđuje jedan od faktora autentifikacije (nešto što imaš). U ovom metodu za proces autentifikacije mogu se koristiti hardverski i softverski tokeni. Hardverski token izvršava autentifikaciju putem metoda *SMS – one time password (OTP).* Na SIM kartici mobilnog uređaja – token (mobilni telefon) mogu biti pohranjeni kriptografski ili biometrijski ključevi. Mobilni softverski token zahtijeva

od korisnika da instalira na mobilnom uređaju softver koji stvara lozinku za autentifikaciju – metod OTP upotrebljavajući SMS.

5.3.1. Autentifikacija korišćenjem jednokratne šifre *(engl. A one time pasword – OTP)*

A one time pasword – OTP je lozinka koja je upotrebljiva samo za jednu autentifikaciju. Ovaj metod predstavlja jednofaktorski mobilni metod autentifikacije čija upotreba zasnovana na jednom od tri moguća autentifikaciona faktora koja korisnik stvara na mobilnom uređaju bez konekcije korisnik – softver. Kao što je prethodno pomenuto, mobilni uređaj služi kao token i koristi određene kredencijale da stvori lokalni OTP (na svom mobilnom uređaju). Da bi server djelovao sinhronizovano i izvršio komparaciju lozinki dostavljenih od strane korisnika neophodno je da oba od njih imaju algoritam i potrebne parametre koji generišu lozinka za autentifikaciju – OTP vrijednost. Lozinku korisnik može podnijeti onlajn ili putem uređaja kao što je ATM mašina. Dakle, primjena OTP metoda u okviru aplikacija je skoro uvijek 2FA. Prednost ovog metoda je da može biti primjenjen na bilo kom mobilnom uređaju i nije zavisan od mrežnog operatera.

5.3.2. A one time pasword – OTP korišćenjem SMS

A one time pasword – OTP korišćenjem SMS je dvofaktorski mobilni metod autentifikacije u kojem korisnik zahtijeva od servera da generiše vrijednost OTP. Ovaj metod zasniva se na principu da korisnik putem SMS poruke šalje serveru svoje kredencijale. Server provjerava sadržaj SMS poruke i ukoliko je potvrđena ispravnost, na bazi tih kredencijala generše OTP koji odmah putem poruke vraća korisniku. Takođe, korisniku se ostavlja dovoljno vremena za upotrebu OTP prije njenog isteka. Lozinka ovog tipa je prilično kratka, vremenski ograničena samo za jednu sesiju. Nedostaci ovog metoda su što imaju ograničenu entropiju, mogu biti opservirani ili presretnuti, ostaju validni samo kratki vremenski period [93], i zahtijevaju plaćanje SMS usluga kako za SP-e tako i za korisnke. Postoji nedostatak u pogledu hardverskih ograničenja mobilnih telefona jer mnogi posebno stari mobilni telefoni ne podržavaju pokretanje više aplikacija u isto vrijeme. Prosto rečeno, mobilni telefon ne podržava istovremeno slanje poruke i mogućnost da ima otvorenu aplikaciju veb pretraživača, što ukazuje da zatvoren veb pretraživač čini beskorisnim SMS.

Najvažnije prednosti ovog metoda su dostupnost praktično za svakoga, nenarušavanje privatnosti, i ne zahtijeva dodatni hardver ili instaliranje softvera čak i pri promjeni SIM kartice. Takođe, ne zahtijeva primjenu novih tehnogija kao što su pametne tehnologije. Iz korisničke perspektive, ovaj metod je veoma jednostavan i lak za razumijevanje. Upotreba ovog metoda autentifikacije je alternativa ukoliko server i korisnik ne djeluju sinhronizovano. Ovaj metod autentifikacije je posebno popularan u sistemima, kao što je e-bankarstvo.

5.3.3. Režimi token operacija

Dva opšta režima token operacija su sinhronizovani i asinhronizovani. U asinhronizovanom modu, softver upravljanja pristupom izdaje inicirajući otvoreni tekst prema korisniku koji je izložen na ekranu terminala ili radne jedinice. Korisnik aktivira generator lozinke, unosi PIN, i zatim inicirajući otvoreni tekst čime aktivira ključ koji generiše token odgovor izložen na displeju. Sa druge strane, u zaštićenim računarskim sistemima softver upravljanja pristupom prepoznaje jedinstvene nizove (šifrovane algoritme) dodijeljene od strane korisnika, pomoću kojih može izračunati očekivani odgovor. Ukoliko se ta dva odgovora podudaraju korisniku je odobren pristup. U sinhronizovanom modu, softver upravljanja pristupom zahtijeva lozinku bez izračunavanja i prezentovanja inicirajućeg teksta prema korisniku. Korisnik pokreće generator lozinke, unosi PIN i čita odgovor na displeju. Održavanje lozinki sinhronizacijom je ključni faktor u sinhronizaciji tokena. Svaki put nakon upotrebe asihroni tokeni su resinhronizovani, jer sistem upravljanja pristupom izdaje novi zahtjev za svaku sljedeću upotrebu. Svaki novi zahtjev za sinhronizovani token suštinski predstavlja njihov sopstveni izazov dok sistem upravljanja pristupom treba da bude u stanju da odredi šta je izazov.

Režim token operacije u sinhronizovanom modu djeluje u sinhronizovanom vremenu, uključujući upotrebu vremena i drugih faktora (korišćenjem sata u tokenu i u sistemu upravljanja pristupom, kao i mogućnost satnog pomjeranja). Dakle, slučaj sinhronizacije uključuje vrijednost razvijenu od jednokratne modifikacije od posljednjeg ulaza dok algoritamska sinhronizacija uključuje suprotne tehnike odgovora u određivanju da li specifični tokeni mogu generisati taj odgovor. Kao i kod asinhronog režima, ukoliko se podudaraju dva odgovora tada je korisniku odobren pristup.

5.4. *PKI*

Infrastruktura javnog ključa – PKI (*engl. public key infrastructure*) je složena infrastruktura koja obuhvata skup kompleksnih tehnologija zasnovanih na korišćenju para kriptografskih ključeva. PKI spada u drugi metod autentifikacije sa kojim se obezbijeđuje viši nivo zaštite. Autentifikaciono rješenje zasnovano na PKI rješenju omogućava bolju zaštitu i efektivniju primjenu PKI kroz organizacije povećavajući zaštitu digitalnih resursa, upravljajući sa autentifikatorima i povećavajući saglasnost sa regulacionim propisima. Ovaj metod može biti alternativa za korišćenje lozinki i biometrijskih sistema ili može biti korišćen u kombinaciji ovih tehnologija pri stvaranju nFA rješenja.

Svaki korisnik u procesu autentifikacije posjeduje jedinstven kriptografski par ključeva, koji su stečeni od povjerljivih autoriteta nazvnih Sertifikovani autoriteti – CA (*engl. cerificate authority*). Jedan od para ključeva je tajan, dok je drugi javan. Moć PKI autentifikacione tehnologije ogleda se u pristupu osjetljivim informacijama koji nije moguć bez kompletiranja oba kriptografska ključa. Pri tom potrebno je naglasiti, da ključevi ne mogu biti otkriveni jedan iz drugog jer su međusobno povezana složenim matematičkim algoritmom. Ako se šifrovanje informacija vrši sa jednim od para ključeva (javnim ili privatnim) njegovo dešifrovanje treba da bude obavezno sa drugim komplementarnim ključem i obrnuto.

Ranjivost PKI tehnologije direktno zavisi od stepena čuvanja privatnog ključa. Što je veći stepen čuvanja tajnosti privatnog ključa obezbijeđen je i veći nivo zaštite PKI aplikacija, i obrnuto. Pohranjivanjem šifrovanih privatnih ključeva na pametnim karticama omogućava se najviši nivo zaštite privatnih ključeva za razliku od pohranjivanja u računarskim sistemima u kojima ostaju ranjivi na potencijalne fizičke i maliciozne napade. PKI tehnologija ima veliki potencijal u autentifikacionim pristupima zasnovanim na mobilnim uređajima. Opšte je poznato da mobilni uređaji poput mobilnih telefona u svom funkcionisanju koriste SIM karticu. SIM kartice igraju ključni dio u mobilnim PKI aplikacijama.

Ova kartica predstavlja imovinu mobilnog operatora i korišćena je primarno za autentifikaciju mobilnog telefona na mobilnim mrežama. Međutim, mobilni operator može instalirati i dodatne aplikacije na SIM kartici što uključuje treću particiju aplikacija. Primjenom ove opcije mobilni PKI dopušta korisniku sopstevenu autentifikaciju prilikom pristupa internim servisima i digitalnom potpisu elektronskih informacija. Prednosti upotrebe PKI u mobilnim autentifikacionim pristupima su široka raspostranjenost mobilnih uređaja i standardizacija tehnologija koja se koristi u zaštiti i interperabilnosti. Primjenom PKI aplikacija obezbijeđuje se bazično informaciono trojstvo, a time i povjerljivo okruženje u kojima se primjenjuju metode autentifikacije. Primjer primjene PKI tehnologije u mobilnim metodama autentifikacije je mobilni sertifikat.

5.4.1. Mobilni sertifikat

Mobilni sertifikat je zasnovan na javnim ključevima infrastrukture – PKI. Sertifikat može sadržavati jedinstven identifikacioni broj (broj socijalne zaštite) i druge personalne detalje kao što su ime, dan rođenja, pol, nacionalnost, i sl. ali nije time uslovljen. Primjer za ovo je sertifikat *microsoft-a*. Praksa metoda autentifikacije zasnovana na mobilnim sertifikatima je uslovljen poznavanjem korisničkog telefona od strane SP-a. Proces autentifikacije je zasnovan tako da nakon što SP autentifikuje korisnika na osnovu unijetih kredencijala traži dodatnu provjeru korisnika od strane operatora mobilnog telefona (sertifikatora autoriteta – *engl. certificate authority - CA*). Po prijemu zahtjeva CA šalje autentifikacioni zahtjev prema korisniku radi utvrđivanja verifikacije korisničkog mobilnog telefona. Tada korisnik unosi PIN broj koji se zove SPIN koji otključava tajni ključ pohranjen na SIM kartici sa kojim korisnik potpisuje zahtjev. Na osnovu potpisa CA vrši provjeru da li je zahtjev bio potpisan sa pravim tajnim ključem ili ne, i o tome obavještava SP. Mobilni sertifikati mogu biti korišćeni za verifikaciju korisnika za vrijeme trajanja njihovog telefonskog poziva. Da bi mobilni sertifikat mogao biti upotrebljen potrebno je da korisnik obezbijedi sticanje nove SIM kartice od njihovog operatora mobilnog telefona. Prednosti ovog metoda autentifikacije je jednostavnost pri korisničkoj upotrebi, te omogućavaju upotrebu mobilnog sertifikata za vrijeme trajanja telefonskog poziva. Sa druge strane, mana ovog metoda autentifikacije je u cijeni jer zahtijevaju od učesnika u komunikacionom procesu (SP-a i korisnika) da plaćaju usluge servisa. Takođe, moguće je da servis bude upotrebljen

isključivo mobilnim telefonom što dovodi do problema nemogućnosti pokretanja više aplikacija u isto vrijeme koji karakterišu metod zasnovan na OTP korišćenjem SMS.

5.5. *RFID*

Akronim RFID – radio frekvencijska identifikacija (*engl. radio frequency identification*) je opšti pojam za savremenu tehnologiju bežičnog prenosa identiteta objekata ili ličnosti. Svrha RFID tehnologija je da omogući prenos informacija posredstvom radio talasa sa prenosivih uređaja – tagova, koje čita čitač i procesuira prema potrebama određenih aplikacija. RFID tehnologija je grupisana pod široku kategoriju automatskih identifikacionih tehnologija. Istorija RFID tehnologija se dovodi u vezu sa tehnikom čiji je orginalni naziv bio *"identifikacija prijatelja ili neprijatelja"* (*engl. identification friend or foe – IFF ")*. Ova tehnologija je korišćena u Drugog svjetskom ratu od strane Kraljevskih vazdušnih snaga za identifikovanje prijateljskih odnosno neprijateljskih aviona. Danas je ovaj sistem evoluirao u pojam koji zbog svoje raznolikosti i fleksibilnosti i mogućnosti kombinovanja sa drugim tehnologijama, prije svih biometrijskih, primjenjiv gotovo u svim oblastima ljudskog djelovanja. Odlikuje ga visok stepen prilagodljivosti koji ne zahtijeva neposredni kontakt između taga i čitača, već je dovoljno da tag bude u sferi čitačovog djelovanja radio talasa. Na ovaj način se mogu izvršiti automatska višestruka čitanja i ubrzati sveukupni procesi čitanja koji su značajni u poređenju sa sistemom bar koda. RFID sistemi u poređenju sa bar kodom imaju sličnosti i različitosti. Sličnosti su u vidu podržavajućeg alata u automatskim procesima i unapređenja operacionog menadžmenta, i smanjenja ljudskih aktivnosti, a time i eliminisanja ljudskih grešaka. Različitosti su što tag može biti ugrađen i sakriven bez potrebe za linijom vida, često je nevidljiv i za samog korisnika. Oni mogu biti očitavani kroz drvo, plastiku, beton, karton ili bilo koji materijal osim metala. Tag može biti brzo reprogramiran. Primjenjiv je u zahtjevnom okruženju kao što su atmosferski uslovi, hemikalijama, vlaga, visoka temperatura, i sl.

5.5.1. Osnovne komponente RFID tehnologije

Osnovne komponente RFID tehnologije su RFID tag (transponder), antena (kalem) i čitač (transiver) koji mogu biti kombinovani na dva načina. Prvi, transiver

(transmiter/resiver) i antena obično su kombinovani kao čitač, i drugi, transponder (transmiter/responder) i antena su kombinovani da čine RFID tag.

RFID tag je sastavljen od minijaturnog elektronskog kola – mikročipa i antene koja je najčešće zalivena u kućište otporno na uticaj okoline. Tag je "odašiljač" ili elektronski programirana komponenta RFID sistema sa jedinstvenim digitalnim informacijama. Najčešće se pohranjuju osnovne digitalne informacije, maksimalno do 2 kilobita, u obliku identifikacijskog serijskog broja proizvoda ili personalne informacije korisnika. Radi se o identifikatoru elektronskog produkt koda – EPC (*engl. electronic product code*), koji obično koristi 96-bitni format (GID 96) definisan od strane MIT instituta. Neki RFID tagovi ne sadrže informacije već imaju funkciju osiguranja proizvoda od krađe. Takvi tagovi se koriste za elektronsko nadgledanje artikala – EAS (*engl. electronic article surveillance*) i imaju funkciju prikazivanja prisutnosti kada prolaze kroz čitačko polje. Najčešće korišćeni oblik RFID taga je u obliku pametne naljepnice. Radi se o specijalnoj vrsti taga malih dimenzija koja je utisnuta u papirni omot, i može se nalijepiti na proizvod. Spada u najjeftiniju vrstu taga poznat pod nazivom RFID niskih troškova. Posebnost ovog taga je što nude mogućnost da se na njihovoj površini prelijepi bar kod i time učini dostupnost u sistemu koji ne podržavaju RFID tehnologiju. Pored navedenog, tag se može pojaviti i u drugim oblicima npr. kao plastična kreditna kartica ili RFID pločica, pri čemu se radio frekventne zavojnice nalaze na papiru ili foliji zajedno sa memorijskim mikročipom.

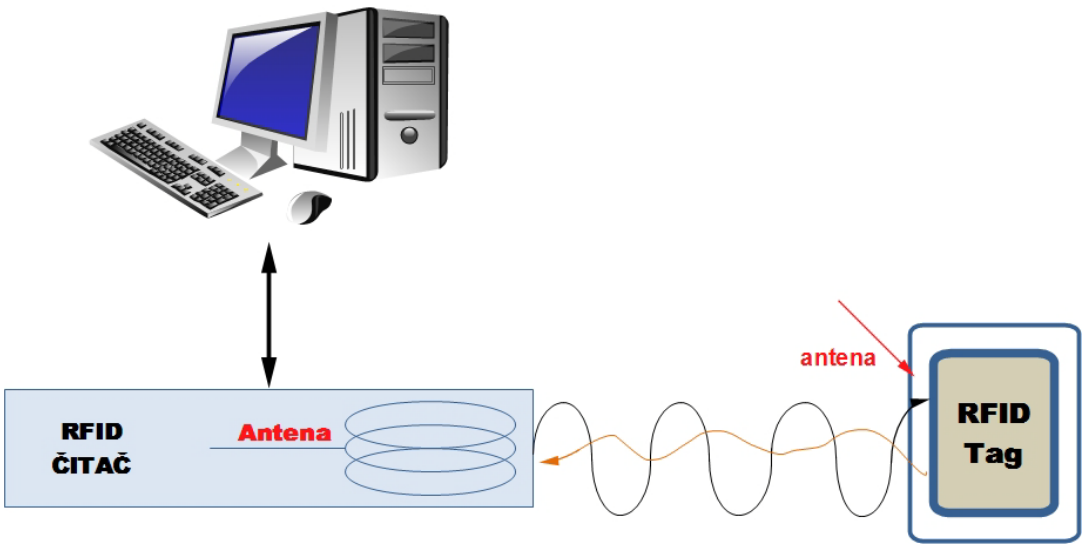
Čitač je komponenta RFID sistema postavljena na određenoj lokaciji s ciljem identifikovanja i praćenja objekta sa tagom. Čitač u dometu svog radio fekventnog polja "komunicira" sa tagom i od njega zaprima potrebne informacije. To je uređaj čije su osnovne funkcije čitanje i upis – korekcija informacija na tagu, i proslijeđivanje informacija na daljnju obradu. Čitanje i upis su napredni oblik RFID-a koji korisniku nudi specifične mogućnosti neograničene izmjene samog sadržaja zapisa. Posjeduje jednu ili više antena koje emituju radio talase i primaju povratne signale od taga. Karakteristike čitača su radna frekvencija, podrška za razne protokole tagova, različite regulative svjetskih regija, mogućnost umrežavanja više čitača, mogućnost upravljanja višestrukim antenama, itd. Čitanje informacija može se vršiti na udaljenostima od 3-5m, a neki čitači mogu da vrše čitanje i na udaljenosti do 100m. Sa aspekta tipa memorije razlikuju se *Read-only* (memorija nepromijenjivog tipa), *Read-Write* (memorija

promijenjivog tipa) i kombinovani tagovi (memorija nepromijenjivog i promijenjivog tipa).

Antene su najkompleksniji dio RFID-a sistema po pitanju dizajna. Antene mogu biti integrisane sa čitačem ili u drugom slučaju integrisane sa tagom. Postoje sistemi u kojima ima više antena jedna za primanje signala, a druga za emitovanje signala. Za kraći frekvencijski domet (manji od 10 cm) antene su integrisane u čitač, dok za duži domet antene su eksterne i vezane na nekoj udaljenosti za čitač. Antene čitača rade u kontinuitetu ili na zahtjev. Stalni rad antene je u slučajevima kada je očitavanje tagova svakodnevno kao npr. naplata putarine, dok na zahtjev rade u slučajevima kada je potrebna povremena identifikacija npr. kontrola ulaza.

5.5.2. RFID princip rada i podjela

Princip funkcionisanja RFID tehnologije je zasnovan na korišćenju radio frekventnih talasa prilikom razmjene informacija između čitača i taga. Princip rada RFID sistem je dat na slici 12.



Slika 12. Princip rada RFID sistema

Sistem funkcioniše na principu neprekidnog "osluškivanja" radio signala emitovanog od strane čitača. Proces aktiviranja nastaje kada se tag nađe u određenom radio frekventnom području čitača. U tom čitačkom polju tag detektuje signal i koristi dobijenu energiju od čitača da bi aktivirao mikročip i proslijedio energiju. Kada RFID čip detektuje odgovarajući signal kao valjan, on putem antene koja kontinuirano stvara

radio frekvencijsko polje šalje informacije sa mikročipa prema čitaču inicirajući time svoju prisutnost u čitačkom polju. Čitač pretvara dobijeni radio signal u informaciju koja se u digitalnoj formi proslijeđuju centralnom računara na obradu. Sistem za obradu vrši njihovo filtriranje i upoređivanje uglavnom posredstvom softvera *ERP* (*engl. Enterprise Resource Planning)* posebno prilagođenom RFID sistemu. Na osnovu rezultata preduzima se odgovarajuća radnja ”*on-off*”.

5.5.3. Podjela RFID tagova

Najznačajnija podjela tagova napravljena je sa aspekta izvora energije za rad i iniciranja kontakta sa čitačem na aktivne, pasivne i polupasivne.

Pasivne tagove karakteriše napajanje putem indukcije jer ne posjeduju sopstveni izvor napajanja, a time ni sposobnost da iniciraju kontakt sa čitačem. Sastoje se iz tri dijela antene, poluprovodničkog čipa prikačenog anteni i nekog oblika kapsule. Proces funkcionisanja ostvaruje se posredstvom energije koju im čitač šalje. Tradicionalni pasivni tagovi su obično u “*spavajućem*” stanju sve dok ne bude probuđen od strane čitača emitovanog polja. Čitač šalje energiju koja se zaprima posredstvom antene taga. Na taj način se kondenzator puni energijom koju proslijeđuje tagu čime se omogućava pravovremeni odgovor. Kapsula ima ulogu u održavanju integriteta taga, i štiti antenu i čip od uticaja okoline. Tagovi imaju sposobnost da rade na različitim frekvencijama, obzirom da čitač može da odašilje radio signale tokom cijele komunikacije. Odgovor taga, pored identifikacijskog broja može i sadržavati razne personalne informacije iz memorije ukoliko ih posjeduje. Zbog snage signala koji se zahtijeva, pasivni tagovi su najčešće korišćeni za aplikacije kratkog dometa. Zavisno od vrste antene i odabrane radio frekvencije domet signala se kreće od od 2mm-1,5m.

Pasivni tagovi su malih dimenzija, veoma lagani, kompaktni i sa neograničenim operacionim životnim periodom. To ih čini vrlo pogodnim za praktičnu ugradnju naljepnica ili ugradnju pod kožu živih bića. Često djeluje zbunjujuće poređenje pasivnog taga sa beskontaktnim pametnim karticama kojima se može pristupiti putem čitača. Iako je komunikacioni metod potpuno isti, beskontaktne pametne kartice imaju čip sa funkcijom obrađivanja i pohranjivanja informacija koji nisu potrebni na pasivnom tagu. Tag za razliku od beskontaktne pametne kartice sadrži identifikator koji sadrži personalne identifikacione informacije, kompleksne metode šifrovanja, ili aplikacije

specifične logike. Pasivni tagovi zbog mogućnosti niske cijene izrade predstavljaju najpopularnije tagove u masovnoj primjeni kod modela elektronskog plaćanja npr. tržnim marketima.

Aktivni tagovi za razliku od pasivnih tagova posjeduju sopstveni izvor napajanja u obliku integrisane baterije ili direktne konekcije sa električnom izvorom iz infrastrukture. Mogu da iniciraju kontakt sa čitačem tako što uspostavljaju sesije. Time imaju i veću snagu radio emitovanog talasa i spadaju u daleko pouzdanije RFID tagove. U posljednjih nekoliko godina aktivni tagovi se izrađuju u elektronskoj formi sa internom malom baterijom za podršku lokalnih funkcija. Vremensko trajanje baterije striktno zavisi od kapaciteta pohranjene energije. Aktivni tagovi mogu kontinuirano emitovati i detektovati signal, i obično su u formi čitaj/piši sa povećanim memorijskim prostorom. Postoje i aplikacije koje mogu pohranjivati informacije primljene od čitača. Ovi tagovi su teži, mnogo skuplji sa ograničenim životnim vijekom, najčešće do 10 godina. Upotrebljavaju se u zahtjevnom radnom okruženju na većim udaljenostima npr. poput radio komunikacija (upotreba u navigacionom sistemu u vazdušnom saobraćaju). Takođe, ovi tagovi imaju sposobnost ugradnje različitih senzora kao što je senzor za nadzor sazrijevanja betona ili nadgledanja temperature kvarljive robe. Posebna pogodnost korišćenja ovih tagova je u mogućnosti povezivanja sa sistemom za globalno pozicioniranje (GPS), što ih čini povoljnim za primjenu u praćenju kretanja vozila i transportnih sistema.

Polupasivni ili poluaktivni tagovi imaju sopstveni izvor napajanja u obliku baterije koja napaja mikročip, dok se za napajanje antene koristi energija prikupljena iz signala čitača. Ne iniciraju kontakt sa čitačem, već samo odgovaraju na njegove signale. Proces funkcionisanja ovih tagova je veoma sličan funkcionisanju pasivnih tagova, ali obzirom da posjeduju internu bateriju, snaga njihovih signala i domet očitavanja su znatno veći od snage signala i dometa pasivnih tagova. S obzirom, da polupasivni RFID tagovi po strukturi napajanja imaju karakteristike i pasivnih i aktivnih RFID tagova, time imaju i određene prednosti odnosno nedostatke u odnosu na iste. Ovi tagovi komuniciraju sa čitačem ukoliko su pasivni tagovi ali oni takođe posjeduju i bateriju da bi podržali specifične funkcije kao što je pohranjivanje periodičnih temperaturnih informacija od temperaturnog senzora. Tagovi se međusobno mogu razlikovati prema radio-frekventnim talasnim dužinama, obliku i veličini, protokolu i načinu pohranjivanja informacija. Prema radio talasnim dužinama tagovi se klasifikuju na nisko-frekventne

(30-500 KHz) sisteme, koji imaju kratak domet čitača i niže cijene, visokofrekventne sisteme (850-950 MHz) i ultra visokofrekventne sisteme (2,4-2,5 GHz) koji imaju znatno veće domete i mnogo veće brzine skeniranja, ali im je shodno tome i cijena znatno veća.

5.5.3.1. Prednosti i nedostaci RFID tag

Prednosti RFID tehnologije se ogledaju u mogućnostima automatskog prikupljanja informacija u realnom vremenu, upravljanju sa informacijama na nivou jednog poslovnog sistema i efikasnoj razmjeni informacija između više poslovnih sistema. Postiže izuzetnu visoku tačnost prvog očitavanja gotovo 100%. RFID tehnologija pri detekciji ne zahtijeva ljudsku intervenciju čime se smanjuje cijena održavanja i eliminišu ljudske greške u procesu prikupljanja. Kako RFID tehnologija ne zahtijeva liniju vida time je i zahtjevano mjesto taga uslovljeno mnogo manjim ograničenjima. RFID tehnologija ima mogućnost čitanja na većim udaljenostima. Tag može imati memorijske sposobnosti čitaj/piši i mogućnost pohranjivanja veće količine informacija dodatih jedinstvenom identifikatoru. RFID tehnologija je manje osjetljiva na nepovoljne uslove (prašinu, hemikalije, fizička oštećenja, i sl.). Ima sposobnost kombinovanja različitih senzora, identifikovanja pojedinačnih stvari i mogućnost istovremenog očitavanja. Takođe, automatsko očitavanje sa više različitih mjesta značajno doprinosi skraćenju ukupnog vremena očitavanja i netačnosti inventara. Tag može lokalno pohranjivati dodatne informacije kao distribuirane informacije, i može smanjiti greške tolerišući cijeli sistem. Skraćuje inventursku kontrolu, troškove rezervisanja i garancije troškova obrade. Sa mogućnošću većeg obima pohranjivanja personalnih informacija u RFID tagovima stvaraju se i brojne mogućnosti njihove zloupotrebe.

Osnovni nedostaci RFID tehnologije se ogledaju u mogućnostima zloupotrebe personalnih informacija, standardizacije, cijena, kolizija, frekvencije, neispravnosti proizvedenih tagova, pogreškama ili manjkavostima detekcijskih tagova, brzom tehnološkom zastarijevanju, zaštiti i privatnosti personalnih informacija, mogućim virusnim napadima, nepostojanju univerzalnog čitača sposobnog da čita bilo koju vrstu taga, i sl. Trenutno, svaki tip taga uslovljen je čitanjem namjenskom opremom. Zloupotreba personalnih informacija podrazumijeva da neautorizovano lice pristupi osjetljivim informacijama, izvrši njihovo čitanje, modifikovanje ili brisanje. Smanjenje zloupotrebe personalnih informacija u RFID tehnologijama se postiže primjenom

biometrijskih metoda i metoda šifrovanja. Primjena metoda šifrovanja u vidu stvaranja šifrovanih specifikacija za RFID tagove su u snažnom progresu od strane standardizovanih organizacija. Primjer primjene zaštitnih šifrovanih algoritama zasnovanih na frekvenciji 13.56 MHz (uspostavljeni od ISO/IEC 14443 standarda) je u automatskoj naplati puteva u javnim tranzitnim aplikacijama. Primjera radi, mobilni uređaji mogu imati funkciju čitača i/ili distribucijom tagova mogu da budu obogaćeni sa senzorima i drugim funkcionalnostima. Ipak, neophodno je pažljivo pristupiti razmatranju upotrebe RFID tehnologije u sistemu koji zahtijeva viši nivo bezbjednosti. Prije svega to je zbog pitanja privatnosti koje predstavlja suštinsko pitanje za buduću primjenu RFID tehnologija.

5.5.3.2. Primjena RFID tagova

I pored nekih nesavršenosti, za integraciju RFID tehnologija se odlučuje sve veći broj kompanija širom svijeta, jer ona sa svojom praktičnošću, izdržljivošću i preciznošću predstavlja budućnost u praćenju tokova informacija, roba i resursa. RFID tehnologija je idealna za primjenu u sistemima kod kojih je potrebna sigurna i precizna identifikacija bez direktne vidljivosti, kao i dugotrajna i izuzetna otpornost identifikatora na razne specifične uticaje okoline (temperatura, prašina, vlažnost i sl.). RFID tehnologija je posebno važna tehnologija za upotrebu u primjeni univerzalnih mrežnih senzora. Njihova velika fleksibilnost i raznolikost omogućava izrazito velik broj primjena koji su sa vremenskim i tehnološkim razvojem u rapidnom usponu. Primjena ove tehnologije susreće se u svim ljudskim sferama života od transporta (vazdušnog, vodenog, kopnenog, i sl.) i logistike, prozvodnih i kontrolnih procesa poput kontrola pristupa vozilima, kontrola ulaza i radnog vremena, nadzora artikala u trgovinama, tekstila, građevinarstva do označavanju životinja tokom uzgoja, kućnih ljubimaca, naplate puteva i parking prostora, zaštite od krađa, autentifikacionim pristupima, i dr.

5.6. Pametna kartica (*engl. smart cards*)

5.6.1. Šta je pametna kartica

Prema Al-Khouri, pametna kartica (*engl. smart card*) je plastična karta sa integrisanim kolom – čipom sposobnim da pohranjuje i obrađuje informacije koji mogu doći sa

različitih kartičnih tijela kao što su magnetne trake, bar kodovi, optičke trake, holografi, itd. Koncept pametnih kartica evoluirao je iz magnetnih traka. Pametna kartica predstavlja fascinantan tehnološki proizvod, veličine kreditne kartice dimenzija 85.6 x53.98 x 0.76 mm. Napravljena je od plastike ili u novije vrijeme od papira. Suštinski, potpuno je ista kao bankovna ili kreditna kartica. Sa ubrzanim razvojem interneta i različitih oblika e-trgovine, pametne kartice su postale sve zastupljenije u korisničkoj upotrebi. Pametne kartice intereaguju sa korisnikom i sistemom dopuštajući upotrebu infomacija. Pametna kartica sadrži karticu sa informacijama i logiku koja podržava upotrebu takvih informacija, ali sama kartica ne obezbjeđuje širi skup servisa. Važno je razumijeti da je pametna kartica efiksan "*mini*" računar sa mnogo istih operacionalnih sposobnosti. Unutar velikih organizacija pametna kartica može obezbijediti jaku zaštitu u procesima autentifikacije za SSO. Pametna kartica spada u metodu autentifikacije zasnovanu na autentifikacionom faktoru korisnika "nešto što ima". Generalno, pametne kartice se smatraju bezbjednim okruženjem za pohranjivanje kriptografskih ključeva i drugih biometrijskih faktora.

5.6.2. Osnovne komponente pametne kartice

5.6.2.1. Mikroprocesor

Pametne kartice sastoje se od integrisanog kola koji sadrži mikroprocesor, memoriju i logički kontrolor. Ono što karticu determiniše "*pametnom*" je čip – mikroprocesor ili centralna procesna jedinica. Čip predstavlja najvažniju komponentu pametne kartice. Veoma je krhak i lomljiv, i pri ugradnji neophodno ga je staviti u kućište koje se naziva modul čipa. Internacionalna organizacija za standarde – ISO (*engl. international organization)* koristi pojam integrisanih kola kartica – ICC *(engl. integrated circuit card)* zaokružujući sve ove uređaje gdje su integrisana kola – IC (*engl. integrated circuit*) sadržani unutar ISO 1 plastične identifikacione kartice. Ne sadrže u sebi nikakv uređaj za napajanje već napajanje dobija od uređaja za prihvat kartica (čitača) – CAD (*engl. card acceptance device*). Inače, proces napajanja pametne kartice se može obaviti na tri načina:

- iz vanjskog izvora preko kontakta, (posredstvom uređaja koji vrši pisanje/brisanje podataka).
- iz vanjskog izvora posredstvom prenosa energije, (bežičnim putem npr. induktivnim putem).

- iz sopstevenog napajanja putem baterije ugrađene u kartici, (manje popularna metoda zbog povećanja cijene izrade kartice i zadovoljavanja ISO standarda).

Takođe, čip se posebno odlikuje veoma pouzdanim i efektivnim načinom obrade kao i upravljanja informacijama u memoriji. Čip čini ”mozak” pametne kartice koji obrađuje, pohranjuje informacije i daje njihovu interpretaciju, čime doslovce drži ključ za jaku zaštitu. Softver je zadužen za obradu i interpretaciju informacija i primljenih komandi, izdaje odgovarajuće upravljačke signale ka drugim uređajima na pametnoj kartici, prihvata rezultate obrade, formira odgovor i prosljeđuje ka terminalu. Softver može biti upisan u memoriju prilikom proizvodnje ili naknadnim upisom pod kontrolom čipa.

Memorija je nepromjenljiva i omogućava pohranjivanje informacija. U memorije se mogu ugraditi programi koje procesor koristi stvarajući naprednije servise. Memorija može biti struktuirana tako da omogućava različite nivoe bezbjednosti. Nekoliko tipova memorije može biti integrisano u pametnu karticu [95] i to:

- *Memorija samo za očitavanje – ROM,* (*engl. read-only memory*), nema mogućnost procesuiranja već samo očitavanja informacija. Informacije sadržane unutar ROM-a memorije su predodređene od strane proizvođača bez mogućnosti promjene.
- *Programbilna stalna memorija – PROM (engl. programmable read-only memory*). Ovaj tip memorije može biti modifikovan ali zahtijeva primjenu visoke voltaže donoseći topljive linkove u integrisanim kolima.
- *Stalna memorija s mogućnošću programiranja – EPROM* (*engl. erasable programmable ROM)* je široko korišćena u ranijim pametnim karticama. Arhitektura integrisanog kola ove kartice djeluje u jednokratnom programskom modu – OTP (*engl. one-time programmable*) što ograničava ponuđene servise od integrisanog kola kartice. Povrh toga, to zahtijeva ultravioletnu svijetlost za brisanje memorije što opet pravi poteškoće organizacijama u smislu upravljanja sa karticama.
- *Elektronska stalna memorija s mogućnošću programiranja – EEPROM* (*engl. electrically erasable PROM)* je servis sa integrisanim kolom koji nudi korisnički pristup i mogućnost ponovnog pisanja u nekim slučajevima i do milion puta. Jasno ovi atributu su ono što pametna kartica treba da ima da bi bila upotrebljiva u današnjem okruženju.
- *Elektronski izmjenljiva memorija – EAROM* (*engl. electrically alterable ROM*)
- *Memorija sa direktnim pristupom – RAM* (*engl. random access memory*), do ove tačke svi primjeri su postojani, što znači da kada je napajanje isključeno podaci

ostaju nepromjenjeni. RAM memorija nema navedene karakteristike i sve informacije sa nestankom napajanja se brišu. Informacije u RAM memoriju se mogu upisivati, modifikovati i brisati. Za neke pametne kartice koje imaju svoja sopstvena napajanja RAM se može koristiti za velika pohranjivanja i brzine. Međutim, u određenim dijelovima memorije informacije će biti izgubljene što može biti prednost ili nedostatak zavisno iz kog ugla se posmatra.

5.6.2.2. Logički kontrolor

Logički kontrolor je ugrađen u memoriju kontrolora. Podržava različite servise i male aplikacije ugrađene u procesoru. Jedan od najinteresantnijih aspekata pametne kartice (u pogledu zaštite aplikacija) zasnovan je na činjenici da je kontrolor pridružen sa podacima u samoj konstrukciji integrisanog kola. Logička kontrola pristupa memorije je značajan atribut u pogledu obezbijeđivanja zaštite privatnosti podataka. Dakle, pametna kartica može da bude konfigurisana tako da dopusti samo sertifikatu (koji sadrži privatni ključ u svrhu digitalnog potpisa) pristup kartici ali nikad da omogući i pristupe eksternim procesima ili aplikacijama. Na primjer, procesor ima sposobnosti da izvrši kriptografske funkcije prema podacima podržanim od strane vanjskih izvora koristeći algoritme koji su ugrađeni u procesor kao i ključ koji je sačuvan u memoriji računara. Osnovna sredstva kojima se postiže vrlo visok nivo bezbjednosti kod pametnih kartica su bezbjednosni mehanizmi. Oni su zasnivani na složenim matematičkim algoritmima. U mehanizme se ubrajaju algoritmi šifrovanja, jednosmjerne funkcije i algoritmi za razmjenu ključeva.

Proces očitavanja pametnih kartica se obavlja pomoću posebnih čitača koji imaju električni kontakt sa interfejsom i moćnim procesorom pametne kartice. Posebna svrha čitača pametnih kartica ogleda se u verifikovanju informacija pohranjenih na kartici. Za korisnika pametna kartica predstavlja dobar izbor u čuvanju kriptografskih ključeva što nije slučaj za administratore. Međutim, vrlo često administrator se nalazi u ulozi korisnika jer isti pametnu karticu kortisti u svrhu pohranjivanja kriptografskih ključeva zaštićenih servera. Ipak, za te svrhe je mnogo bolje rješenje pohranjivanje ključeva na tzv. *hardware security module* – HSM.

5.6.3. Proces autentifikacije zasnovan na pametnoj kartici

Metoda autentifikacije zasnovana na pametnoj kartici je 2FA koja se odvija u dva osnovna koraka. Prvi, odvija se lokalno unošenjem kartice u čitač čime se utvrđuje ispravnost kartice. Sam proces očitavanja pametne kartice predstavlja prvi autentifikacioni faktor korisnika (nešto što ima). Komunikacija između CAD čitača i kartice odvija se preko jedne linije čime se razmjena informacija obavlja naizmjenično, dok jedna šalje druga prima informacije i obrnuto. Ovakav protokol se naziva poludupleks (*engl.half-duplex*) protokol. U tom protokolu odnos kartice i CAD čitača zasnovan je na komunikacionom modelu gospodar – sluga (*engl. master – slave*), gdje je kartica sluga, a čitač gospodar. Na ovaj način se obezbjeđuje da kartica zapravo aktivira CAD čitač. Dvije vrste CAD uređaja su čitač kartice – CR (*engl. cad reader*) i terminal. Terminal je računar koji ima čitač kartice integrisan kao sopstvenu komponentu, npr. automatska govorna mašina – ATM. Drugi, zahtijeva od korisnika da unese PIN ili lozinku (nešto što zna) što predstavlja drugi autentifikacioni faktor. Na taj način se obavlja ”*otključavanje*” informacija koje procesor obrađuje. Kompletiranjem oba koraka obezbjeđuje se mehanizam jake autentifikacije.

5.6.4. Prednosti i nedostaci pametnih kartica

Pametna kartica zbog posjedovanja mikroprocesora, u poređenju sa ostalim autentifikacionim tehnologijama se ubraja u bezbjednije metode autentifikacije. Prvenstveno, prednosti pametnih kartica se ogledaju u mogućnosti višestruke primjene kao što je proces autentifikacije, čuvanja informacija i kredencijala, i sl. U korisničkoj autentifikaciji pametna kartica omogućava postizanje višeg nivoa modularnosti, jednostavnosti i funkcionalnosti, bezbjednosti, kao i pouzdanosti i fleksibilnosti. Suštinska odlika pametne kartice je što korisnik nema direktan pristup ključu onemogućavajući ga da dijeli sa drugim licima. Posjeduje mehanizam samozaključavanja koji poslije određenog broja nepravilnih unijetih vrijednosti PIN-a karticu ”*zaključa*”, i za ponovno ”*otključavanje*” (deaktiviranje) zahtijeva od korisnika kontakt sa prodavačem. Neke kartice imaju opciju da nakon nekoliko pogrešnih pokušaja logovanja nuliraju (poništе) samu sebe, čineći se potpuno beskorisnom. U tom slučaju za ponovno aktiviranje kartice neophodno je izvršiti reprogramiranje kartice.

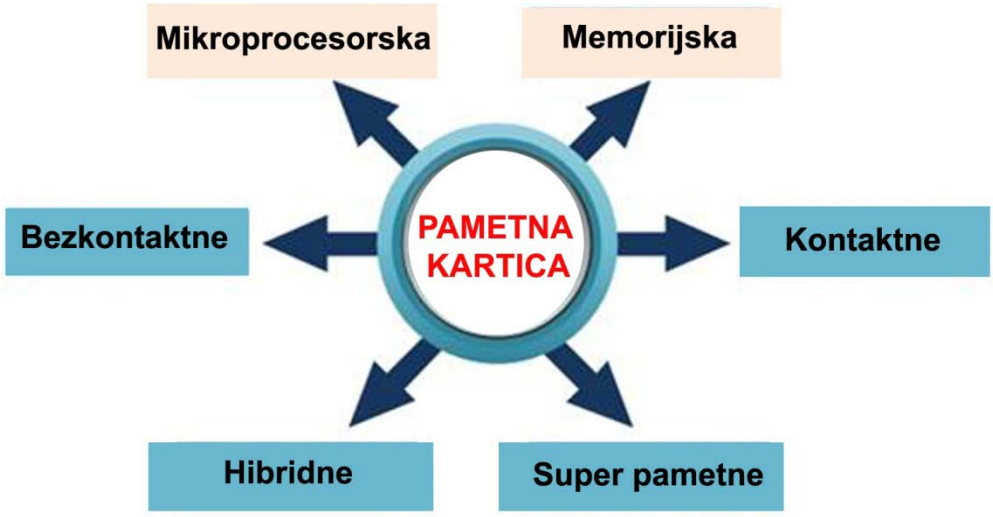
Pametna kartica se teško kopira, zaštićena je na pokušaje neautorizovanog pristupa i izmjene internih informacija. Pametna kartica omogućava proces šifrovanja i dešifrovanja informacija stvarajući time relativno bezbjedno zaštitno okruženje za pohranjivanje informacija i kredencijala. Na taj način se pruža viši nivo bezbjednosti pohranjenih informacija. Takođe, jedna od prednosti je praktičnost, minijaturnost i laka prenosivost kao i visok stepen podešavanja. Trajnost pametne kartice je još jedna odlika koja je izdvaja u odnosu na karticu sa magnetnom trakom (vijek do dvije godine). U poslednje vrijeme razvoj mobilnih tehnologija učinio je dostupnim sve veći broj uređaja koji imaju integrisan čitač kartica.

Nedostatak pametne kartice je u mogućem fizičkom oštećenju, gubitku ili krađi. Takođe, većina korisnika ne posjeduju čitač čime se stvaraju dodatni troškovi rada. Osim navedenog, nedostatak pametne kartice je u mogućnosti napada na karticu nakon izdavanja kartice, a da korisnik pri tom nije ni svjestan. Jednostavno ne postoji način ni senzor sa kojim bi bilo moguće otkriti signal napada. U nekim slučajevima prenizak naponski nivo ili povišena frekvencija takta mogu ukazivati na napad, dok u drugim slučajevima se to može desiti usljed zaprljanosti kontaktnih površina.

Zaista, uzimajući u obzir sve navedeno korisnik pametne kartice nije u mogućnosti prepoznati da li se radi o stvarnom napadu ili ne. Radi toga, dostupni mehanizmi pametnih kartica za automatsko blokiranje i brisanje ključeva se i najčešće ne koriste. Za razliku od personalnih računara kod kojih se uglavnom čitači priključuju putem USB priključka, za čitanje pametnih kartica neophodno je svakom krajnjem korisniku uz karticu dostaviti i čitač koji mora biti uračunat u cijenu njihove implementacije i vijeka trajanja.

5.6.5. Podjela pametnih kartica

Uzimajući u obzir način prenosa informacija i mehanizma pristupa tj. interakcije sa drugim sistemima razlikuju se kontaktne, beskontaktne, hibridne i super pametne kartice, a zavisno od čipa razlikujemo memorijske i mikroprocesorske (slika 13).



Slika 13. Podjela pametnih kartica

Memorijska kartica – spada u najstariji tip koja ima ugrađen čip s memorijom i neprogramibilnom logikom. Funkciju obrade informacija kod memorijske kartice preuzima neprogramibilna logika koja omogućava direktan pristup memoriji i podržava izvršavanje nekoliko neprogramibilnih naredbi. Karakteristika neprogramibilnih logika je neupotrebljivost nakon izvršenja naredbi. Memorijske kartice se koriste za pohranjivanje kriptografskog ključa dok se kriptografske operacije izvršavaju izvan kartice u aplikaciji *host* platforme. Memorijska kartica koristi serijski sinhroni protokol za razmjenu podataka sa čitačem. Tipičan primjer memorijske kartice je SIM kartica. Osnovna odlika ovih pametnih kartica je jednostavnost tehnologije i niska cijena. Nedostatak je mogućnost zloupotrebe.

Mikroprocesorske kartice – kartice koje imaju ugrađen čip sa mikroprocesorom. Aplikacije interaktivno rade sa mikroprocesorom preko aplikativnog programirajućeg interfejsa – API (*engl. application programming interface*). Mikroprocesor ima funkciju obrade informacija čime se zaštita podiže na jedan viši nivo. Funkcionalnost mikroprocesorskih kartica je direktno zavisna od veličine memorije i snage obrade. Mikroprocesorske kartice omogućavaju ugradnju šifrovanih algoritama i primjenu širokog skupa zaštitnih mehanizama. Na taj način omogućava se bezbjedno pohranjivanje kriptografskog ključa i izvršavanje kriptografskih operacija na samoj kartici. Mikroprocesorske kartice su mnogo pouzdanije za zaštitu aplikacija jer kriptografski ključevi ne napuštaju bezbjedno okruženje. Međutim, da bi se u potpunosti ostvarilo bezbjednosno okruženje potrebno je voditi računa o prvom autentifikacionom faktoru – PIN-u. U tom slučaju, korisniku je potreban eksterni čitač kako PIN ne bi

prolazio kroz operativni sistem. Primjena ovih kartica je u sistemu koji zahtijeva viši nivo zaštite personalnih informacija i privatnosti, npr. kontrola pristupa, aplikacije bankovnih sistema, aplikacije u telekomunikacionim sistemima, i sl.

Kontaktne kartice – sam naziv kontaktne kartice je prilično razumljiv sam za sebe. Koristi fizički kontakt u komunikaciji sa drugim sistemom (potrebno ih je unijeti u čitač). Zasnovane su na ISO-7816-2 standardu, pri čemu je prenos i obrada informacija moguća samo u slučaju kada je kartica postavljena u CAD čitač. Kontaktna pametna kartica je u obliku jednog čipa veličine oko 10mm kod koga se na površini nalaze zlatni kontakti za komunikaciju sa okruženjem. Čitač pametnih kartica je u direktnoj konekciji sa provodljivim mikromodulima na površini kartice. U svrhu te namjene, kartica je konstruisana tako da je kontakt integrisanog kola kartice obezbijeđen sa 8 električnih kontakata (samo 6 u upotrebi) za interakciju sa drugim sistemom ili čitačem. Kontakti na pametnoj kartici obezbjeđuju pristup različitim elementima ugrađenim u integrisano kolo. Kontaktne kartice ne posjeduju sopstveni izvor napajanja i nemaju mogućnost generisanja unutrašnjeg signala. Jedna od najvećih odlika kontaktnih kartica je bezbjednost. Samo autentifikovani korisnici imaju pristup kartici tako da izgubljena ili ukradena kartica ne dozvoljava pristup internim informacijama. Prednost kontaktne kartice je takođe u mogućnosti interne obrade informacije i prosleđivanju rezultata prema izlaznom okruženju. Nedostatak kontaktnih kartica ogleda se u brzini očitavanja i nepogodnosti primjene za sve tipove aplikacija, posebno kod masovnih transakcija. Takođe, mane ovih kartica su moguća fizička oštećenja, nakupljanja nečistoća na kontaktnim površinama, i u procesu aktiviranja zahtijeva tačno određeni položaj u prostoru u odnosu na čitač. Pored svih navedenih nedostataka, kontaktne kartice su daleko u najširoj upotrebi.

Bezkontaktne kartice – su kartice čija je primjena u stalnom porastu. Razlozi su prvenstveno zbog njihove izdržljivosti, jednostavnosti, pristupačnosti, brzine i pogodnosti očitavanja informacija. Ne koristi fizički kontakt u komunikaciji sa drugim sistemom (nije ih potrebno unijeti u čitač) ali je obavezno da budu unutar područja čitača. Komunikaciju sa okruženjem se ostvaruju posredstvom antene ugrađene u kućište tjela kartice. Napajanje se izvode internom baterijom ili elektromagnetnom indukcijom posredstvom ugrađene antene. Kao prenos energije i informacija na kartici se koristi induktivna ili kapacitivna veza. Informacije do čitača se prenose interno elektromagnetnim poljem. Frekvencija radio frekvntno djeluje u polju 13.56 MHz sa

odstupanjem 7kHz, i djeluje konstantno unutar minimuma i maksimuma dometa. ISO14443 definiše fizičke karakteristike, radiofrekvencijsku snagu i signal interfejsa, inicijalizaciju, antikoliziju i prenošenje protokola za bezkontaktnu karticu. Visoko frekventno elektromagnetno polje ima dvostruku ulogu, ulogu prenosa energije elektromagnetnom indukcijom – antenom i prenosa informacija posredstvom faznom ili amplitudnom modulacijom. Proces slanja informacija prema čitaču obavlja se na udaljenosti do 50cm. Primjena beskontaktnih kartica je u sistemima pristupa određenim prostorijama ili u javnom saobraćaju gdje je neophodna kontrola većeg broja ljudi u kratkom vremenskom periodu.

Njihov dizajn koji eliminiše fizičku interakciju sa okruženjem, a time i moguća oštećenja kartice, značajno produžava životni vijek kartice. Posebna prednost bezkontaktnih kartica je u mogućnosti bezbroj korišćenja i integracije sa npr. telefonima ili PDA uređajima. Bezkontaktna kartica u procesu aktiviranja kartice može zauzeti bilo koji položaj u prostoru u odnosu na čitač za razliku od kontaktne koja zahtijeva preciziran položaj. Veoma je zahvalna za održavanje i rukovanje. Nedostaci bezkontaktnih kartica su u cijeni i malom prenosu informacija prema CAD čitaču. U pogledu bezbjednosnog aspekta, obezbijeđuju niži nivo bezbjednosti u poređenju sa kontaktnim karticama, jer su moguća presretanja i zloupotreba informacija. Definisane su prilično lošim standardom, imaju povećanu osjetljivost na savijanje, i moguća oštećenja usljed reljefnih obilježja.

Hibridne (kombinovane) pametne kartice –čine kombinaciju kontaktnih i bezkontaktnih kartica integrisanih u jednu multiaplikacijsku karticu. Nastale su kao korisnička potreba da se integrišu prednosti pametnih kartica u jednu karticu s ciljem približavanja i olakšavanja korisničkih zahtjeva. Kombinovana kartica ima dva čipa, jedan za kontaktni čitač i drugi za bezkontaktni čitač. Mogu se koristiti u obe situacije i upotreba je moguća gotovo u svim sistemima. Posjeduje dodatak za magnetnu traku sa strane jedno–dvodimenzionalni kod. Njihova glavna odlika je što se jedna kartica koristi u različite svrhe poput kreditne kartice, bankovne kartice, članske kartice, ID karte, itd.

Super pametne kartice – predstavlja proizvod treće generacije i spada u aktivne kartice. Nastala je kao potreba da se eliminišu nedostataci prethodnih pasivnih kartica. Odlikuje ih fleksibilnost, potpuna samostalnost ili mogućnost konekcije sa uređajima iz okruženja. Informacije se mogu direktno pohraniti na kartici od strane korisnika.

Posjeduju sopstveni izvor napajanja, tastatura i LCD monitor na površini kartice, i kontaktne površine putem kojih ostvaruju konekciju. Prednost ovakvih kartica su primarno u mogućnostim *"offline"* rada i samoprovjeravanja. U poređenju sa pasivnim pametnim karticama njihova upotreba je moguća bilo gdje i u bilo koje vrijeme. Osnovni nedostaci ovih kartica su u visokoj cijeni i problemi u vidu ispunjavanja ISO standarda. Takođe, zbog malih dimenzija kartice veoma je nezgrapno rukovanje sa tastaturom.

Super pametna kartica obezbijeđuje maksimalnu zaštitu usljed jedinstvene arhitekture koja je ugrađena u hardver. Super pametna kartica multiaplikacijski dizajnirana nudi višestruke nezavisne i zaštitne aplikacije koegzistiranja, i operacija na istoj kartici. Takođe, ova kartica posjeduje biometrijski sistem identifikovanja korisnika (npr. metod otiska prsta) koji karakteriše većom otpornošću na uticaj vlažnosti, prljavštine, i sl. Sa ovim implementiranim sistemom zaštite obezbijeđuje se najviši nivo zaštite. Sistem na taj način sprečava neautorizovanu upotrebu kartice ili aplikacija na kartici, zahtijevajući samo autorizovane korisnike. Ukoliko je izgubljena ili ukradena kartica je potpuno beskorisna.

5.6.6. Primjena pametnih kartica

Širok je djelokrug primjene pametnih kartica. Posebno široku primjenu je našla u informacionoj zaštiti gdje se koristi u PKI sistemu za korisničku identifikaciju i autentifikaciju, pohranjivanje digitalnih sertifikata i kriptografskih tajnih ključeva. Osim toga, primjena pametnih kartica je u kontroli pristupa od prostorija u kojima se čuvaju povjerljive informacije do parking prostora, garaža, glavnih ulaza, čak i kanti za smeće. Takođe, u mnogim organizacijama pametne kartice predstavljaju alat koji se najčešće primjenjuje za individualnu kontrolu zaposlenih gdje se ista kartica koristi za određivanje različitog nivoa pristupa internim zonama. Pametna kartica, pored pohranjivanja kredencijala može se koristiti i za pohranjivanje zdravstvenih, bankovnih i drugih osjetljivih personalnih informacija. Pametna kartica je našla svoju primjenu i u telekomunikacijama gdje su postale jedna od najvažnijih komponenti. Sve mrežne, preplatničke i druge bitne informacije mobilnih mreža pohranjuju se unutar kartice. Takođe u procesu e-plaćanja, pametna kartica služi za pohranjivanje novčanih sredstava u formi elektornskog novca. Ovaj proces se uglavnom koristi za manje elektronske

transakcije. Cijena pametnih kartica je danas u opadanju što značajno utiče na njihovu širu upotrebu.

5.7. Biometrija

Teroristički napad na Kule blizankinje izveden u Americi 2001. godine predstavlja prekretnicu u razvoju i intenziviranju primjene biometrijskih sistema širom svijeta. Ti događaji su u prvi plan istakli potrebu za biometrijom kao tehnologijom koja je u stanju da iz mase ljudi sa velikom preciznošću izdvoji pojedince (potencijalne teroriste), primjera radi na mjestima sa velikom frekventošću ljudi kao što su aerodromi, luke, i sl. Biometrija (*engl. biometrics*) je nauka koja u procesu automatskog prepoznavanja korisnika koristi biometrijski faktor. Biometrijski faktor opisuje nešto što korisnik jeste poput bihejviorističkih karakteristika kao što su iris, lice, otisak prsta, geometrija dlana, retina, vene, i druge fizičke karakteristike kao što su glas, potpis, dinamika kucanja, i sl. Dakle, biometrijska autentifikacija je zasnovano na *nečemu što jesi* ili u Šnajerove besmrtne riječi "ti si svoj ključ" [96].

U praksi, metod autentifikacije zasnovan na biometriji može koristiti kombinaciju fizičkih i bihejviorističkih osobina. Biometrija kao metoda funkcioniše samostalno ili kao dopuna drugim metodama autentifikacije stvarajući nFA mehanizme. U poređenju sa prethodnim metodama autentifikacije, biometrija spada u najbezbjednije mehanizme. Biometrija u procesu autentifikacije dodaje novi dodatni sloj zaštite obezbijeđujući pri tom najviši nivo zaštite koji eliminiše nedostatke prethodnih metoda.

Osnovna svojstva biometrije korišćena u procesima autentifikacije su:

- univerzalnost,
- jedinstvenost,
- trajnost,
- prikupljivost,
- efikasnost,
- prihvatljivost, i
- mogućnost zaobilaženja [97].

Razlikujemo unimodalni i multimodalni biometrijski sistem. Unimodalni u procesu autentifikacije koristi jednu biometrijsku metodu, dok multimodalni koristi više biometrijskih metoda. Unimodalni biometrijski sistemi, pored povoljnosti i jednostavnosti nisu savršeni i trpe nekoliko praktičnih problema poput:

- neuniverzalnost,
- bučnost senzora,
- varijacije unutar klase,
- ograničeni stepeni slobode,
- neprihvatljiva stopa greške,
- pogreške pri upisu, i
- spuf (*engl. spoof*) napada [98].

Primjera radi, nedostaci unimodalnih biometrijskih sistema implementirani u konkretnim metodama mobilne autentifikacije su:

- kod dinamike kucanja – nezgrapnost metode zbog male tastature sa osjetljivim ekranom na dodir [99],
- kod dužice i lica – skupa oprema (zahtijeva kamere veće rezolucije), moguće zloupotrebe poput lica maski i odstupanja sa pozicije uzimanja slike, ugla, osvjetljenja, i sl. [100],
- kod glasa – podložnosti prevarama u vidu snimanja glasa, zatim objektivni korisnički problemi u vidu promuklosti, prehlade, bučnosti pozadine, i sl. [101],
- kod otiska prsta – nakupljanju prašine i nečistoća na dodirnoj površini te zloupotreba otiska pomoću želatina [100].

Savladavanje unimodalnih biometrijskih nedostataka postiže se primjenom multimodalnih biometrijskih metoda. Većina biometrijskih problema i ograničenja su nametnuti unimodalnim biometrijskim sistemima. Unimodalni biometrijski sistemi oslanjaju se očigledno samo na pojedinačne biometrijske crte. Neki od ovih problema mogu se savladati primjenom multimodalnih biometrijskih sistema.

Prema tome, prednost biometrije u odnosu na sve druge metode ogleda se u brzini i jednostavnosti sistema, i nivou pružene zaštite. Biometrija koristi kredencijale koji se ne mogu zaboraviti, izgubiti ili ukrasti. Nasuprot prednostima, mane ovog metoda su kompleksnost, cijena, faktori koji utiču na sistemsku efikasnost, i posebno pitanje privatnosti. Zbog jedinstvenosti i nepromijenjivosti biometrijskih kredencijala kod

korisnika postoji određeno nepovjerenje prema načinu pohranjivanja tih kredencijala i mogućnosti zloupotrebe. Posljednjih godina, upotreba biometrijskih metoda autentifikacije je u ekspanziji sa primjenom u vladinim visoko zaštićenim aplikacijama (pasoši i lične karte) i komercijalnim aplikacijama (praćenja prisustva zaposlenih, zaključavanja kućnih vrata, kupovne kartice za tržne centre, i sl.) [100]. Takođe, sve je veća primjena biometrije i u privatnom sektoru. Primjer primjene biometrije u privatnom sektoru je u kompaniji *Disney World*, koja koristi biometrijski sistem za sezonske karte.

Posljednih godina, ubrzani razvoj novih digitalnih tehnologija stvorio je uslove šire primjene biometrije u mobilnim metodama autentifikacija. Biometrijske metode autentifikacije su dobro – studirano područje istraživanja. Kao prethodnik za biometrijska mobilna istraživanja, Clarke *et al.,* [102] su objavili studiju izvodljivosti različitih biometrijskih metoda autentifikacije na mobilnim uređajima. U istraživačkom radu [103] Furnell *et al.,* su opisali okvir nazvan *Non- Intrusive Continuous Authentication (NICA)* u kojem potvrđuju da upotreba biometrijskih metoda obezbjeđuje viši nivo zaštite nego što su to metode zasnovane na tajni ili znanju. Dakle, ključni razlog za uvođenje biometrije u procese autentifikacije predstavlja zaštita [104].

5.7.1. Vrste biomerijskih sistema

Biometrijski sistem može da bude dizajniran da testira jednu od dvije moguće hipoteze [105]:

1. podnijeti uzorak od pojedinca je poznat za sistem – pozitivna identifikacija,
2. podnijeti uzorak od pojedinca nije poznat za sistem – negativna identifikacija.

Svi biometrijski sistemi rade na jednom ili drugom principu. Najvažnija razlika između sistema je što pozitivna identifikacija zahtijeva podudaranje rezultata dok negativna identifikacija zahtijeva nepodudaranje rezultata. Pozitivna i negativna identifikacija su suprotne jedna u odnosu na drugu. Pozitivni sistemi identifikacije sprečavaju višestruke korisnike da koriste pojedinačni identitet, dok negativni sistemi identifikacije sprečavaju upotrebu višestrukih identiteta od strane pojedinačnog korisnika. U pozitivnom sistemu identifikacije, upisni šablon ili model pohranjivanja može biti centralizovan ili decentralizovan dok negativni sistemi identifikacije zahtijevaju centralizovano pohranjivanje. Pozitivni sistem identifikacije odbija korisničku potvrdu identiteta ako ne

pronađe podudarnosti uzorka sa prethodno upisanim šablonom. Negativni sistem identifikacije odbija korisnički potvrdu identiteta ako je podudarnost pronađena.

Bez obzira na tip sistema, greške u odbijanju prave smetnje korisnicima na primjer u slučaju pogrešne prihvatljivosti dopušta prevaru. Pozitivna identifikacija odobrava da sam "*ja*" neko koje poznat sistemu dok negativna identifikacija odobrava da sam "*ja*" neko ko nije poznat sistemu. Primjer primjene pozitivne identifikacije je kontrola pristupa dok je primjer negativne identifikacije baza podataka sumnjivih lica. Biometrijski sistemi se najčešće koristi za povećanje bezbjednosti računarskih mreža, zaštitu finansijskih transakcija, obezbjeđivanje međunarodnih granica, kontrolu pristupa zaštićenim radnim mjestima i sprečavanje različitih prevara.

U tabeli 1 Wayman *et al.*, [105] su dali pregled razlike između pozitivne i negativne identifikacije.

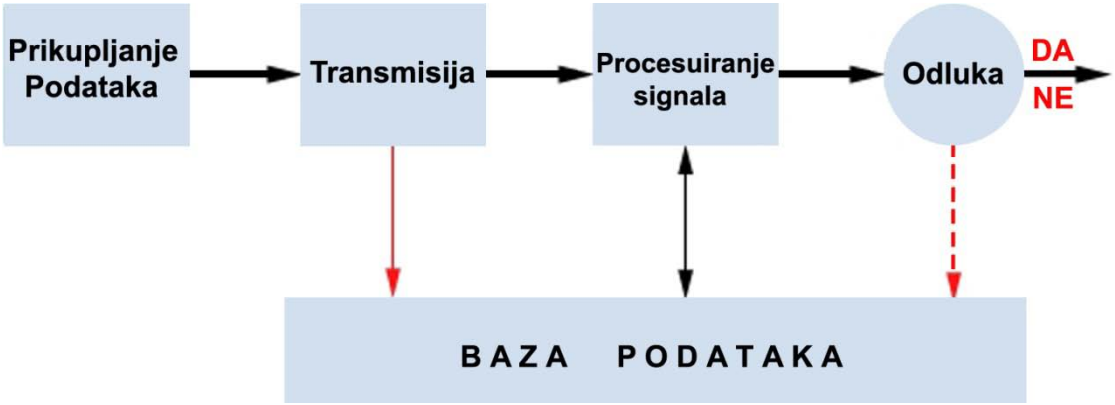
Tabela1. Identifikacija "pozitivna" i "negativna" [105]

Pozitivna	**Negativna**
Odobrava da je neko koje poznat sistemu	Odobrava da je neko ko nije poznat sistemu
Sprečava upotrebu višestrukih korisnika za isti identitet	Sprečava upotrebu višestrukih identiteta od strane jednog korisnika
Upoređuje podnijeti uzorak sa pohranjenim šablonom "*one-to-one*"	Upoređuje podnijeti uzorak sa svim pohranjenim šablonima "*one-to-many*"
"Pogrešna podudarnost" vodi "pogrešnom prihvatanju"	"Pogrešna podudarnost" ili "pogrešno sticanje" vodi "pogrešnom odbijanju"
"Pogrešna ne-podudarnost ili "pogrešno sticanje" vodi "pogrešnom odbijanju"	"Pogrešna ne-podudarnost" vodi "pogrešnom prihvatanju"
Alternativne metode identifikacije postoje	Alternativne metode identifikacije ne postoje
Zasnovana je na dobrovoljnoj osnovi	Treba da bude obavezna za sve
Moguće je podnošenje lažnih biometrijskih karakteristika	Nije moguće podnošenje niti zamjena biometrijskih karakteristika.

5.7.2. Princip rada biometrijskog sistema

Princip rada biometrijskog sistema se zasniva na mjerenju i analizi bioloških informacija pojedinca, izdvajanju karakterističnih obilježja i upoređivanja sa onima koja su već prethodno pohranjena u bazi podataka. Opšti biometrijski sistem autentifikacije koji je podijeljen u pet podsistema prikazan je na slici 14:

1. Prikupljanje informacija (*engl. collection information*) – sastoji se od ulaznog senzora putem kojeg se prikupljaju biometrijske karakteristike i pretvara ih u digitalnu formu.
2. Transmisija (*engl. transmission*) – neki sistemi ali ne svi, prikupljaju podatke na jednoj lokaciji ali pohranjivanje i obrađivanje je na drugom mjestu. Takvi sistemi zahtijevaju transmisiju podataka koja uključuje i prethodnu kompresiju radi uštede memorijskog prostora.
3. Procesuiranje signala (*engl. signal processing*) – sastoji se iz četiri podprocesa, segmentacije, ekstrahovanja karakteristika, kontrole kvaliteta i algoritma podudaranja. U algoritmu podudaranja se vrši upoređivanje novih biometrijskih šablona jednog ili više sa prethodno pohranjenim u bazi podataka. U ovom podsistemu se vrši razvoj biometrijskih šablona.
4. Pohranjivanje informacija (*engl. date storage*) – baza podataka čuva informacije sa kojima će biti upoređivani novi biometrijski šabloni.
5. Donošenje odluke (*engl. decision process*) – implementira politiku na sistemskom nivou (automatski ili uz pomoć čovjeka) i na osnovu rezultata iz algoritma podudaranja direktno se donosi odluka.



Slika 14. Opšti biometrijski sistem

Odluke biometrijskih sistema u procesima autentifikacije su u binarnom obliku i moguće su dvije vrste grešaka:

- Pogrešno odobijanje – FR (*engl. false rejection*) – kada korisnik dobije identifikator kao napadač.
- Pogrešno prihvatanje – FA (*engl. false acceptance*) – kada napadač dobije identifikator kao korisnik.

Proces rada biometrijiskih sistema je potpuno automatizovan i za utvrđivanje identiteta potrebno je u prosjeku nekoliko sekundi, što ovaj proces čini vrlo brzim i efikasnim. Bitno je istaknuti, da prilikom odabira biometrijskog sistema potrebno je voditi računa o pouzdanosti (odnosi se na tačnost, brzinu i faktore koji mogu uticati na rad), prihvatljivosti (spremnost ljudi da prihvate korišćenje ovih sistema u svakodnevnom radu), kao i otpornosti (koliko je sistem otporan na zloupotrebu i na napade).

5.7.3. Savremene korisničke biometrijske metode

O ovom dijelu rada opisani su savremene korisničke biometrijske metode koje imaju široku upotrebu u mobilnim autentifikacionim pristupima kao i one za koje se u narednom periodu može očekivati veća primjena.

5.7.3.1. Fingerprint

Fingerprint je metod autentifikacije koji se zasniva na upoređivanju minutiae (grebenova, bifurkacija, ili ostrva na prstu) koje su stečene korišćenjem senzora čitača otiska prsta [106]. Fingerprint je jedan od najpopularnijih i najprihvatljivih biometrijskih metoda [100]. Posebnu popularnost ovog metoda podigao je razvoj pametnih telefona sa integrisanim čitačem otiska prsta. Ovaj inovativni čitač prsta koristi tehnologiju radio talasa koji detektuju subepidermalne slojeve korisničke kože, zahtijevajući "živi prst" korisnika pri procesu logovanja. Na ovaj način savladava se najveći nedostatak prethodnih metoda otiska prsta, a to je mogućnost kopiranja poput želatna ili nasilne amputacije prsta. Prednosti ovog metoda su pouzdan rad, brzina, tačnost i čitljivost za 360-stepeni sa slikom dobrog kvaliteta. Ovaj metod sa integrisanom radio - frekventnom tehnologijom obezbjeđuje visok nivo zaštite za korisničku autentifikaciju.

Čitljivost za 360-stepeni podrazumijeva bilo koji položaj prsta u trenutku logovanja. Najveći nedostatak ovog modela je u nakupljanju prašine, nečistoća, znoja i drugih tečnosti na dodirnim površinama prsta i čitača ili uređaja. Sa druge strane, u mobilnim autentifikacionim pristupima trenutno je mali broj mobilnih uređaja koji imaju integrisanu novu tehnologiju otiska prsta. Posebna primjena ovog metoda je u korisničkom otključavanju mobilnih uređaja kao i u procesu identifikacije kriminalnih lica. U budućnosti ovaj metod autentifikacije je obećavajući metod čija primjena je moguća u svim sektorima. Ovaj inovativni metod autentifikacije je alternativa lozinkama.

5.7.3.2. Voice/Speech

Voice/Speech je metod autentifikacije koji se isključivo oslanja na karakteristike glasa/govora. Ovakav metod zahtijeva da korisnik pri autentifikaciji izgovori neku frazu koja se upoređuje sa pohranjenim uzorkom. Postoji mnogo radova koji su se bavili ovim metodom kao što su [107-110]. Njihovi zaključci su jedinstveni da ovaj metod ispunjava sva željena biometrijska svojstva, ali da je to nedovoljno za upotrebu kao jedinstvene biometrijske metode u procesu autentifikacije. Metod atentifikacije glasa je usmjeren na spoznaji ko govori, dok je prepoznavanje govora u velikoj mjeri usmjereno na prepoznavanju riječi odnosno fraza nezavisno ko govori [111].

Metoda autentifikacije korišćenjem glasa je zasnovana na analizi glavnih karakteristika govora kao što su korelacija tona i intonacija, i fonetika. Prednosti ovog metoda su u cijeni, prihvatljivosti i nenametljivosti za korisnika. U mobilnom autentifikacionom pristupu, ne zahtijevaju skupe mobilne uređaja jer svaki mobilni uređaj ima integrisanu funkciju glasa/govora. Nedostatak ovog metoda je u podložnosti prevarama u vidu snimanja glasa legitimnog korisnika koji se kasnije može reprodukovati pri autentifikaciji. Poboljšanje verzije ovog metoda postiže se sa uvođenjem određene vrste pitanja za korisnika od strane sistema. Nedostaci ovog metoda su u promjenjivosti korisničke boje glasa koja može biti uzrokovana objektivnim i neobjektivnim korisničkim problemima. Objektivni korisnički problemi su u vidu, bolesti, promuklosti, prehlade i raspoloženja korisnika (pjevanjem ili glasnim pričanjem). Neobjektivni korisniči problemi su bučnost pozadine, dob korisnika i promjenjivosti boje glasa u jutarnjim u odnosu na podnevne ili večernje sate.

5.7.3.3. Face

Face je metod autentifikacije koji omogućava prepoznavanje ličnosti putem lica. Zasniva se na opštem principu uzimanje korisničke slike lica posredstvom kamere. Prilikom očitavanja karakteristika stvara se dvodimenzionalna (2-D) slika lica. Proces se sastoji iz izdvajanja karakterističnih tačaka na licu i njihovim poređenjem sa ranije stečenim uzorkom pohranjenim u bazi podataka. Na osnovu tih poređenja odgovor može biti verifikujući ili odbijajući. Međutim, poput drugih metoda autentifikacije i ova metoda pokazuju određene nedostatke, prije svih u cijeni. U postupku uzimanja slike lica mnogo je faktora koji mogu uzrokovati nepodudarnost slike. Na primjer, uticaj okoline, odstupanja od pozicije uzimanja slike, ugla kamere pri snimanju, količine svijetlosti koja padne na lice, promjena ugla gledanja u kameru, i sl. Moguće zloupotrebe ove metode su poput maske lica [112], problema promijenjivosti lica uzrokovani biološkim procesom starenja, nošenja brade ili naočala, promjene frizure, šminke izraza lica i brade. Stoga, metode 2-D imaju visoku stopu jednakog udjela pogreške – EER (*engl. equal error rate*). U novije vrijeme sistemi rade na principu 3-D metoda uzimanja slike, čime se neutrlišu određeni nedostaci prisutni u 2-D metodu uzimanja slike. Prvenstveno, neki sistemi koji zahtijevaju veći nivo zaštite koriste više kamera u procesu očitavanja lica iz različitih uglova, dok neki sistemi prate određene pokrete lica (treptaje oka, micanje usana, i sl.) kako bi obezbijedili da se radi o živoj osobi.

5.7.3.4. Iris

Iris je metod autentifikacije veoma sličan licu, koji omogućava prepoznavanje ličnosti putem irisa. Ovaj biometrijski metod koristi predstavljanje tekstualne podloge od irisa što znači da verifikuje lični identitet [113,114]. Metod prepoznavanja irisa se zasniva na opštom principu uzimanje korisničke slike irisa posredstvom kamere. Proces se zasniva na izdvajanja karakterističnih tačaka na irisu te njegovo matrično poređenje sa ranije stečenim uzorkom pohranjenim u bazi podataka. Na osnovu tih poređenja, odgovor može biti verifikujući ili odbijajući. Zbog jedinstvenih karakteritika, kao što je vremenska nepromjenjivost za svaku osobu (koja nije genetski zavisna) i brzine raspadanja nakon smrti, iris je gotovo nemoguće zloupotrijebiti. Stoga, za ovaj metod se može reći da ispunjava sva željena zaštitna svojstva. Nizak EER, ovaj metod svrstava među najbolje metode autentifikacije. Nedostatak ovog metoda je velika složenost

matričnog algoritama, skupoće mobilnih uređaja koji zahtijevaju kameru izuzetno visoke rezolucije. Takođe, kao i kod metoda *face* isti uzroci mogu uticati na nepodarnost irisa.

5.7.3.5. Keystroke Dynamics

Keystroke Dynamics je dobro – prostudirano područje istraživanja. Zasnovano je na korisničkom jedinstvenom načinu kucanja na tastaturi definisano vremenskom sekvencom. Podloga između kucanja i trajanja kucanja oblikuje korisnički profil. Postoji značajan broj studija koje su bile urađene u ovom području kao što su [115-118]. Njihovi zaključci su jedinstveni da dinamika kucanja na tastaturi ispunjava sva željena biometrijska svojstva. To je posebno podržano od strane sljedećih radova [119,120], gdje je navedeno da je *False Accept Rates (FAR)* i *EER* manje od 10%, i *False Reject Rates (FRR)* je 2.5%. Prednost ovog metoda su da omogućava istovremenu korisničku autentifikaciju i postojanost nadgledanja dinamike kucanja. Ovaj metod može biti klasifikovan kao statični i dinamični [121]. Statički se odnosi na analizu dinamike kucanja izvršene u određenom vremenskom intervalu npr. proces logovanja, dok se kontinuirani odnosi na analizu kucanja izvršenu tokom cijele sesije [122]. Ipak, pored gore pomenutih prednosti ovog metoda, metod dinamike kucanja je nedovoljan za upotrebu kao jedinstvene biometrijske metode u procesu autentifikacije [108]. Nedostaci ovog metoda su što dinamika kucanja predstavlja naučenu tehniku koja je promijenjivog karaktera. Ovaj metod kada su u pitanju mobilni uređaji, je takođe veoma nezgrapan metod zbog male tastature na mobilnim uređajima, kao i problema sa mobilnim uređajima koji posjeduju meki metod unosa poput osjetljivih ekrana.

5.7.3.6.Gait recognition

Gait recognition je mobilni metod autentifikacije koji dopušta automatsku verifikaciju identiteta ličnosti pri njegovom hodu. Sa tehnološkim napretkom mobilnih tehnologija zasnovanih na primjeni skupa različitih senzora ovaj metod je postao primjenjiv na mobilnim platformama [123]. Ovaj biometrijski metod je takođe dobro – ispitano područje istraživanja. Istraživanja u ovom području su nezavisno započeta od strane autora Ailisto [124] i Gafurov *et al.*, [125], a kasnije i kroz radove kao što su [126-130]. Generalno, popularnost ovog metoda je zbog mogućnosti njegove primjene u mnogim različitim područjima kao što su zdravstvo, fitnes, industrija, zaštita, i sl. Postoje tri

različita formata ovog metoda kao što su vizija mašina (*engl*. *machine vision* [131,132], podni senzor (*engl*. *floor sensor* [133] i senzor nošenja (*engl*. *wearable sensor* (WR) [134]. Ovaj metod je zasnovan na principu da korisnik nosi pokretni snimajući senzor oko struka, u džepu ili na cipelama, na osnovu kojeg se autentifikuje. Nosivi senzor – WR može biti akcelerometar (mjeri akceleraciju), žiro senzor (mjeri rotaciju i broj stepeni po drugoj rotaciji), senzor sile (mjeri silu pri hodu), i tako dalje [133]. Ovaj metod može biti viđen kao pogodnost nad drugim oblicima biometrijskih metoda zbog njegove kompleksnosti i zaštite. *Gait recognition* omogućava korisničko – prijateljski i nenametljivu autentifikaciju za mobilne uređaje koji već sadrže akcelerometar (poput mobilnih telefona, PDA, i sl.). Pri poređenju sa drugim biometrijskim metodama, ovaj metod popravlja najgore preoznavajuću stopu, na primjer, stopu prepoznavanja EER kod otiska prsta [135]. U radu Mjaaland *et al.*, [136] navode da zaštitno pitanje ovog metoda leži u činjenici da je pojedinačno prepoznavanje koraka teško za imitiranje. Nedostaci ovog metoda su u cijeni (cijena senzora), i nepogodnosti (nametanju obaveza za korisnika da nosi senzor).

VI DIZAJN NOVOG MODELA ZAŠTITE INFORMACIJA U SISTEMIMA IAM

6.1. Pregled postojećih modela zaštite informacija

Trend ubrzanog razvoja digitalnih tehnologija stvorio je potrebu povećanog širenja informacija među različitim organizacijama, institucijama, korporacijama, i sl. U tom pogledu, kritično je da se osigura adekvatna zaštita informacija. Sa uporednim razvojem novih tehnologija nameće se potreba za učestalim preispitivanjem zaštite. Da bi zaštita odgovorila novim izazovima potrebno je da ide u korak sa tehnološkim razvojem tj, poboljšanju postojećih i razvijaju novih modela zaštite informacija. Danas postoje brojni različiti modeli za zaštitu informacija. Modeli zaštite definišu osnovu za stvaranje politike zaštite. Cilj svih modela zaštite je da definišu autorizovano i neautorizovano stanje sistema tj. da posredstvom elementa ograniče kretanje sistema prema neautorizovanom stanju. Element je mehanizam (dobro oblikovana transakcija, razdvajanje dužnosti, programi, i sl.) sa kojim se obezbijeđuje bazična zaštita informacija. Modeli su razvijeni prema tipu sistema za koji treba da budu korišćeni. Neki modeli su razvijeni da obezbijede zaštitu za operativni sistem dok su drugi razvijeni za specifične aplikacije kao što su baze podataka [137]. Dakle, mnogi izazovi u modelima zaštite informacija zahtijevaju sveobuhvatan pristup i tehnike u postizanju što boljeg modela zaštite. Danas postoji mnoštvo razvijenih modela zaštite i teorija koji su korišćeni u zaštiti *e-government* prema tehničkim i ne-tehničkim pitanjima [138].

U literature, ne postoji model koji u isto vrijeme pokriva sve bazične aspekte zaštite kao što su integritet, tajnost i povjerljivost. Mnoga istraživanja su bila usmjerena u stvaranje takvog modela koji bi obuhvatio sve aspekte zaštite. Nesumnjivo, veliki broj modela zaštite informacija koji danas egzistira, nastao je upravo kao posljedica stvaranja sveobuhvatnog modela zaštite koji bi mogao pokriti istovremeno sve bazične zaštitne aspekte. Svi ti modeli, po svom stvaranju smatrani su sveobuhvatnim modelom zaštite, koji su kasnije u svom funkcionisanju pokazali određene nedostatke koji su ih učinili ranjivim prema napadima. Većina modela bili su razvijeni da se bave različitim pitanjima zaštite, dovoljnim da podrže neke od bazičnih aspekata zaštite. Međutim, ovaj novi stari izazov je i dalje aktuelan. Izvan svake sumnje, da budući model zaštite treba

da uzima najbolje karakteristike trenutnih modela integrisane u jednu cjelinu sa novim pristupima. Za stvaranje takvog modela potrebno je istražiti neke od sličnosti i različitosti između postojećih osnovnih modela zaštite. Stoga, u ovom dijelu rada daje se komparacija osnovnih i najvažnijih modela zaštite poput *Bell-LaPadula, Biba, Clark Wilson , Take Grant i Sea-View*. U tom komparativnom pristupu *Biba* model je zbog svoje jednostavnosti, lake primjenjivosti i integracionih povoljnosti korišćen kao model za poređenje. Njihov poseban značaj i važnost leži u činjenici što ovi modeli predstavljaju bazičnu osnovu za razvijanje svih drugih modela.

6.1.1. Modeli zaštite

6.1.1.1. Model Bell-LaPadula (BLP)

Model Bell-LaPadula (BLP) je razvijen od Bell i LaPadula (BLP) kao jedan od najranijih i najpoznatijih modela [139]. Ovaj model obezbjeđuje okvir za upravljanje klasifikovanim podacima i radi tog je nazvan višestruki model zaštite [140]. Svrha *BLP* modela je da dobije minimalne zahtjeve u pogledu povjerljivosti koji treba da budu ispunjeni od strane bilo kog višestrukog sistema zaštite. Spada u jedan od najpopularnijih modela zaštite koji štiti povjerljivost informacija unutar sistema.

Postoje četiri komponente za *BLP* model [141]:

1. *Subjekti* su korisnici i sistem sposobni da izvrše procese.
2. *Objekti* su elementi podatka.
3. *Čvorovi pristupa* uključuju čitanje, pisanje, izvršavanje i mogućnost njihovog kombinovanja.
4. *Nivoi zaštite* su suštitnski nivoi klasifikacija zaštite.

BLP model se sastoji od sljedeća dva pravila [142]:

1. Uslov jednostavne zaštite: subjekat ne može čitati podatke ako i samo ako nivo objekta je viši od nivoa subjekta, "*ne čitaj gore*".
2. Zvjezdano svojstvo: subjekat ne može pisati podatke ako i samo ako nivo subjekta je viši od nivoa objekta, "*ne piši dole*".

Ovaj model je zasnovan na informacionom toku u rešetci zaštitnih klasa, sa dopuštenim informacionim tokom samo u jednom pravcu rešetke. Informacioni tok *BLP* modela je

zasnovan na *High Water Mark* principu, koji dopušta informacioni tok na-gore. Dakle, u ovom modelu dopušta se upotreba matričnog kontrolnog pristupa i zaštitnih nivoa pri čemu mandatorna pristupna kontrola sprečava informacioni tok samo između zaštitnih klasa. Politika zaštite zasnovana je na zaštiti informacija slijedeći od višeg nivoa prema nižem nivou. Kao što se može uočiti, glavni nedostatak ovog modela je da model ne riješava druga zaštitna pitanja koja su definisana u jezgru zaštite informacija kao što je integritet i raspoloživost. Nažalost, mandatorne kontrole djelimično rješavaju probleme po pitanju trojanaca. Ipak, ovaj model i pored navedenih nedostataka još uvijek je korišćen kao višestruki zaštitni model, posebno u vojnim i obavještajnim oranizacijama u kojima je povjerljivost podataka od prvorazredne važnosti.

6.1.1.2. Biba model

Biba model je razvijen 1977. godine od strane Bibe [143]. Ovaj model je bio prvi model koji se bavio pitanjem integriteta u informacionim sistemima. *Biba* model štiti integritet informacije unutar sistema i veoma je sličan *BLP* modelu. Nedostaci *BLP* modela su bili osnovna motivacija za stvaranje *Biba* modela s ciljem narušavanja integriteta u kompjuterskim sistemima. *Biba* model po pitanju zaštite informacija ima dva dijela, prvi koji se bavi podesnim širenjem informacije, dok drugi dio se odnosi prema cjelovitosti ili integritetu informacija. Ovaj model je fokusiran na obezbijeđivanje mjera integriteta za subjekat i objekat, i sprečavanje nevidljivog uvođenja podataka sa manjim integritetom unutar definisanog sistema. Ovaj model kao i *BLP* model je takođe zasnovan na informacionom toku u rešetci zaštitnih klasa, sa dopuštenim informacionim tokom samo u jednom pravcu rešetke. Informacioni tok ovog modela je zasnovan na *Low Water Mark* principu, koji dopušta informacioni tok na-dole.

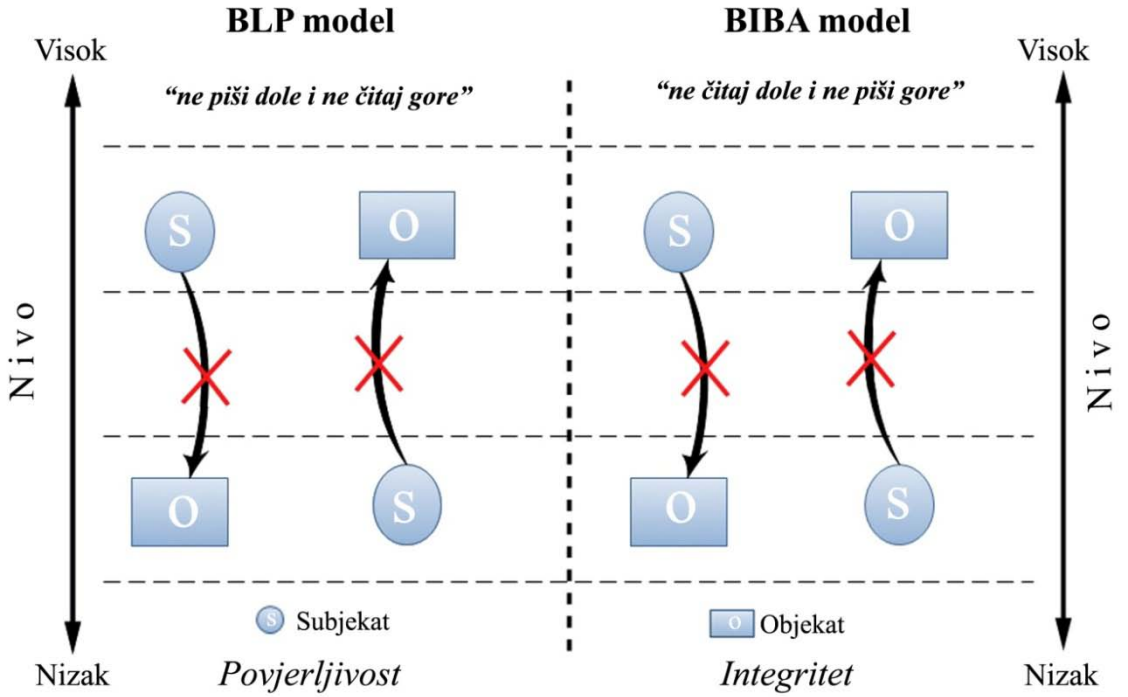
U okviru ovog modela definiše se familija različitih politika koje mogu biti korišćene za primjenu integriteta. Pristup je zasnovan na hijerarhijskoj rešetci nivoa integriteta tj. zasnovan na klasifikaciji zaštite subjekata i objekata gdje je upotrebljen nivo integriteta za klasifikaciju. Dakle, *Biba* model sprečava neautorizovanu modifikaciju podataka i održava nepromjenjivost podataka [144]. Ovaj model dodijeljuje subjektima i objektima integritet naljepnicu koja ukazuje u kom stepenu je povjerljivost dodjeljena prema informacijama. Sastoji se od četiri pristupna moda: modifikovanja, posmatranja, pozivanja i izvršenja [145].

Biba model podržava pet različitih mandatornih politika integriteta [141]:

1. *Low Water Mark Policy*
2. *Low Water Mark Policy for Objects*
3. *Low Water Mark Integrity Audit Policy*
4. *Ring Policy*
5. *Strict Integrity Policy*

U ovom modelu, tri su diskrecione politike uspostavljene: pristupna kontrol lista, hijararhija objekata i prsten. U praksi, mandatorna politika *Biba* modela je najčešće korišćena. Najograničenija politika *Biba* modela je strogo svojstvo integriteta. Upravo, ovo svojstvo integriteta je suštinska suprotnost *BLP* modela. Strogi model integriteta je sastavljen od tri svojstva. Prvi, jednostavno integritet svojstvo dopušta subjektu da primjećuje (čita) objekat koji ima viši nivo integriteta nego subjekat. Subjekat sa višim nivom integriteta ne može da čita objekat sa nižim nivom integriteta – "*ne čitaj dole*". Drugi, integritet stanja zvjezdanog svojstva je da subjekat ne može modifikovati (pisati) objekat koji ima viši nivo integriteta – "*ne piši gore*". Poslednje, svojstvo pozivanja u kojem subjekat ne smije zahtijevati servis od subjekta koji ima viši nivo integriteta. U ovom modelu su uspostavljene brojne druge politike zasnovane na stanju strogog integriteta. Svaka od tih politika je manje restriktivna nego što je politika strogog integriteta. Na primjer, *low-water mark* politike su dinamičnije i nižeg nivoa integriteta subjekta i objekta, koji rezultira u modelu da je lakši za upotrebu ali sa manjim nivoom zaštite. Model ima brojne dinamične politike koje imaju niži nivo integriteta bilo subjekta ili objekta zasnovanog na operacijama pristupnog moda. U radu [137] Korać je dao komparativni pregled *Biba* i *BLP* modela (slika 15).

Ipak, neki autori poput Sandhu-a *et al.*, [146] navode da ne postoji fundamentalna razlika između BLP i Biba modela. Međutim, kako *Biba* model radi suprotno od *BLP* modela, upravo ta činjenica predstavlja glavnu karakteristiku ovog modela jer omogućava njegovu integraciju sa *BLP* modelom kao i mnogim drugim modelima. Jedan od modela kao što je Lipnerov model integriteta, kombinuje *Biba* model i *BLP* model tako što integriše oba principa integritet i povjerljivost [147]. Prednosti *Biba* modela su jednostavnost i laka primjena, kao i stvaranje i upotreba brojnih različitih politika zasnovanih na potrebi sistema. Glavni nedostatak je što nije jasno kako dodijeljuje odgovarajuće nivoe kao i ne postojanje kriterijuma za određivanje istih. Ovaj model ne podržava principe odobrenja i opoziva autorizacija.



Slika 15. BLP naspram Biba modela

Takođe, njegovo ograničenje je što nije striktno korišćen za integritet. Upotreba ovog modela zahtijeva da svi kompjuteri u sistemu moraju imati naljepnicu integriteta za subjekte i objekte. Postoje i drugi problemi u mrežnom okruženju koji ne podržavaju naljepnice integriteta, i sl. [137].

6.1.1.3. Take-Grant model

Take – Grant model je diskrecioni model zaštite [148]. Ovaj model kao i prethodni modeli su primarno teoretski alati korišćeni da analiziraju pitanje zaštite. Za razliku od drugih modela, ovaj model predstavlja okvir u kojem je na pitanje zaštite odgovoreno sa "*da*". Takođe, ovaj model omogućava derivaciju rezultata ukazujući pod kojim pravima mogu biti prenijeti kao i kompleksnost određivanja *da li su ili nisu* ovi uslovi sadržani u partikularnim sistemima.

Ovaj model je u suprotnosti prema *Biba* modelu, koji je uglavnom korišćen da podrži mandatnu politiku koja podržava privilegovanu autorizaciju. Poput *Biba* modela, *Take – Grant* model takođe opisuje zaštitu zasnovanu na subjektima i objektima. Ovaj model upotrebljava usmjereni graf da opiše zaštitna stanja. U grafu, subjekti i objekti su prezentovani kao čvorovi kao što je to *Bishop* predstavio u radu [149]. Pristupni modovi

su predstavljeni na ivici koja povezuje čvorove kao što su subjekat prema objektu. Ivice, takođe imaju naljepnice koje formulišu pridružena prava sa tim. Lukovi između čvorova su označeni sa ovim pristupnim pravima. Ovaj model upotrebljava graf za model pristupa kontrole; model je fundamentalni model matričnog pristupa [151]. Pristupni modovi koji podržavaju Take – Grant model su čitanje, pisanje, odobrenje i opoziv.

U poređenju sa *Biba* modelom, ovaj model predstavlja prošireni model jer podržava operacije odobrenja i opoziva. Pravo odobrenja/opoziva dopušta subjektu da odobri/oduzme mogućnost pisanja koje subjekt posjeduje prema drugom subjektu ili objektu. Pravo odobrenja i opoziva, takođe poznato kao pravo transfera [145], podržava modifikaciju autorizacije sistema koji dopušta pravo da bude prenijeto prema drugom objektu. Transfer prava dopušta subjektu da da ili uzme prava objekta. Na ovaj način savladava se jedan od problema *Biba* modela, kao što je ne obezbjeđivanje bilo koje administrativne opcije za odobrenje ili opoziv autorizacija [151]. Takođe, *Take – Grant* model može lako biti primjenjen za zaštitu baze podataka.

Neki modeli, kao u slučaju *Biba* modela, nisu bili razvijeni za zaštitu baza podataka odnosno veoma ih je teško bilo primjeniti u te svrhe. Svojstvo odobrenja ili opoziva autorizacija omogućava da mnogi sistemi koriste ovaj model za autorizaciju privilegija. Na primjer, *Oracle* upotrebljava *Grant* (odobrenje) komandu da dopusti *Oracle* da zna ko autorizuje korisnika ili ulogu, da ima jednu ili više sistema ili objekata privilegija [152]. Sa druge strane, *Revoke* (opoziv) uklanja privilegiju koju korisnik ima na objektu. Sintakse za dvije komande u *Oracle* su:

grant <privilege> to <USERNAME or ROLE>
revoke <privilege> from <USERNAME>

Međutim, ni ovaj model nije bez nedostataka. Nedostatak ovog modela u odnosu na *Biba* model je što ovaj model ne razmatra pitanje integriteta. Takođe, i ovaj model je ranjiv prema trojancima. Ipak, najveći problem ovog modela je ograničenost u broju čvorova koji mogu biti prikazani u nekom vremenu sa modelom. Grafovi sa velikim brojem čvorova i lukova predstavljaju kompleksan i težak zadatak za pojedinca da shvati i odobri zaštitu.

6.1.1.4. Sea-View Model

Sea – View Model je razvijen od strane Denning *et al.*, na Istraživačkom institutu Stanfordu. Poput *Biba* modela, *Sea View* model koristi mandatnu kao i diskrecionu politiku da upravlja pristupom prema pohranjenim podacima u bazi podataka. Međutim, za razliku od *Biba* modela koji se ne bavi principom tajnosti, *Sea View* model kombinuje oba principa, tajnost i integritet. Ovaj model se sastoji od dva sloja. Prvi, kontrolni pristup – MAC (*engl. Mandatory Access Control*) je obavezan i odgovara prema odgovarajućem referentnom monitoru koji pojačava mandatnu politiku zaštite *BLP* modela. Drugi sloj je povjerljivo izračunavanje baze – TCB (*engl. Trusted Computing Base*) i "*definiše koncept višestrukog nivoa odnosa, podrške diskrecionih kontrola za višestruke odnose i poglede, i formalizovanje podržavajućih politika*" [151].

U MAC modelu, korisniku je dat pristup da klasifikuje informacije zasnovane na korisničkoj dozvoli (autorizacionoj tajnosti i integritetu) za informacije. U ovom modelu mandatna politika je formalizovana u pojmu subjekata, objekata i pristupnih klasa. Takođe, primjenjuju se isti aksiomi koji su korišćeni u *BLP* i *Biba* modelu. Pristupne klase i identifikatori dodjeljeni su za cijeli život objekta i sastoje se iz dvije komponente: tajnost i integritet. Klasa tajnosti odgovara prema nivou zaštite *BLP* modela dok klasa integriteta odgovara prema integritetu nivoa *Biba* modela. Poput *Biba* modela, *Sea – View* model formira povezanost rešetke. Sličnost ovog modela sa *Biba* modelom je u tome što su subjekti definisani kao procesi koji djeluju u ime korisnika. Za razliku od *Biba* modela, svakom korisniku u sistemu koji koristi *Sea – View* model dodjeljeno je područje minimalnih i maksimalnih klasa tajnosti i integriteta unutar kojeg je dozvoljeno korisniku da djeluje. Ove klase su nazvane kao *minzaštita, minitegritet, makszaštita i maksintegritet*. Klase su sastavljene od strane korisnika za pisanje subjekta od para *minzaštita* i *maksintegritet* dok za čitanje od para *makszaštita* i *minitegritet.*

Mandatni pristup modova *Sea – View* modela su: čitaj, piši, i izvršavaj. Operacija čitanja dopušta subjektu da čita informacije pohranjene u objektu. Ova operacija je veoma slična operaciji opserviranja pristupnog moda kod *Biba* modela. Pristupni mod pisanja dopušta subjektu da piše informacije u objektu, dok mod izvršenja dopušta subjektu da izvrši na objektu. Ovi modovi su uporedivi za operacije modifikovanja i izvršavanja kod *Biba* modela, za svakog posebno. U svojstvu čitaj, subjekat *i* može čitati objekat *j* samo ako njegova klasa čitanja dominira klasom pristupa objekta. Ovo

svojstvo je formulisano *ne čitaj – gore* tajnost *BLP* modela, i *ne čitaj – dole* integritet *Biba* modela. U svojstu piši, subjekat *i* može pisati objekat *j* ako njegova klasa pisanja dominira klasom pristupa objekta. Ovo svojstvo je formulisano *ne piši – dole* tajnost *BLP* modela, i *ne piši – gore* integritet *Biba* modela. Na kraju, svojstvo izvršenja dopušta subjektu *i* da izvrši objekat *j* samo ako njegov maksimalni integritet je manji ili jednak nego što je to integritet klase objekta, i njegova maksimalna tajnost je veća ili jednaka nego što je to tajnost klase objekta. Ovo svojstvo savladava ograničenja Bibe modela. Stoga, prema Castano *et al*., [151], *Sea – View* model izvršava pomenuta svojstva na sljedeći način: "*razlikujući pristup izvršenja od pristupa čitanja, dopuštajući povjerljivim subjektima da čitaju podatke manjeg nivoa integriteta nego što je njihov maksimalni integritet, i ograničavaju pristup izvršenja za sve subjekte da programiraju veći ili jednak integritet*".

6.1.1.5. Clark – Wilson model

Clark – Wilson model je razvijen 1987 godine od strane *Clark – Wilson*. U poređenju sa *Biba* modelom, ovaj model predstavlja prošireno područje održavanja integriteta koji se bavi zaštitom integriteta informacija u svrhu sprečavanja, modifikovanja ili krađe informacija u komercijalnim sistemima. Potrebno je naglasiti da su *Clark – Wilson* u radu [153] pravili jasnu razliku između vojne i komercijalne zaštite. Oni dokazuju da politika zaštite u pogledu integriteta predstavlja najviši prioritet u komercijalnim informacionim sistemima za čiju primjenu su potrebni posebni mehanizmi. Dakle, široka upotreba ovog modela je u bankarskim sistemima gdje je integritat važniji nego povjerljivost.

Clark – Wilson predlaže dva nivoa integriteta [154]: *constrained data items – CDIs* (podaci koji su već dio sistema) i *unconstrained data items – UDIs* (podaci koji će biti uvedeni u sistem). Prema, Krause-u *et al.*, [141] ovaj model definiše tri cilja integriteta:

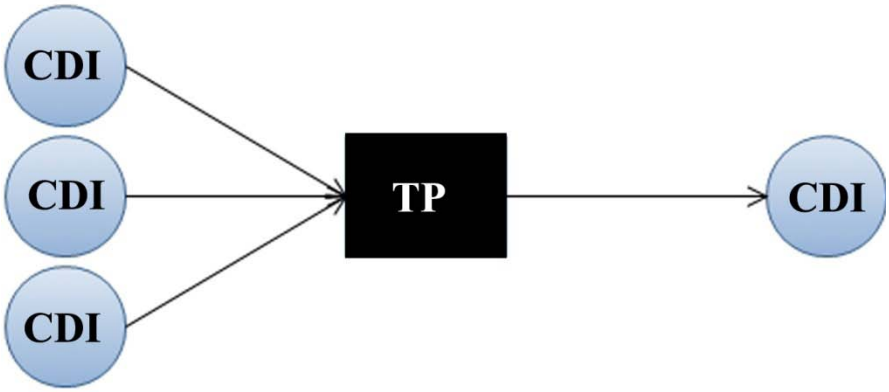
1. Neautorizovani subjekat ne može činiti bilo kakve izmjene.
2. Autorizovani subjekat ne može činiti bilo koje neautorizovane izmjene.
3. Unutrašnja i vanjska nepromjenljivost je održana.

U komercijalnom okruženju, ovi ciljevi su pogodni da obezbijede integritet korporativnih finansija podataka ili zapisa. Prednost ovog modela ogleda se u tome što ne samo da je neautorizovanim pojedincima zabranjen pristup zaštićenim podacima, već

je i autorizovanim pojedincima zabranjeno činjenje izmjena koje mogu rezultirati u gubljenju ili korupciji finansijskih podataka ili zapisa [141]. Ovaj model ima dva primarna elementa za postizanje integriteta podataka: zahtjev za provjerom (dobro oblikovanu transakciju) i razdvajanje dužnosti [141]. Prema tome, ovaj model je integrisani model primjenjen da zaštiti integritet podataka i da obezbijedi kako se desila ispravno oblikovana transakcija. Dobro oblikovana transakcija je struktuirana tako da subjekt ne može proizvoljno manipulisati podacima, već na ograničen način sa kojim se obezbijeđuje *unutrašnja* konzistentnost podataka. Sa ovim principom je uveden princip dualiteta za svaku transakciju. To podrazumijeva zapis svake transakcije na najmanje dva mjesta čime se ostavlja njen dupli trag. Pri tom je neophodno istaći, da postojanje duplog traga nema za cilj kopiranje transakcija već odvajanje zapisa koji je korišćen da potvrdi tačnost i validnost orginalnih transakcija. Dakle, *Clark – Wilson* model u poređenju sa *Biba* modelom dopušta postojanje traga.

Principom razdvajanjem dužnosti sprečava se neodgovarajuća modifikacija podataka od strane autorizovanog korisnika, čime se obezbijeđuje *vanjska* konzistentnost podataka objekta. Drugim riječima, obezbijeđuje se korespodencija među objektima podataka različitih poddijelova zadatka. Ova korespodencija je obezbijeđena kod odvajanja svih operacija u nekoliko poddijelova i zahtijevaju da svaki poddio bude izvršen od strane različitog subjekta. Model integriteta ne primjenjuje klasifikacione nivoe za podatke ili korisnike. Umjesto toga, postavlja se stroga kontrola korisničkog pristupa i upravljanja podacima i programima.

Takođe, ovdje je bitno naglasiti da se kroz princip razdvajanja dužnosti obezbijeđuju i dopunski zaštitni zahtjevi u pogledu korisničke identifikacije, autentifikacije i provjere. *Clark – Wilson* model primjenom principa razdvajanja dužnosti obezbijeđuje integritet podataka kod subjekata na istom ili nižem nivou integriteta, dok je to u *Biba* modelu bilo zasnovano na pretpostavci da subjekti neće namjerno ili slučajno modifikovati podatke. Dakle, dobro oblikovana Transformaciona procedura – TP i integritet verifikaciona procedura – IVP uvedeni su kao sredstvo za osiguravanje ispravnog sistemskog funkcionisanja od jednog stanja do drugog, zasnovanom na jednom ili više ulaza kao što je to prikazano na slici 16 (zasnovano na tri ulaza).



Slika 16. Dobro formirana TP operativna na tri CDI-s sa kombinovanim izlazom

Najčešće TP-s djeluje na skupu CDI-s. Međutim, određeni procesi mogu takođe djelovati na skupu UDI-s kako bi se uveli podaci u sistem. U takvim situacijama dodjeljuje im se naljepnica CDI-s. Verifikaciona procedura potvrđuje da je verifikacija izvršena kada su podaci prilagođeni prema specifikacijama integriteta u vremenu. Transformacione procedure su dizajnirane da ispravno prevedu sistem iz jednog u drugo stanje. Ipak, *Clark – Wilson* model pretpostavlja pojedinačni visoki nivo integriteta primjenjen prema CDI-s, dok model kao što je *Biba* sa eksplicitnim pravima za upravljanje sistema podataka na nivoima višestrukog integriteta može biti inkorporisan unutar tog modela [144]. Autori ovog modela su vjerovali da se bave sa sve tri cilja integriteta. U literaturi se može pronaći nekoliko aplikacija i različitosti *Clark – Wilson* modela kao što su [144, 155]. Ipak, na kraju je potrebno istaknuti, da ovaj model je kompleksan i ne riješava druga pitanja zaštite [143].

6.1.2. Ograničenja osnovnih modela zaštite

U ovom dijelu rada diskutuje se o problemima koji mogu narušiti bazična načela zaštite informacija. Problemi modela zaštite informacija manifestuju se pri njihovoj upotrebi. Prije svega, to su neočekivani problemi koji nastaju pri praktičnoj primjeni nekog modela zaštite. Dakle, modeli zaštite imaju teoretska ograničenja. Ne može se uvijek dokazati da model zadovoljava određene uslove zaštite. Praktično, primjenom određenog zaštitnog modela pojavljuju se problemi koji nisu teoretski mogli biti identifikovani. Sa druge strane, modeli zaštite informacija koji su zasnovani na strogim matematičkim svojstvima mogu da vode ka sistemima koji su potpuno neupotrebljivi. Razvijanje sistema zasnovanih na strogim matematičkim modelima zaštite je ekstremno vremenski zahtjevan i veoma skup proces. Ovakvi modeli zaštite nisu ekonomski

isplativi, i radi toga većina komercijalnih sistema neće biti zasnovana na formalnim modelima. Modeli zaštite i formalne metode ne omogućavaju uspostavljanje zaštite sistema. U slučajevima, ako bi dokazljivost bazičnog principa zaštite i bila moguća, to nije prihvatljivo rješenje. Razlog je što model zaštite u trenutku testiranja može da potvrdi sigurnost sistema, dok već u sljedećem testiranju može pokazati određene ranjivosti.

Nesumnjivo, čovjek predstavlja najveću prijetnju i ranjivost bilo kog modela zaštite. Ljudski faktor i socijalni inženjering mogu da kompromituju i najzaštićenije sisteme. Takođe, kontinuirani napredak digitalnih tehnologija stvorio je uslove za razvoj novih oblika prijetnji po modele zaštite. Brz i snažan razvoj digitalnih tehnologija uslovio je da mehanizmi zaštite za koje se mislilo u određenom vremenu da su sigurni u bliskoj budućnosti se pokazalo da su potpuno nesigurni. Primjer za ovo su kriptografski algoritmi. Zbog snažnog razvoja procesorske moći kompjutera, algoritmi poput DES koji su po razvijanju smatrani najsigurnijim algoritmima u veoma kratkom periodu nisu se mogli više smatrati sigurnim. Sa razvojem procesorskih kompjuterskih perfomansi takvi algoritmi su u trenu bili razbijani. Dakle, bez obzira koji je model zaštite primjenjen u sistemu, sistem će uvijek biti izložen kontinuiranom riziku od moguće zloupotrebe.

Nesumnjivo je da *Clark – Wilson* model obezbijeđuje opšti okvir u kojem je moguće upravljati integritetom podataka primjenom strogog vodiča. Međutim, ovaj model u poređenju sa *Biba* modelom dopušta za procese da djeluju na višestrukim izvorima podataka ali nijedan od modela ne razmatra kako postojanje višestrukih izvora povezanih podataka mogu uticati na njihov nivo dodjeljenog integriteta. Na primjer, neki dio podatka može povećati ili smanjiti nivo integriteta drugog podatka zasnovanog na tom da li je podatak potvrđen ili kontradiktoran, i zasnovanog na stepenu nezavisnosti izvora podataka. Nadalje, modeli ne obuhvataju kontekstualne informacije kod kojih je nezavisnost zaključena.

Na osnovu diskusije ograničenja modela zaštite došlo se do zaključka, da i pored brojnih razvijenih modela zaštite, ne postoji savršen model tj. model koji u isto vrijeme pokriva sve bazične aspekte zaštite. Kako je kompjuterska zaštita uvijek dio reakcionog procesa, potpuno je svejedno koji će model zaštite biti primjenjen, problemi će uvijek iznova iskrsavati. Ukoliko jedan model zaštite ima nedostatke u određenom pravcu, u

drugom modelu koji se pojavi kao korektura, obavezno se javljaju problemi druge prirode. Razlozi mogu biti uzrokovani ljudskim faktorom kao i ubrzanim razvojem digitalnih tehnologija. Nesumnjivo, prijedlog za ublažavanje identifikovanih problema je usmjeren prema stvaranju odgovarajućih alata koji će značajno onemogućiti ili odvratiti napadače u namjerama zloupotrebe informacija. Za praktičnu primjenu zaštite informacija u većini slučajeva potrebna je primjena više od jednog modela zaštite [137].

6.2. Pregled postojećih autentifikacionih rješenja

Sva postojeća autentifikaciona rješenja su bila razvijena u pogledu nekog od korisničkih faktora kao što su zaštita, upotrebljivost, pristupačnost, kompleksnost, cijena, privatnost i pogodnost (SUAPCPC)[6]. Nesumnjivo da je najveći broj autentifikacionih rješenja, poput [156-163] obuhvatao kao primarni fokus pitanje zaštite, upotrebljivosti i pristupačnosti. Takva pitanja su razmatrana pojedinačno ili uzajamno. U prethodnom radu Vapen i Shahmehri [163] pokrivaju različita područja autentifikacije i ukazuju da ne postoji komparacija metoda autentifikacija specifično napravljena za mobilne uređaje. Takođe, u radu [164] Burr *et al.*, pokrivaju različita područja autentifikacije i diskutuju o zaštitnim zahtjevima kao jedinom korisničkom faktoru. Ipak, sa uvidom u prethodne radove, nije bilo moguće naći jedinstveno mobilno autentifikaciono rješenje u pogledu "*najpogodnijeg*" šablona za mobilne autentifikacije.

6.2.1. Pregled kriterijuma za komparaciju i komparacija

Postoji značajan broj radova koji su dali pregled različitih biometrijskih autentifikacija [92, 163]. Njihovi istraživački programi su naglasili važnost različitih komparativnih pristupa u metodama autentifikacija zasnovanih na biometrijskim tehnologijama, gdje svaki fokus usredsređen na specifično pitanje ili poglede iz određene perspektive. Na primjer, Clarke i Furnell [92] su predstavili rezultate komparacije perfomansi biometrijskih tehnologija koje je vodio *The UK National Physical Laboratory.* Na osnovu prezentovanih rezultata moguće je zaključiti da je komparacija zasnovana na nekoliko biometrijskih metoda, čija je primjenjivost prema mobilnim uređajima bila diskutovana. Takođe, potrebno je istaknuti da je O'Gorman [165] bio jedan od prvih

[6] Da bi se u izbjegla konfuzija pri upotrebi ovih korisničkih faktora u matematičkim jednačinama u nastavku disertacije ovi faktori su u jednačinama (2) i (6) označeni sa $SUAP_1C_1P_2C_2$.

koji je poredio metode autentifikacije lozinke, tokena i biometrije zasnovanih na glavnim komparativnim faktorima kao što su zaštita, pogodnost i cijena. Postoji mnogo radova kao što su [108, 156, 157, 162, 163], čiji primarni fokus je uključivao prioritete kao što su zaštita, upotrebljivost i pristupačnost. Helkala i Snekkenes [166] su se bavili različitim područjima autentifikacije u pogledu na korisničke faktore kao što su zaštita, cijena i upotrebljivost. Vapen and Shahmehri [163] su pokrivali i diskutovali unutar različitih područja autentifikacija zasnovanih na korisničkim prioritetima kao što su zaštita, upotrebljivost i dostupnost. Burr *et al.,* [164] su pokrili i diskutovali unutar različitih područja autentifikacija zasnovanih na prioritetu zaštite, kao jedinom korisničkom prioritetu. Sa druge strane, postoji više radova koji su pokrivali komparacije unutar kategorije. Primjer su Pond *et al.,* [167] koji su pokrivali komparaciju unutar kategorije *"nečemu što znaš*", Abott [168] i Husemann [169] unutar kategorije *"nešto što imaš*", dok Maio *et al.,* [170], Phillips *et al.,* [171], Mansfield i Wayman [172], i Maltoni *et al.,* [97] unutar kategorije *"nešto što jesi*". Takođe, u radu Maltoni *et al*., [173] kao i Karovaliya *et al.,* [174] bavili su se komparacijom opštih korišćenih biometrijskih svojstava gdje su deskriptivne vrijednosti klasifikovane u tri nivoa (visok, srednji i nizak).

U nekoliko istraživačkih studija [12, 175-178], pored komparativne procjene veb metoda autentifikacija, autori su predložili okvire za kvantifikovanje vrijednosti različitih metoda autentifikacija zasnovanih na nekom od SUAPCPC faktora. Renaud [175] je predložio okvir za komparaciju metoda autentifikacija u kojem posmatrani prioriteti imaju iste težine i važnosti. Ovaj okvir obezbijeđuje odvojenu izlaznu vrijednost za posmatrane korisničke prioritete ali sa kvantifikovanim sveukupnim rezultatom bez numeričke vrijednosti. Bonneau *et al.,* [176] su predložili okvir za procjenu aspekata na pojedinačnom nivou za korisničke prioritete kao što su upotrebljivost, zaštita i *deployability* ali ne dodijeljuju konkretnu numeričku vrijednost. Termin *deployability* predstavlja kombinaciju korisničkih prioriteta pristupačnosti (korisnika sa invaliditetom) i cijene. Takođe, u tom istraživanju je dat prijedlog od 25 kriterija koji mogu biti opaženi kao karakteristike potrebne za razvoj idealnog metoda autentifikacije. Nedostaci ovog okvira predstavljaju lingvistički pojmovi kojima su izražene vrijednosti i težine kriterijuma, kao i nepostojanje integrisane vrijednosti koja dopušta lakšu sveukupnu komparaciju između procijenjenih metoda autentifikacija. Ovaj okvir omogućava promjenu težine kriterijuma zasnovanih na specifičnim ciljevima prema kojima su metode autentifikacija poređene ali se pri tom ne daje mogućnost

promjene težinskih kriterijuma za pojedinačne korisničke prioritete. Mihajlov *et al.*, [177, 178] su dali konceptualni okvir, koji u poređenju sa [175] uključuje i alternativni matematički model ali sa smanjenjenim brojem korisničkih prioriteta koji smanjuju i izlazni okvir. Fokus ovog okvira je bio na vrijednostima posmatranih korisničkih prioriteta gdje je integrisana vrijednost data kao krajnji rezultat procjene. Kiljan *et al.*, [12] su bili predložili okvir koji proširuje [175] sa aspekta povezanosti prema korisničkom kriterijumu upotrebljivosti. Takođe, u tom istraživanju autori su u manje detalja poredili sve gore pomenute okvire sa [175]. Cilj takvog istraživanja je bio usmjeren na procijenu različitih implementiranih i predloženih onlajn metoda autentifikacija korišćenih u bankarskom sektoru, i identifikacija mjesta za daljnja poboljšanja. Osim toga, Kiljan *et al.,* [12] su dali informacionu šemu za univerzalni pristup koji može biti primjenjen za dizajn metoda autentifikacija koje mogu obuhvatiti mnoge korisničke prioritete. Ponuđena rješenja u svim gore pomenutim istraživanjima predstavljaju samo jedno rješenje (zasnovano na jednom ili više SUAPCPC faktora) kao jedan okvir iz skupa mogućih okvira.

U prethodnim radovima, univerzalni pristupi u mobilnim metodama autentifikacija su bili razvijeni u pogledu da se ponudi više autentifikacionih rješenja za isti pristup prema aplikativnim područjima. Primjer za ovo je *Fast Identity Online (FIDO) Alliance* [179] koji podržava nFA u formi *Universal Authentication Framework* (UAF) i *Universal Second Factor* (U2F) protokola. FIDO omogućava kombinovanje različitih metoda zasnovanih na dva faktora autentifikacije u korisničko-prijateljskom okruženju. Sa ovom metodom pokušava se postići pristup za što je moguće veći broj korisnika. FIDO metod obuhvata sve SUAPCPC faktore ali ne u istom ponuđenom rješenju. U istraživačkom radu, Sabzevar and Stavrou [180] su takođe dali *Universal Multi-Factor Authentication.* U tom istraživanju, pametni telefoni su korišćeni kao drugi faktor autentifikacije u konjukciji sa grafičkom lozinkom koja omogućava primjenu različite grafičke prezentacije. Može se primjetiti da gore prezentovani univerzalni pristupi nisu dali numeričku vrijednost ponuđenih metoda autentifikacija. Da bi se ublažili ovi problemi, nove metode autentifikacije su razvijene. Takve metode ukazuju da je moguće postići istovremeno poboljšanje različitih korisničkih prioriteta. Primjer za ovo je *Harmonized Authentication based on ThumbStroke dynamics* (HATS) [181]. Ovaj metod ukazuje da je moguće istovremeno postići poboljšanje korisničkih prioriteta kao što su zaštita i upotrebljivost.

Takođe, sa uvidom u prethodne radove nije bilo moguće pronaći kvantifikovanje nFA metoda. Dakle, istraživanja opisana u ovom radu su razmatrana kroz *Fishbone* model. Ovaj model je sve ključne korisničke kriterije i savremene mobilne metode integrisao u jednu cjelinu. Istraživanja opisana u ovoj disertaciji proširuju listu korisničkih kriterijuma prilikom poređenja mobilnih metoda autentifikacija. Svrha ovog istraživanja je da izdiferencira prednosti i nedostatke mobilnih metoda autentifikacija, i na osnovu tih rezultata da se napravi komparacija u pogledu SUAPCPC faktora. Dakle, glavna svrha ovog rada nije direktna komparacija između metoda autentifikacija zasnovanih na SUAPCPC faktorima već opšta analiza i daljnja upotreba razultata za razvoj *Fishbone* modela. Međutim, da bi se došlo do komparativnih rezultata potrebno je prethodno dati pregled i opis SUAPCPC faktora.

6.2.1.1. Zaštita

Zaštita je prvi i najvažniji korisnički faktor u svim procesima autentifikacija, značajan za korisnike i SP-e. U radu [182] Memon *et al.,* su naveli da je zaštita postala suštinska tema u trenutnim mobilnim i bežičnim mrežama. Definisanje zaštite u informacionom društvu nije trivijalno. Teškoće leže u činjenici definisanja pojma zaštite koji pokriva različite aspekte zaštite informacija na različitim nivoima. U kontekstu ovog rada, zaštita je definisana kao grupa metoda, tehnika i aktivnosti koje imaju za cilj da spriječi krađu ili neovlašćenu modifikaciju informacija. Bazični cilj i svrha pitanja zaštite su sadržana unutar osnovnog zaštitnog trojstva pouzdanosti, integriteta i dostupnosti. Pored, postojanja osnovne zaštite informacija postoji još komplementarna zaštita informacija koja uključuje identifikaciju, autentifikaciju, autorizaciju, nadgledanje, tajnost i neporecivost. Zaštita zahtijeva sveobuhvatni integrisani pristup u procesima autentifikacije u kojem je potrebno da podržava poslovni cilj ili misiju kompanije.

Međutim jedan od bazičnih problema je taj što tradicionalni mehanizmi mobilnih metoda autentifikacija su ekskluzivno fokusirani na interes zaštite definisan u polju inženjeringa zaštite. To podrazumijeva da visok nivo zaštite kao ključni faktor je često preporučen i korišćen bez razmatranja drugih korisničkih prioriteta. Stoga, moguće je reći da faktor zaštite blisko subordinira sve druge korisničke faktore. Nivo zaštite može biti različit u mobilnim autentifikacionim rješenjima. Pored upotrebe hardverskih uređaja, na nivo zaštite veliki uticaj ima upotreba različitih kanala i metoda autentifikacije. Upotreba nivoa zaštite koristi se u procijeni zaštite u autentifikacionim

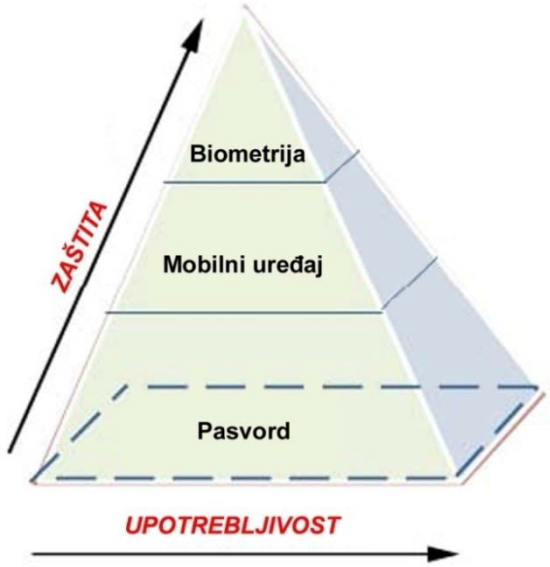
rješenjima. U tom kontekstu je veoma važno naglasiti, da nivoi zaštite koji su trenutno korišćeni kao uobičajena IT rješenja nisu specifično fokusirana na mobilne uređaje. Primjer je *The Electronic Authentication Guideline from NIST* [164] koji definiše četiri nivoa zaštite (1 - 4 gdje je nivo 4 najveći). Zaštita kao SUAPCPC faktor ima za cilj da postigne viši nivo zaštite.

6.2.1.2. Upotrebljivost

Upotrebljivost je faktor ništa manje važan nego zaštita. U radu [162], Pribeanu *et al.*, su naveli da postoji opšta saglasnost oko pitanja upotrebljivosti u smislu da ovaj faktor zauzima sve veću važnost u autentifikacionim pristupima. Postoji značajan broj radova koji su dali definiciju upotrebljivosti kao što su [183, 184]. U kontekstu ovog rada, upotrebljivost je preliminarno definisana kao sposobnost prema ostvarivanju optimalnih interakcija sa sistemskim funkcionalnostima [157]. Prema tome, upotreba ovog faktora podrazumijeva da mobilne metode autentifikacije budu lako razumljive za korisnika. U preglednom radu [185], Harrison *et al.*, su identifikovali u pojmu upotrebljivosti sedam mjerljivih atributa efektivnost, učinkovitost, zadovoljstvo, učitljivost, memorljivost, greške i kognitivno punjenje. Prema Bevan-*u* [186], atributi zadovoljstva uključuju dopadljivost, uživanje, komfor i povjerenje. Upotrebljivost je suštinski faktor u mobilnim metodama autentifikacija, mnogo značajniji nego mobilna nFA rješenja koja su podržana kriptografskim i biometrijskim ključevima.

Zanemarivanje činjenica da korisnici imaju različite fizičke i mentalne sposobnosti, potrebe, godine i umijeća mogu, iz korisničke perspektive, rezultirati da ponuđene metode autentifikacije u slučaju da ih korisnik ne uspije iskoristiti budu potpuno beskorisne. Postoji takođe nekoliko srodnih radova [187-189] u kojima su se autori bavili isključivo problemima u vezi sa mobilnim uređajima i prihvatanjem novih funkcija. Postizanje dobre upotrebe je izazov za male uređaje. Veliki broj različitih mobilnih uređaja čije su sve operacije pomalo različite čine ovo još izazovnijim. Upotrebljivost kao faktor omogućava korisniku jednostavnu i laku upotrebu samog autentifikacionog sistema čime se smanjuju barijere za njegovo usvajanje. Zaista, upotrebljivost se prožima kao pitanje od velike važnosti u mobilnom okruženju u kojem se primjenjuju metode autentifikacije.

Visok nivo upotrebljivosti ima nekoliko benefita za korisnike kao što su smanjenje nivoa greške, minimiziranje zahtjeva za obuku, povećano prihvatanje, povećana efikasnost i produktivnost [190, 191], i ima snažan uticaj na korisnika sa specifičnim potrebama [158]. Takođe, uvidom u istraživačke studije o e-bankarstvu koje su vođeni od strane Weir-a *et al.*, [192, 193] može se zaključiti da povećana upotrebljivost vodi ka siromašnoj zaštiti i obrnuto. Odnos zaštite i upotrebe kao dva osnovna faktora u opštim metodama autentifikacija je predstavljen na slici 17.



Slika 17. Odnos zaštite i upotrebe opštih mobilnih autentifikacinih tehnologija

Na slici 17 se može vidjeti da teoretski posmatrano, pojedinačni metod autentifikacije sa ostvarenim većim nivoom zaštite ima manju korisničku upotrebu i obrnuto. Nesumljivo, ova dva korisnička faktora se nalaze u određenom balansu. Povrh toga, visok nivo upotrebljivosti je povezan prema kompleksnosti. Nizak nivo kompleksnosti ima za cilj da postigne viši nivo upotrebljivosti i obrnuto. U kontekstu postizanja višeg nivoa upotrebljivosti može se zaključiti da sva buduća autentifikaciona rješenja treba da vode ka smanjenju korisničkih aktivnosti potrebnih da izvrše autentifikaciju uz postizanje što većeg nivoa zaštite. Upotrebljivost kao SUAPCPC faktor ima za cilj da postigne viši nivo vrijednosti.

6.2.1.3. Pristupačnost

Pristupačnost je posebno važan faktor iz korisničke perspektive. Pristupačnost može biti posmatrana kao sposobnost za upotrebu i benefite od entiteta (na primjer uređaj,

interfejs, izvori, sistem, servis ili okruženje), i takođe je korišćena da opiše stepen za koji različiti entiteti mogu biti upotrebljeni kod što je moguće većeg broja korisnika [158]. Ovaj faktor podrazumijeva, kao i faktor upotrebljivosti, da autentifikacija treba da bude dizajnirana u što moguće jednostavnijem obliku tj. lako razumljiva i pristupačna za korisnika. U tom kontekstu posmatranja, najbolja mobilna autentifikaciona rješenja biće potpuno beskorisna ako su nepristupačna. Problem pristupačnosti je fokusiran na sprečavanje korisničkog pristupa u procesu autentifikacije. U literaturi, neki radovi veoma blisko povezuju pristupačnost sa upotrebljivošću. Na primjer, Thatcher *et al.,* [194] su naveli da je pristupačnost podskup od upotrebljivosti.

Međutim, uzimajući u obzir sedam gore pomenutih atributa od upotrebljivosti, može se zaključiti da atribut zadovoljstva je mnogo manje važno pitanje za pristupačnost. Faktor pristupačnosti se mnogo više tiče tehničkog aspekta atributa kao što su opažljivost, operabilnost i razumljivost. Sa ovim atributima faktor pristupačnosti čini efektivnijim i efikasnijim proces autentifikacije i svrstava ga u važan korisnički faktor. Za razliku od faktora upotrebljivosti, faktor pristupačnosti je fokusiran prema korisnicima sa invaliditetom. Na primjer, korisnik sa invaliditetom u pogledu prema pristupu je u nedostataku u odnosu na korisnika bez invaliditeta. Zbog svih navedenih činjenica, u ovom radu je faktor pristupačnosti odvojeno razmatran od faktora upotrebljivosti. Pitanja invaliditeta korisnika se odnose na oštećenja kao što su vizuelna, slušna, mobilnosti, kognitivna [195], i govorna oštećenja. Postoji značajan broj radova [196-198] koji su se bavili ovim pitanjima. Jedno od mogućih rješenja za ove probleme je upotreba pomoćnih tehnologija. Međutim, ova rješenja su uslovljena sa korisničkim znanjem i sposobnostima rukovanja pomoćnim tehnologijama. Ipak, postoje i drugi problemi pristupačnosti koji su zavisni od konteksta upotrebe, područja i prirode zadataka koji će biti izvršene, kao i tehnoloških uređaja i korišćenja infrastruktura [194]. Svakako, prema Stephanidis-u *et al.,* [199] univerzalni pristup promoviše ovaj faktor nezavisno od individualnih sposobnosti i karakteristika, područja i prirode zadataka, kao i konteksta upotrebe. Unutar ovog rada, takav koncept univerzalnog pristupa je zadržan. Pristupačnost kao SUAPCPC faktor ima za cilj da postigne viši nivo vrijednosti tj., da omogući efektivniji način pristupa prema autentifikacijama za različite korisnike u različitim situacijama. Postizanje višeg nivoa pristupačnosti u autentifikacionim rješenjima je moguće pod uslovom da upotreba komunikacionih kanala nije zasnovana na upotrebi pomoćnih tehnologija. Generalno, u mobilnim autentifikacionim pristupima

upotreba pomoćnih tehnologija negativno utiče i na druge faktore kao što su kompleksnost, cijena i upotrebljivost. Ove činjenice ukazuju da pristupačnost nije samo povezana prema upotrebljivosti već takođe i prema drugim faktorima.

6.2.1.4. Cijena

Cijena je drugi važan faktor u svim komercijalnim sistemima. Cijena kao faktor zaoukuplja sve veću pažnju u mobilnim autentifikacionim pristupima. Postoji mnogo definicija pojma cijene ali u kontekstu ovog rada cijena je definisana kao novčano izražena vrijednost mobilnog autentifikacionog rješenja. Dva ključna cilja ovog faktora su osjećaj zadovoljstva za korisnike i profitabilnost za SP-e. Cijena je suštinski faktor za postizanje profitabilnosti. Visoka cijena je limitirajući faktor za širu upotrebu mobilnih metoda autentifikacija. Sa druge strane, visoka cijena posmatrano iz korisničke perspektive utiče na neprihvatanje novih autentifikacionih sistema. Takav pristup rezultira neinvenstiranjem u nove sisteme za SP-e. Iz navedenog može se zaključiti, da je cijena veoma važan faktor za sve učesnike u sistemu. Ključni problem ovog faktora (visoka cijena) je usmjeren prema tehničkom aspektu. Na primjer, upotreba pomoćnih tehnologija može zahtijevati dodatnu upotrebu opreme kao što su, kabl, čitač, i sl. Upotreba pomoćnih tehnologija u procesima autentifikacije doprinosi povećanju cijene. Cilj ovog faktora je da se postigne što je moguće manja vrijednost. Dakle, cijena kao SUAPCPC faktor ima za cilj da postigne niži nivo vrijednosti.

6.2.1.5. Kompleksnost

Kompleksnost je relativan pojam koji je jednako važan faktor za oba učesnika, korisnika i SP-a. U kontekstu ovog rada, kompleksnost je definisana kao faktor koji se bavi sa analizom kompleksnog ponašanja mobilnih autentifikacionih rješenja u mobilnom okruženju. To podrazumijeva da se mobilno autentifikaciono rješenje sastoji najmanje od dvije ili više tehnologija, njihovih međusobnih odnosa i povezanosti sa mobilnim okruženjem. Dakle, pitanje kompleksnosti je povezano sa mobilnim tehnologijama [200]. Svakako, razvoj novih tehnologija ima veliki uticaj na ovaj faktor. To se može dvostruko tumačiti. Prvo, nove tehnologije mogu učiniti stvari lakšim, manje složenim, prijateljskim, i nude viši osjećaj prijatnosti za korisnike. Drugo, ova tehnologija zahtijeva određeni nivo vičnosti koja može stvoriti kompleksne probleme za mnoge korisnike, posebno za starije životne dobi. To je dobro poznat problem u kojem stariji

korisnici doživljavaju poteškoće u prihvatanju novih tehnologija. Takođe, kompleksnost kao faktor treba da promoviše osjećaj prijatnosti za korisnike. Da bi postigli taj cilj u procesima autentifikacija potrebno je da dodatna oprema bude korišćena što je moguće manje i da bude napravljena za upotrebu na najjednostavniji mogući način. Veća upotrebljivost određenih mobilnh metoda autentifikacija postiže se smanjenjem kompleksnosti i obrnuto. Radi toga, kompleksnost kao SUAPCPC faktor ima za cilj da postigne niži nivo vrijednosti.

6.2.1.6. Privatnost

Privatnost je veoma kompleksan i subjektivan faktor sa različitim značenjima prema različitim korisnicima. U radu [201] i [202], autori su dali poglede na nekoliko istraživanja po pitanju privatnosti i njegovih aspekata. U kontekstu ovog istraživanja, značenje privatnosti je povezano prema senzitivnosti korisnika i metodama autentifikacija u kojima su informacije korišćenje. Prosto rečeno, u sajber prostoru pitanja privatnosti je moguće narušiti sa otkrivanjem detalja korisničkog profila odnosno personalnih informacija. Stoga, privatnost je definisana kao limitirajući faktor u sprečavanju narušavanja korisničke autonomnosti i slobode u prihvatanju mobilnih metoda autentifikacija. Tokom protekle decenije, usljed razvoja mobilnih tehnologija i mreža, privatnost postaje sve veća briga za korisnike. U radu [203], Ntalkos *et al.*, su posebno naglasili značaj i važnost pitanja privatnosti u mobilnim autentifikacijama, dok u radu [204] Bettine *et al.*, su se bavili cjelovitim pogledom problema privatnosti kao i tehničkim izazovima.

Sa razvojem mobilnih tehnologija, mnoge biometrijske metode su postale pristupačne za širu upotrebu. U mobilnim metodama autentifikacija, zbog visoke osjetljivosti biometrijskih kredencijala upotreba biometrijskih metoda uvijek uzdižu pitanje privatnosti. Mnoge zemlje su usvojile oštre zakonske mjere za pitanje privatnosti. Nesumnjivo, pitanje privatnosti je povezano prema pravu i politikama. Prema Veeningen-u *et al.*, [205] jedan od ključnih principa u zaštiti privatnosti je minimizacija podataka. Unutar konteksta ovog rada, ovaj princip podrazumijeva da proces autentifikacije potrebno da bude izvršen sa minimalnom količinom informacija. Da bi to bilo postignuto, potrebno je da se razmotre svi tehnički aspekti koji mogu obezbijediti visok nivo privatnosti. Uzimajući u obzir gore pomenuto, mobilna autentifikaciona rješenja treba da budu razvijena tako da omoguće maksimalno postizanje privatnosti

umjesto da se isključivo oslanjaju na pravne mjere. Na taj način, moguće je da se postigne visok nivo privatnosti. Takođe, postizanje najvišeg nivoa privatnosti moguće je ostvariti primjenom anonimnosti i pseudonimnosti. Ovi pojmovi podrazumijevaju da korisnici žele da ostanu neprimjećeni i neidentifikovani tokom procesa autentifikacija. Postoji značajan broj radova koji naglašavaju važnost privatnosti u bliskoj budućnosti posebno u pogledu e-glasanja. Primjer je rad [156] u kojem Fuglerud i Røssvoll navode da je pitanje privatnosti među glavnim nedostacima u pogledu primjene e-glasanja. Privatnost kao SAUPCPC faktor ima za cilj da postigne viši nivo vrijednosti.

6.2.1.7. Pogodnost

Pogodnost je takođe veoma važan faktor u svim komercijalnim sistemima. Njegova važnost je posebno naglašena u e-bankarstvu u kojem je prisustvo pogodnosti poželjnije nego postizanje visokog nivoa zaštite [192]. Ovaj faktor predstavlja suštinsku motivaciju u fundamentalnom korisničkom naginjanju na upotrebu određenog mobilnog metoda autentifikacije. Postoji mnogo definicija pogodnosti, ali u kontekstu ovog rada pogodnost je definisana kao korisnička sposobnost da se izvrši proces autentifikacije na što je moguće komforni način. To podrazumijeva da proces autentifikacije treba da bude izvršen u najkraćem vremenu sa najmanjim rasipanjem energije. Kao i faktor upotrebljivosti, i ovaj faktor je takođe povezan prema faktoru cijene. U istraživačkoj studiji [206] Jiang *et al.*, su ukazali da povećana pogodnost može biti postignuta sa višom cijenom i obrnuto. Korisnička želja za pogodnijim mobilnim metodama autentifikacije je povezana sa tehnološkim napretkom. Dakle, ovaj faktor je zavisan od razvoja novih tehnologija koji mogu povećati pogodnost i povećati korisničko zadovoljstvo [207]. Sa druge strane, O'Gorman [165] je naglasio da faktor pogodnosti smanjuje administrativne cijene, na primjer, resetovanje lozinke. Nadalje, u tom istraživanju je istaknuto da, ako je metod autentifikacije pogodan tada on predstavlja preduslov da bude ispravno i upotrebljen. Prema tome, pogodnost kao faktor treba da promoviše osjećaj zadovoljstva kod korisnika. Zbog toga, pogodnost kao SUAPCPC faktor ima za cilj da postigne viši nivo vrijednosti. Na kraju, potrebno je istaknuti da u komercijalnim sistemima organizacije su odgovorne za biranje pogodnosti nekog mobilnog autentifikacionog rješenja i to na osnovu balansiranja faktora:

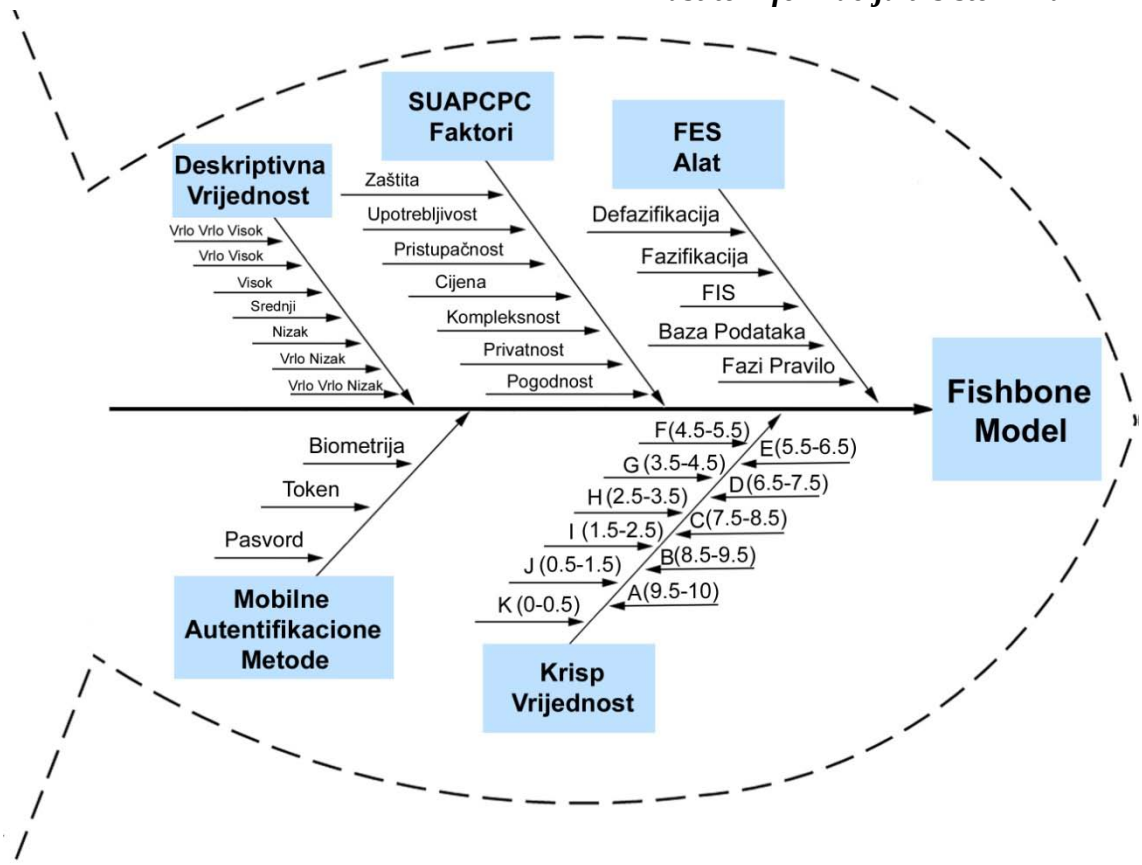
- zaštite naspram cijene odnosno vrijednosti imovine koja se štiti,
- upotrebljivosti naspram privatosti,
- dostupnosti naspram kompleksnosti.

Zaista, u svijetlu svih gore navedenih razmatranja može se zaključiti da je problem jednog faktora značajan kao poseban tip problema drugog faktora. To ukazuje da u mobilnom autentifikacionim pristupima uticaj takvih faktora nije partikularan već simultanog karaktera. U ovom radu, sve te prezentovane činjenice kao i navedene činjenice od strane drugih autora potvrđuju da SUAPCPC faktori su blisko povezani. Stoga, svaki SUAPCPC faktor igra veoma važnu ulogu u savremenim korisničkim metodama autentifikacija.

6.3. Prijedlog novog Fishbone modela zaštite informacija u sistemima za IAM

U ovom dijelu rada, prijedlog novog modela – *Fishbone* modela za zaštitu informacija u sistemima za IAM je dat na slici 18. Kada se govori o pojmu modela potrebno je naglasiti da su modeli korišćeni u opisu koncepta nejasnoće. Prije svega, modeli su mnogo puta korišćeni u prezentovanju složenih sistema, pojmova, termina ili u prezentovanju kompleksnih teorija, učenja lekcija ili razmišljanja. Prema Fournier-Bonilla-u *et al.*, [208] model predstavlja alat koji je često korišćen da razjasni i uprosti kompleksne teorije. Zapravo, značaj i važnost pojma modela je što obezbjeđuju korisnu strukturu za koncepte koji opisuju kompleksnosti i nejasnoće.

U opštem smislu, modeli mogu biti shvaćeni kao tipska rješenja za probleme u organizacijama koji omogućavaju smanjenje šarolikosti organizacionih zahtjeva. U mobilnom autentifikacionom pristupu, modeli mogu biti shvaćeni kao tipska rješenja za probleme u autentifikacijama koji omogućavaju krisp procjenu mobilnih autentifikacionih rješenja. Stoga, za modele se može reći da predstavljaju intelektualni alat koji je fokusiran na ključne elemente ignorišući manje važne detalje. Pojedinačne mobilne metode autentifikacije namjenjene za mobilne uređaje su naizgled veoma jednostavne ali suštinski su veoma kompleksne. Kompleksnost se pojavljuje pri dizajniranju nFA rješenja. Matematički, *Fishbone* model (Fb) je skup rješenja koji su predstavljeni u obliku okvira (f_i). Ovaj model sastoji se iz konačnog broja autentifikacionih rješenja (1), eksplicitno poznatih u početku procesa procjenjivanja.



Slika 18. Fishbone model

Prema tome, *Fishbone* model je vektorski prostor gdje okvir unutar definisanih korisničkih prioriteta predstavlja samo jedno rješenje u tom prostoru (2). To podrazumijeva da izabrana metoda autentifikacije treba da predstavlja najbolje rješenje kao kompromis između različitih konfliktnih interesa korisničkih kriterijuma. *Fishbone* model odgovarajući prema gore pomenutim činjenicama može biti zapisan kao:

$$Fb = \{f_1, f_2, \dots, f_n\} \qquad i = 1,2, \dots, n \qquad (\forall\, n \in N) \tag{1}$$

$$gdje\ je \qquad f_i = \{a_1 S + a_2 U + a_3 A + a_4 P_1 + a_5 C_1 + a_6 P_2 + a_7 C_2\} \tag{2}$$

Dakle, okvir predstavlja podskup Fishbone modela (3):

$$f \subseteq Fb \tag{3}$$

Jednačina (2) opisuje da svaki okvir je definisan sa konkretnim vrijednostima težinskih koeficijenata. Dakle, SUAPCPC faktori predstavljaju vektor definisan sa težinskim koeficijentima (a_i). Korisnici u mobilnim autentifikacionim pristupima nemaju

kriterijume istog stepena značajnosti i potrebno je da se definišu faktori značajnosti korisničkih kriterijuma koristeći odgovarajuće težinske koeficijente (težine) ili pondere za kriterijume. Vrijednosti težinskih koeficijenata dodjeljuju se od strane korisnika, i definisani su na jediničnom intervalu [0,1] pri čemu je njihova ukupna suma 1 – normalizovane težine.

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = 1 \quad \text{or} \quad \sum_{i=1}^{7} a_i = 1 \qquad a_i \in [0,1] \qquad (4)$$

Da bi odredili univerzalni autentifikacioni okvir - UAF u *Fishbone* modelu, potrebno je da se definišu njegovi težinski koeficijenti. Kod ovog okvira, svi težinski koeficijenti imaju jednake vrijednosti koji mogu biti zapisani u obliku:

$$a_{UAF} = \frac{\sum_{i=1}^{7} a_i}{7} \qquad i = 1,2,\dots,7 \qquad (a_i = a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7) \qquad (5)$$

Prema tome, UAF može biti predstavljen kao:

$$f_{UAF} = \{S + U + A + P_1 + C_1 + P_2 + C_2\} \qquad (6)$$

Za vrednovanje višestrukih mobilnih rješenja kao što su 2FA i 3FA, potrebno je da se odredi artimetička sredina pojedinačnih metoda autentifikacija koje grade višestruko rješenje kako bi se dobila jedinstvena krisp vrijednost. Prema tome, odgovarajuća matematička formula za krisp ocjenu 2FA/3FA je data u ovom radu.

$$G_{ij}(2FA) = \frac{G_i + G_j}{2} \qquad i,j = 1,2,\dots,n \qquad (\forall\, n \in N) \qquad (7)$$

$$G_{ijk}(3FA) = \frac{G_i + G_{j+G_k}}{3} \qquad i,j,k = 1,2,\dots,n \qquad (\forall\, n \in N) \qquad (8)$$

Na osnovu tih formula moguće je dati opštu matematičku formula za izračunavanje krisp vrijednosti za nFA-e:

$$G_n(nFA) = \frac{\sum_{i=1}^{n} G_i}{n} \qquad i = 1,2,\dots,n \qquad (\forall\, n \in N) \qquad (9)$$

U ovom dijelu rada, pored datih crisp formula 2FA/3FA i nFA, date su i opšta matematička formula za kvantitativno izračunavanje rizika (10) i ukupnog rizika (11) u EMDI:

$$R = P \times I \tag{10}$$

Kao što je prikazano u (10), rizik (R) je proporcionalan proizvodu vjerovatnoće (P) nekog neželjenog događaja i uticaja tog događaja (I). Domen vrijednosti za uticaj događaja je opisni (npr. *Low, Medium, High, Critical*) [209]. U slučaju EMDI, rizik je i moguće dekomponovati tj. parcijalno posmatrati prema pojedinačnim procesima, i na osnovu matematičke formule (11) za procjenu ukupnog rizika (TR) moguće je odrediti ukupni rizik u EMDI.

$$TR = \sum_{i=1}^{n} R_i \qquad i = 1,2,\dots,n \qquad (\forall\, n \in N) \tag{11}$$

Potrebno je naglasiti da u ovom radu eksterna aplikacija MatLAB koja je korišćena primjenjuje težinske koeficijente koji su zastupljeni u UAF (imaju svi istu vrijednost). Međutim, određivanje težinskih koeficijenata za korisničke kriterijume je uslovljeno korisničkom potrebom. Izbor kriterijuma odnosno njihovog težinskog koeficijenta ima presudan uticaj na izbor mobilne metode autentifikacije tj., na vrijednost njene ocjene. U pogledu određivanja težinskih koeficijenata u *UAF*, ovaj veoma bitan korisnički uslov je ispunjen kroz bazu pravila. U bazi pravila, korisnički kriterijumi su vrednovani sa lingvističkim izrazima koji određuju krajnju ocjenu (A-K) nekog pravila. Lingvistički izraz je način za uvođenje relacija uređenja. Ocjene za pravila se formiraju tako da ocjena predstavlja ukupnu vrijednost svih lingvističkih izraza dodijeljenih za korisničke faktore u posmatranom pravilu. Na primjer, najniža ocjena K – predstavlja najmanju ukupnu vrijednost svih lingvističkih izraza dodjeljenih za korisničke faktore u posmatranom pravilu. Prilikom formiranja pravila korisnički zahtjevi, u pogledu dodijeljenih težinskih koeficijenata, obuhvaćeni su kroz lingvističke ocjene korisničkih kriterijuma koji su takođe poredani prema stepenu korisničkog značaja od najmanjeg do najvećeg. Na primjer, ako za korisnika zaštita kao korisnički prioritet ima stepen najvećeg značaja, zatim slijede ostali korisnički faktori čiji daljni redosljed nema značaj za korisnika, tada u formiranom pravilu za ocjenu K zaštitni kriterijum ima najmanju ili neku drugu manju deskriptivnu vrijednost u pogledu korisnika označenu sa odgovarajućim lingvističkim izrazom.

Posebno je važno, da pri formiranju pravila se vodi računa da ocjena datog pravila slijedi vrijednost lingvističkog izraza za izabrani korisnički prioritet. Takođe, pri tom je neophodno uzeti u obzir, da vrijednosti lingvističkih izraza za korisničke kriterijume nemaju isto značenje za korisnika. Na primjer, zaštita i cijena. Sa korisničkog aspekta, faktor zaštite ima najveću korisničku vrijednost koja je označena sa lingvističkim izrazom *VVH*, dok cijena kao korisnički faktor ima za korisnika najveću vrijednost koja je označena sa lingvističkim izrazom *VVL*. Dakle, pravila se formiraju tako što se vrijednosti lingvističkih izraza za korisničke kriterijume dodijeljuju prema stepenu njihovog korisničkog značaja. Prema *Fishbone* modelu lingvistički izrazi koji se dodjeljuju za korisničke prioritete treba da ispunjavaju najbolja pojedinačna rješenja za korisnike:

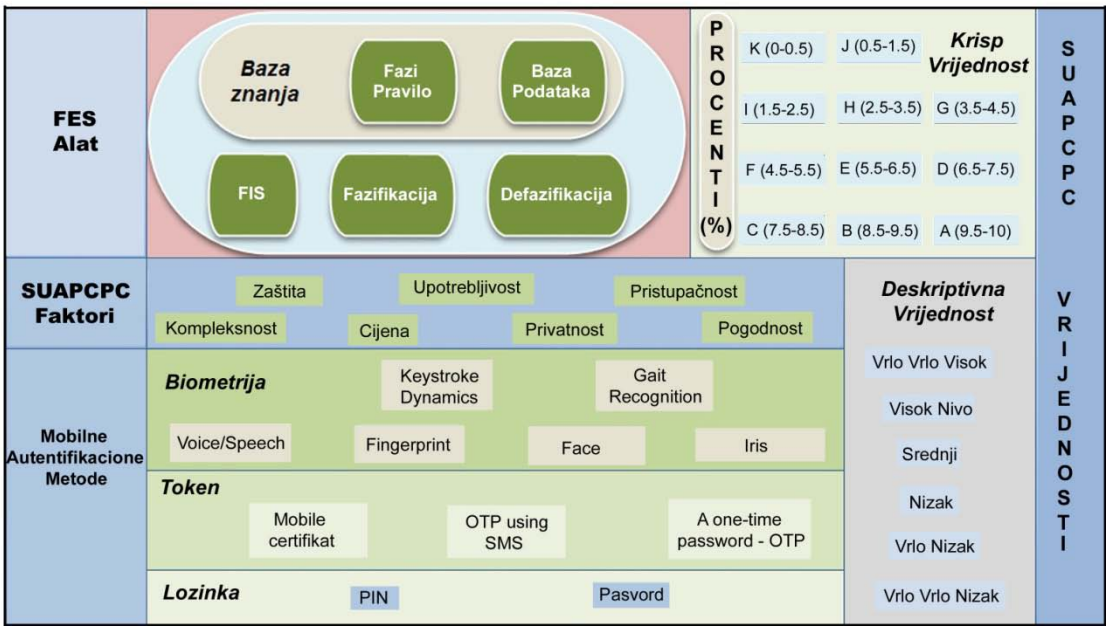
- *Zaštita – VVH*
- *Upotrebljivost – VVH*
- *Pristupačnost – VVH*
- *Cijena – VVL*
- *Kompleksnost – VVL*
- *Privatnost – VVH*
- *Pogodnost – VVH.*

Ovaj model predstavlja specifičan alat u procijenjivanju savremenih korisničkih metoda autentifikacija i dizajniranju nFA rješenja. Specifičnost *Fishbone* modela čine njegovi bazični moduli arhitekture i blok dijagram. *Fishbone* model izgrađuje se na postojećim teorijama SUAPCPC faktora koje su skrojene specifično za mobilne uređaje. Dakle, ovaj model može biti korišćen da rezimira sve mobilne metode autentifikacija u pogledu SUAPCPC faktora. Određivanje SUAPCPC faktora je zasnovano na izdiferenciranim ključnim korisničkim prioritetima. Osnovni bazični moduli ovog modela detaljnije su opisani u sljedećoj sekciji rada.

6.4. Prijedlog arhitekture Fishbone modela u sistemima za IAM

Prijedlog arhitekture *Fishbone* modela u sistemima za IAM je dat pomoću bazičnih modula. Bazični moduli arhitekture *Fishbone* modela su dati na slici 19. Ova arhitektura obuhvata funkcionalne module korespondirajući prema mobilnim autentifikacionim

pristupima. Suštinsko obilježje *Fishbone* modela predstavlja njegova arhitektura. Arhitektura predstavlja kompleksne izraze odnosa između njegovih glavnih modula.



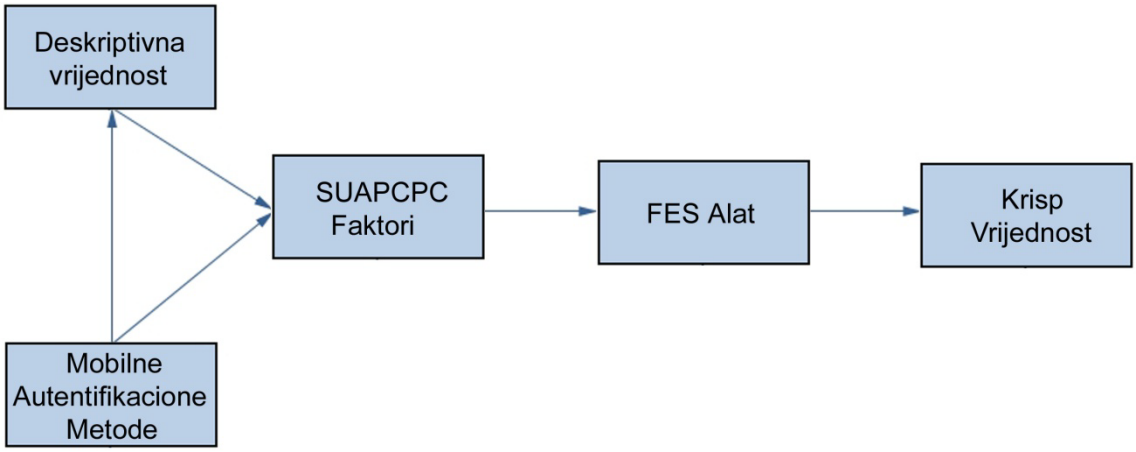
Slika 19. Bazični moduli arhitekture Fishbone modela

Za izgradnju bazičnih modula arhitekture *Fishbone* modela presudan uticaj imaju sljedeći moduli:

- mobilne autentifikacije,
- SUAPCPC faktori,
- SUAPCPC vrijednosti (Deskriptivne i Krisp vrijednosti), i
- Alat Fazi Ekspertnog sistema (FES alat).

Svaki modul sadrži bazičnu grupu komponenti odvojenih po njihovim funkcijama u *Fishbone* modelu. Uticaj bazičnih modula arhitekture *Fishbone* modela nije partikularnog karaktera već simultan. To podrazumijeva da svi moduli treba da budu isključivo razmatrani cjelovito. Drugim riječima, zajedničko za sve komponente je da ne mogu biti posmatrani pojedinačno već isključivo u cjelini. Modul mobilne autentifikacije je modul koji obuhvata savremene mobilne metode autentifikacije koje mogu biti kombinovane pri stvaranju nFA rješenja. Modul SUAPCPC faktora je modul prema kojem se vrijednuju određene mobilne metode autentifikacije. Modul SUAPCPC vrijednosti je modul prema kojem se izražava vrijednost mobilnog metoda autentifikacije. Vrijednost ovog modula može biti izražena deskrptivno ili numerički. Numeričko izražavanje vrijednosti može biti izraženo u procentima (%). Ipak, fundamentalni modul arhitekture *Fishbone* modela koji ga izdvaja od svih drugih

modula je alat FES-a. Specifičnost ovog modula je fazi zaključni sistem (*engl. fuzzy inference system – FIS*) koji koristi fazifikaciju u procesu generisanja krisp vrijednosti mobilnog metoda autentifikacije. FIS je upravo jedna komponenta cijelog FES alata koja ovaj alat izdvaja kao ključni modul u *Fishbone* modelu. Radi potpunijeg razumijevanja bazičnih modula arhitekture *Fishbone* modela, blok dijagram *Fishbone* modela za zaštitu informacija u sistemima za IAM je dat na slici 20.



Slika 20. Blok dijagram Fishbone modela za zaštitu informacija u sistemima za IAM

Blok dijagram *Fishbone* modela predstavlja kompleksne odnose između njegovih bazičnih modula. Modul mobilnog metoda autentifikacije je modul koji je povezan prema modulu SUAPCPC faktora kao i modul deskriptivne vrijednosti. Takođe, modul deskriptivne vrijednosti je povezan prema SUAPCPC faktorima. Modul SUAPCPC faktor predstavlja ulaz u FES alat, dok izlaz iz FES alata predstavlja modul krisp vrijednost.

6.5. *Kombinovanje i integracija tehnologija autentifikacija u dizajniranju Fishbone modela u savremenim korisničkim mobilnim autentifikacijama*

Fishbone model je model koji obuhvata širi skup pojedinačnih mobilnih metoda autentifikacija unutar kojeg je moguće izvršiti kombinovanje i integraciju bilo koje metode u cilju stvaranja nFA rješenja. Međutim, da bi se uopšte izvršila mogućnost kvalitetnog odabira odgovarajuće mobilne metode autentifikacije u pogledu prema nekom od posmatranih korisničkih prioriteta potrebno je formirati komparativnu tabelu

sa izdiferenciranim pojedinačnim autentifikacionim metodama i korisničkim prioritetima.

6.5.1. Prijedlog kriterijuma za komparaciju i komparacija

Kao što je istaknuto u prethodnoj sekciji, pregled savremenih korisničkih mobilnih metoda autentifikacija su elaborirana sa izdiferenciranim prednostima i nedostacima. Na osnovu prikupljenih kvantitativnih i kvalitativnih podataka, komparacija je napravljena u pogledu prema ključnim kriterijima kao što su SUAPCPC. Važan izvor za formiranje tabele 2 je korišćena dostupna literature kao što je [12, 18, 97, 102, 163-165, 168, 169, 170-178, 210, 211]. Komparativni rezultati su deskriptivno opisani u tabeli 1. Deskriptivne vrijednosti su izražene u sedam nivoa:

- vrlo vrlo nizak - *VVL*,
- vrlo nizak - *VL*,
- nizak - *L*
- srednji - *M*,
- visok - *H*,
- vrlo visok - *VH*, i
- vrlo vrlo visok - *VVH*.

Ulazi u tabelu 2 su zasnovani na percepciji autora i na izvorima relevantne gore navedene literature. Pojmovi *vrlo vrlo nizak, vrlo nizak, nizak, srednji, visok, vrlo visok* i *vrlo vrlo visok* su za svakog posebno označene sa *VVL, VL, L, M, H, VH i VVH (engl. Very Very Low, Very Low, Low, Medium, High, Very High and Very Very High)*. Razlika između različitih korisničkih kriterijuma i njihovih mobilnih metoda autentifikacija je važna u razmatranju komparacije savremenih korisničkih mobilnih metoda autentifikacija. Komparativni rezultati sve to deskriptivno obuhvataju. Deskriptivni rezultati imaju poseban značaj u numeričkim pristupima. Oni predstavljaju kvantifikacioni ulaz koji je krucijalni korak u krisp procjeni mobilnih autentifikacionih rješenja.

Prema tome, tabela 2 daje komparaciju različitih korisničkih mobilnih metoda autentifikacija zasnovanih na glavnim komparativnim faktorima kao što su SUAPCPC. Ovi faktori su opšti prioriteti u autentifikacionim pristupima koji nisu samo ograničeni na mobilne metode autentifikacija. Zbog važnosti SUAPCPC faktora koji imaju u

mobilnim autentifikacionim pristupima, a time i uticaja na komparaciju, oni su opisani u više detalja. U svakom od ovih sedam kriterijuma obuhvaćeni su svi ključni problemi koji su izvedeni sa korisničkog aspekta.

Tabela 2. Komparacija različitih mobilnih metoda autentifikacija urađena od strane autora i zasnovana na izvorima u relevantnoj literaturi [12, 18, 97, 102, 163-165, 168, 169, 170-178, 210, 211].

Karakteristike	S	U	A	P	C	P	C
PIN	VVL	VVH	VVH	VVL	VVL	VVH	VVL
Password	VVL	VVH	VVH	VVL	VVL	VVH	VVL
OTP generated applications	VL	VH	VH	L	L	VH	VL
OTP using SMS	L	H	H	M	M	H	L
Mobile certificate	H	L	L	H	H	M	H
Fingerprint	VH	VL	L	VH	H	VVL	VVH
Face	VVH	VVL	VVL	VVH	VVH	VVL	VVH
Iris	VVH	VVL	VVL	VVH	VVH	VVL	VVH
Voice/Speech	VH	M	M	VL	VL	VVL	VVH
Keystroke Dynamics	VH	L	L	M	L	VL	VH
Gait Recognition	VH	M	M	L	VL	VL	VH

Kao što je prethodno pomenuto, ne postoji rad koji bi dao jedinstveno "*najpogodnije*" šablonsko rješenje u mobilnim autentifikacionim pristupima. Na osnovu komparativne analize date u tabeli 2, odgovor daje objašnjenje zašto i nije bilo moguće da se postigne takav šablon u mobilnim autentifikacionim pristupima. Prvo, ne postoji jedinstvena

mobilna metoda autentifikacije koja bi istovremeno obezbijedila maksimalni nivo zaštite i bila opšteprihvatljiva za sve korisnike. Ukoliko jedna mobilna metoda autentifikacije ima nedostatke u određenom pravcu, u drugoj koja se pojavi kao korektura, obavezno se javljaju problemi druge prirode. Prije svega, svojstva metoda autentifikacija imaju različite korisničke vrijednosti (deskriptivne) koje su posmatrane prema izdiferenciranim karakteristikama. Na primjer, ako se porede PIN i Iris prema izdiferenciranim ključnim korisničkim faktorima datih u tabeli 2, deskriptivni rezultati ukazuju da korisnik upotrebom PIN-a obezbjeđuju najnižu zaštitu, cijenu, kompleksnost i pogodnost sa najvišim nivoom upotrebe, pristupačnosti i privatnosti dok upotrebom Iris-a obezbjeđuje najviši nivo zaštite, cijene, kompleksnosti i pogodnosti sa najnižim nivoom upotrebe, prstupačnosti i privatnosti.

Zaključak upućuje, da u takvim mobilnim autentifikacionim pristupima korišćenjem pojedinačnih metoda se ne postiže maksimum korisničkih prioriteta. Na ovaj način se potpuno jasno uočava sva složenost i kompleksnost pojma mobilnih metoda autentifikacija, kao i mogućnost različitih pristupa u procesima autentifikacija. Nesumnjivo, rješenje sa kojim bi se ublažili nedostaci pojedinačnih metoda zahtijeva primjenu nFA rješenja tj. kombinovanje više različitih mobilnih metoda autentifikacija. Stoga, u praksi pri stvaranju bilo kog jakog autentifikacionog rješenja, ove metode su korišćene u kombinaciji sa drugim metodama autentifikacije. Takođe, pri dizajniranju nFA rješenja, postoje i drugi gore pomenuti problemi kao što su sposobnost korisnika – različite fizičke i mentalne sposobnosti, potrebe, godine, znanja, i sl. Pristup prema svim tim problemima je holistički razmatran kroz *Fishbone* model.

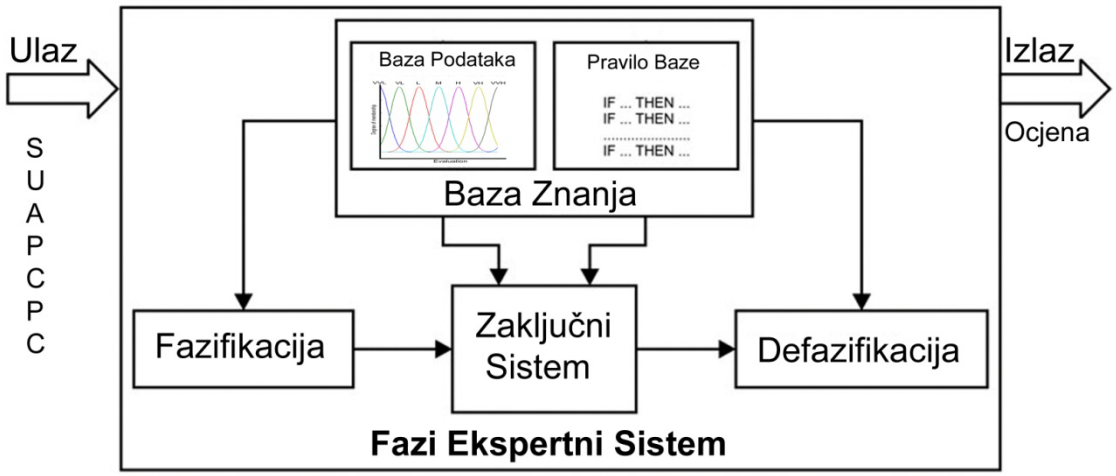
6.6. Dizajn novog Fishbone modela

Na osnovu stečenih kompratívnih rezultata prikazanih u tabeli 2 moguće je izvršiti dizajniranje novog modela zaštite – *Fishbone* modela zaštite u sistemima IAM. Za dizajn *Fishbone* modela u savremenim korisničkim mobilnim metodama autentifikacije razvijen je FES alata zasnovan na teoriji fazi skupova i fazi logike. Značaj i važnost metodologije razvoja FES alata za procijenu mobilnih rješenja detaljnije je opisana u narednoj sekciji rada.

6.6.1. Methodologija razvoja fazi ekspertnog sistema za procijenu mobilnih rješenja

Metodološki pristup razvoja FES-a za procjenu mobilnih rješenja je uveden. Suština predložene metodologije je što određene nepreciznosti i neodređenosti predstavljene kao lingvistički izrazi u mobilnim metodama autentifikacije je moguće zamijeniti sa fazi brojem. Cilj ove metodologije je da pomoću odgovarajućeg zaključnog pravila upravlja i istražuje znanjem u specifičnom mobilnom okruženju kroz rezonovanje vrijednosti metoda autentifikacija [18]. Ova metodologija je orijentisana prema numeričkom procesuiranju. Metodologija razvoja FES-a je data na slici 21. FES sistem može biti podijeljen u nekoliko funkcionalnih blokova kao što su:

- osnovno pravilo,
- baza podataka,
- zaključni sistem,
- fazifikacija, i
- defazifikacija.



Slika 21. Opšta struktura fazi ekspertnog sistema za procijenu mobilnih rješenja.

Pravilo baze sadrži fazi pravila dok baza podataka definiše funkciju pripadnosti fazi skupa korišćenog u fazi pravilima. Funkcija pripadnosti odnosi se prema stepenu istinitosti tj. u kom obimu vrijednosti pojedinog parametra pripadaju prema definisanom skupu. Potrebno je naglasiti da funkcionalni blokovi osnovno pravilo i baza podataka predstavljaju bazu znanja. Zaključni sistem je suštinski dio svakog FES alata koji leži u jezgru strukture. Ovaj sistem izvršava zaključne operacije kroz definisana fazi pravila u

bazi znanja. Drugima riječima, fazi zaključni sistem omogućava preslikavanje iz datog ulaza u izlazne promjenjive upotrebljavajući promjenjive fazi logike takođe označene kao lingvističke varijable. Ove varijable imaju fazi vrijednost u domenu [0,1] koje su dodjeljene za svaku kategoriju unijetog parametra. Cilj fazi logike je da definiše situaciju neodređenosti putem davanja odgovarajuće funkcije pripadnosti za ulazne i izlazne promjenjive, kao i procijenjivanje parametara sistema. Funkcija pripadnosti pridružuje težinske ulaze, definiše funkcionalna preklapanja između njih, i određuje najbolji izlazni odgovor. Određivanje broja izlaznih varijabli je zasnovano na ekspertskom znanju. U ovom metodološkom pristupu, razvoj FES alata koristi metodologiju *Mamdani-type* [212], zbog njegove relativno jednostavne strukture i skupa pravila koja se mogu jednoznačno interpretirati. Ovaj tip razvija pravila u formi *if – then* metoda, dajući pri tom, ako prethodi tada slijedi. Opšti oblik sistema fazi osnovnog pravila sa višestrukim ulazima i izlazima može biti opisan kao:

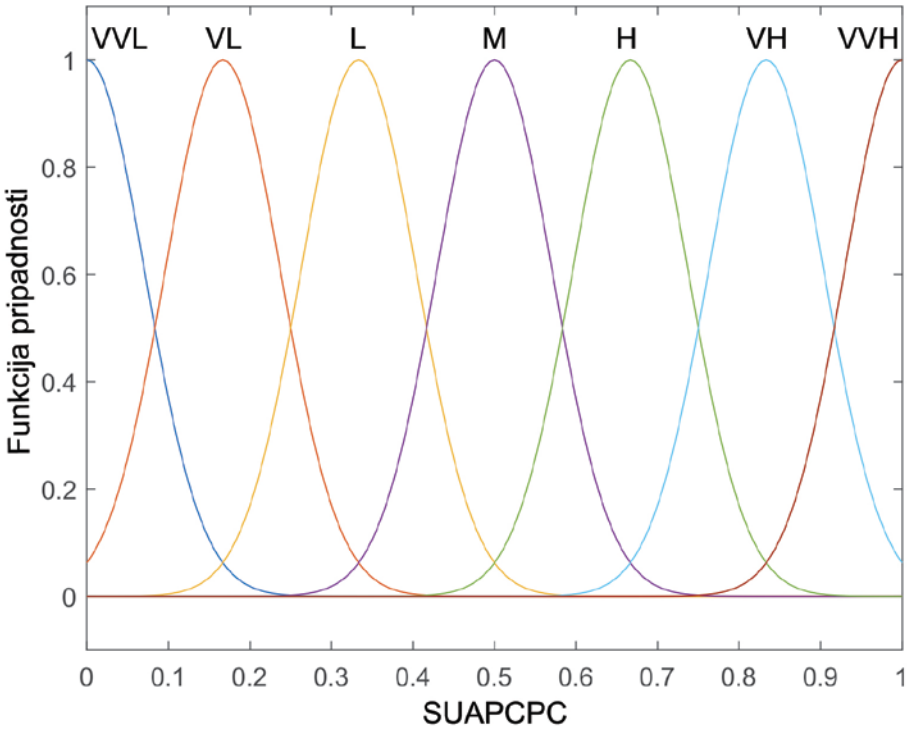
Rule 1: If A_1 is x_1 and A_2 is y_1 and . . . and A_n is z_1, then B is w_1:
Rule 2: If A_1 is x_2 and A_2 is y_2 and . . . and A_n is z_2, then B is w_2:
.....
Rule n: If A_1 is x_n and A_2 is y_n and . . . and A_n is z_n, then B is w_n,

gdje A_i ($i = 1,2, \dots, n$), ($\forall\, n \in N$) su ulazi varijabli koji opisuje korisničke prioritete; B je izlazna varijabla; x_i, y_i, . . . , w_i su lingvistički pojmovi korišćeni za izlazne varijable. Upotrebljavajući ova pravila, ocjene vrijednosti za savremene korisničke metode mobilnih autentifikacija mogu biti izračunate u pojmu procenata (%). Fazifikacija je proces pretvaranja numeričkih ulaznih varijabli u fazi varijable sa lingvističkim oznakama. Defazifikacija je proces pretvaranja fazi rezultata baze znanja u kombinaciji sa rezultatima zaključnog sistema u krisp izlaznu vrijednost. Sistem koristi centroidni metod za agregaciju FES alata [212].

6.6.2. Dizajn Fazi Ekspernog Sistema

Kao što je navedeno u prethodnoj sekciji rada, pri dizajniranju FES alata prvi proces je određivanje fazi pravila. U literaturi ovaj proces je opisan kao jedan od najproblematičnih i najtežih procesa. U radu [213] Mount *et al*., su naveli da "*ne postoji sveobuhvatna jedinstvena teorija kako steći znanje i vjerovatno neće ni biti*". U ovom radu, sticanje znanja je izvedeno od ljudskih eksperata kao i iz podataka pronađenih u

dostupnoj literaturi. Kako je za dizajn ovog FES alata određeno da zaštita bude korisnički prioritet u kome dalji raspored korisničkih prioriteta nije bitan, time je i optimalno baza pravila zasnovana na tom principu. Znanje kao referentna polazna osnova za dizajniranje ovog FES alata predstavlja komparativnu tabelu 2. Deskriptivne vrijednosti mobilnih metoda autentifikacija predstavljaju kvantifikacione ulaze koji su krucijalni korak u procjeni nekog mobilnog rješenja. Prvi korak u dizajnu sistema fazi logike je definisanje fazi promjenjive i određivanje odgovarajuće funkcije pripadnost, tj., određivanja ulaza i izlaza promjenljivih. Funkcija pripadnosti pokazuje u kom obimu određeni korisnički prioritet se podudara sa stepenom funkcije. Dizajn ovog FES alata se sastoji od sedam ulaza i jednog izlaza. Ulazna vrijednost se sastoji od korisničkih prioriteta koji su predstavljeni kao SUAPCPC faktori dok izlazne vrijednosti predstavljaju vrijednost mobilnog rješenja. Potrebno je posebno istaći, da je funkcija pripadnosti ista za sve korisničke prioritete i zbog toga je funkcija pripadnosti predstavljena sa SUAPCPC faktorom. Funkcija pripadnosti sa SUAPCPC faktorom i njegovim lingvističkim varijablama je data na slici 22. Za ulaznu varijablu, oblik Gausove krive funkcije pripadnosti je iskorišćen da opiše fazi skupove. Lingvističke varijable su klasifikovane u sedam kategorija tj, sedam fazi skupova kao što su *very very low*, *very low*, *low*, *medium*, *high*, *very high* i *very very high*. Lingvistički, to podrazumijeva da su ove varijable prezentovane sa sedam Gausovih funkcija pripadnosti.



Slika 22. Funkcija pripadnosti za SUAPCPC faktore

Važnost Gausove funkcije je da aproksimativna deskriptivna vrijednost metode autentifikacije može biti označena sa fazi brojevima koji predstavljaju kvantitativne ulaze definisanih varijabli u domenu 0 do 1. Prosto rečeno, Gausova funkcija pripadnosti dopušta da se odredi tablično pravilo za fazi ulaz kao fazi interval za svaku lingvističku varijablu (tabela 3).

Tabela 3. Tablično pravilo za fazi ulaz

INPUT	Fuzzy interval
Very Very Low	0-0.0835
Very Low	0.0835-0.25
Low	0.25-0.416
Medium	0.416-0.583
High	0.583-0.75
Very High	0.75-0.916
Very Very High	0.916-1

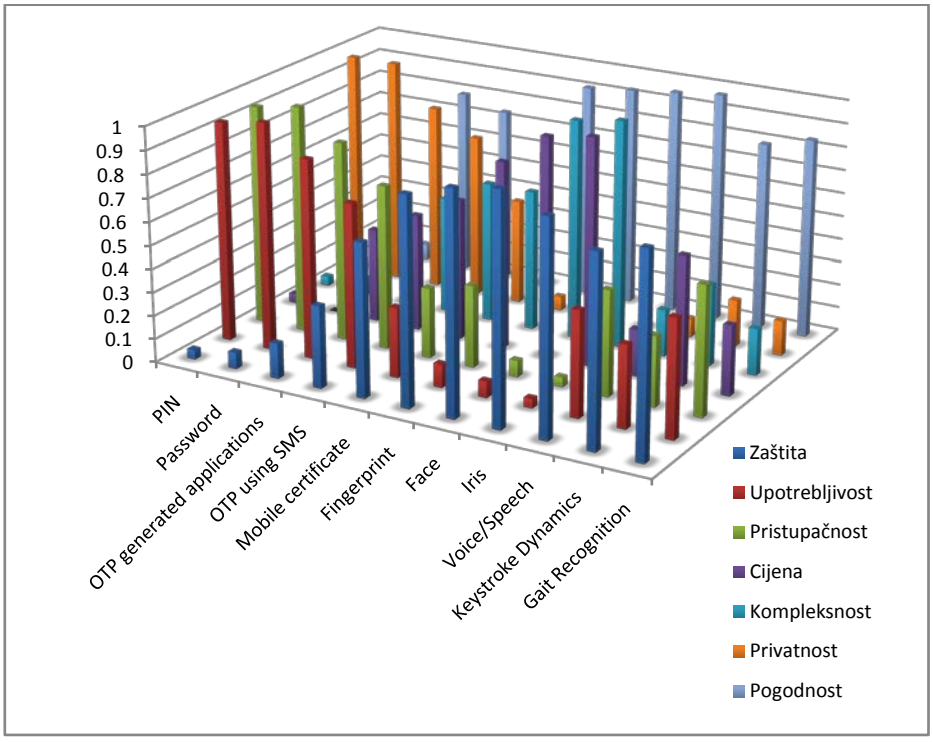
Na osnovu slike 23, deskriptivne vrijednosti savremenih korisničkih metoda autentifikacija namjenjenih za mobilne uređaje su zamjenjene sa fazi brojevima. Vrijednost fazi brojeva su dodjeljene od strane autora i prezentovane u tabeli 4. Potrebno je naglasiti, da je dodijeljivanje vrijednosti za pojedinačne metode autentifikacija izvršeno na osnovu komparativne tabele 2, čija je takođe osnova bila zasnovana na osnovu ranijih komparativnih pristupa.

Tabela 4. Dodjeljene vrijednosti za savremene korisničke mobilne metode autentifikacije.

Karakteristike	*S*	*U*	*A*	*P*	*C*	*P*	*C*
PIN	0.04	0.94	0.94	0.04	0.04	0.97	0.04
Password	0.07	0.97	0.97	0.04	0.07	0.97	0.07
OTP generated applications	0.15	0.85	0.85	0.4	0.4	0.8	0.8

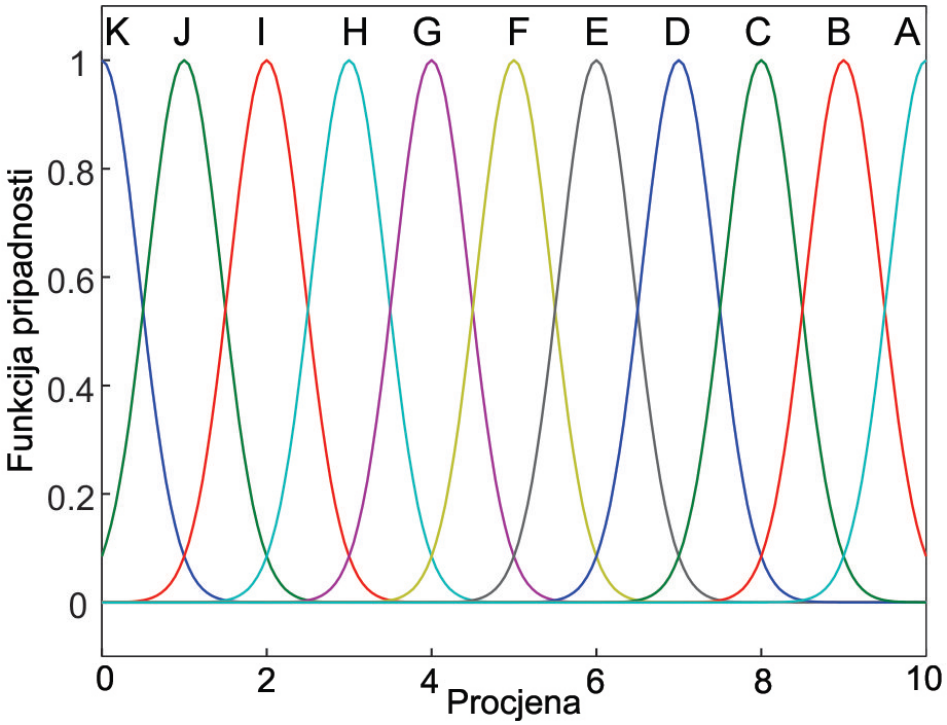
OTP using SMS	0.35	0.7	0.7	0.5	0.5	0.7	0.75
Mobile certificate	0.65	0.3	0.3	0.6	0.6	0.45	0.6
Fingerprint	0.88	0.1	0.35	0.8	0.6	0.06	0.92
Face	0.94	0.07	0.07	0.94	0.94	0.05	0.94
Iris	0.97	0.04	0.04	0.97	0.97	0.04	0.96
Voice/Speech	0.9	0.45	0.45	0.2	0.2	0.08	0.98
Keystroke Dynamics	0.8	0.35	0.3	0.55	0.35	0.2	0.8
Gait Recognition	0.85	0.5	0.55	0.3	0.2	0.15	0.85

Da bi potpunije razumijeli tabelu 4, dat je grafikon 1 (slika 23) koji pokazuje pregled komparacija savremenih mobilnih metoda autentifikacija sa dodjeljenim konkretnim vrijednostima.



Slika 23. Statistički pregled komparacija različitih metoda autentifikacija sa dodjeljenim vrijednostima zasnovanim na korisničkim prioritetima.

U FES fazi ekspertnom sistemu, predloženi fazi zaključni sistem je zasnovan na defazifikacionom modulu, gdje je izlaz predstavljen u domenu [0,10]. Izlaz sistema, koji predstavlja procjenu mobilnog rješenja, ima jedanaest funkcija pripadnosti sa jedanaest ocjena. Takođe, oblik Gausove krive funkcije pripadnosti je iskorišćen da opiše Fazi skup za izlaznu varijablu. Ocjene su klasifikovane od A-K na osnovu ekspertskog znanja, gdje je ocjena K predstavljena kao najniža vrijednost dok je ocjena A predstavljena kao najviša vrijednost. Funkcija pripadnosti i ocjena za procjenu mobilnih rješenja kao izlaznog parametra su dati na slici 24. U sljedećem koraku, fazi pravila su formulisana da odrede odnose između ulaza i izlaza u fazi sistemu. Fazi pravila zasnovanog modela su razvijena iz ekspertskog znanja. Broj fazi pravila je povezan prema broju fazi skupova za svaku ulaznu varijablu. Stoga uzimajući u razmatranje sedam ulaza i sedam lingvističkih varijabli (7^7), maksimalan broj pravila za ovaj sistem je 823543. Kada je broj fazi pravila prevelik postoje dvostruka ograničavajuća pravila za rad sistema. Prvo, sistem može zahtijevati više vremena da generiše izlaz zbog velikog broja numeričkih koraka. Drugo, funkcionisanje ovakvog sistema zahtijeva ograničavajući memorijski resurs (RAM memoriju). Ako je moguće da se odredi aproksimativni izlaz FES alata bez povećavanja pravila tada je sveukupna arhitektura sistema uprošćena, i smanjuje se broj numeričkih koraka kao i memorijski prostor.



Slika 24. Funkcija pripadnosti za procjenu mobilnog rješenja.

U tom pogledu, u ovom radu je samo 110 od 823543 mogućih pravila selektovano za konstruisanje tabličnog baznog pravila (tabela 5). Izbor od 110 pravila je napravljen na osnovu autorovog ekspertskog znanja. Suština izbora redukcionog primarnog pravila je da sadrži sve deskriptivne ocjene (12 ocjena) koji su dati u tabeli 2. Takođe, ostalih 98 pravila sadržanih u redukovanom primarnom pravilu su napravljena na osnovu autorovog ekspertskog znanja pri čemu su obuhvaćene maksimalne i minimalne ocjene koje su sadržane u primarnom osnovnom pravilu. Stoga, redukciono primarno pravilo implicitno sadrži osnovno pravilo sadržavajući svih 823543 mogućih pravila. Ovo jasno ukazuje da redukcija ne utiče na tačnost rezultata. Pošto su sva fazna pravila definisana moguće je ispitati perfomanse sistema.

Tabela 5. Određena fazna pravila

S	U	A	P	C	P	C	VALUE
VVH	VVH	VVH	VVL	VVL	VVH	VVH	A
VVH	VVH	VVH	VVL	VL	VVH	VVH	A
VVH	VVH	VVH	VVL	L	VVH	VVH	A
VVH	VVH	VVH	VVL	M	VVH	VVH	A
VVH	VVH	VVH	VVL	H	VVH	VVH	A
VVH	VVH	VVH	VVL	VH	VVH	VVH	A
VVH	VVH	VVH	VVL	VVH	VVH	VVH	A
VVH	VVH	VH	L	M	VH	VVH	A
VVH	VH	VH	L	H	VH	VH	A
VVH	H	VH	L	VH	VH	VH	A
VVH	VL	VH	L	VL	VH	VH	B
VVH	VL	VH	L	L	VH	VH	B
VVH	VL	VH	M	VL	VH	VVH	B
VVH	VVL	VVL	VVH	VVH	VVL	VVH	B
VVH	VVL	VH	M	M	VH	VVH	B
VVH	VVL	VH	M	H	VH	VVH	B
VVH	VVL	VH	M	VH	VH	VVH	B
VVH	VVL	VVL	VVH	VVH	VVL	VH	B
VVH	VVL	H	VL	L	VH	VH	B
VVH	VL	VL	VH	VH	VVL	VVH	B
VH	VL	L	VH	H	VVL	VVH	C

VH	VL	VL	VH	VL	VL	VVH	C
VH	M	H	H	VL	VH	VH	C
VH	M	M	L	VL	VL	VH	C
VH	M	M	L	L	L	VH	C
VH	L	H	VVH	L	VH	H	C
VH	L	L	M	L	VL	VH	C
VH	M	M	VL	VL	VVL	VVH	C
VH	M	M	L	M	VL	VVH	C
VH	L	L	M	L	VL	VH	C
VH	M	M	VL	L	VVL	VVH	D
VH	VVL	VL	VH	VH	VVL	VVH	D
VH	VVL	L	M	L	VL	VVH	D
VH	VVL	VL	M	M	VL	VVH	D
VH	VVL	VL	M	H	VL	VVH	D
VH	VVL	L	H	VH	M	VVH	D
VH	VVL	M	H	VVH	L	VH	D
VH	VVL	M	VH	H	L	VH	D
VH	VVL	M	H	L	L	VH	D
VH	VVL	L	M	L	L	VH	D
H	M	L	H	L	L	H	E
H	M	M	VH	M	L	H	E
H	M	VL	H	H	L	H	E
H	M	VL	M	VH	L	H	E
H	M	L	H	VVH	VL	H	E
H	M	M	M	L	VL	H	E
H	L	L	H	H	M	H	E
H	L	H	M	L	VL	H	E
H	L	VH	M	VL	VL	H	E
H	L	VH	VL	VH	VL	H	E
M	VH	M	VH	VH	VL	H	F
M	VH	M	L	L	VL	H	F
M	VH	M	VL	M	VL	H	F
M	VH	M	L	H	VL	H	F
M	H	M	H	VH	M	M	F
M	M	M	L	VL	M	M	F

M	M	M	L	L	M	M	F
M	M	M	L	M	M	M	F
M	L	M	M	H	M	M	F
M	L	M	H	VH	M	M	F
L	VVH	M	M	L	M	M	G
L	VVH	M	M	M	M	L	G
L	VH	M	M	H	M	L	G
L	H	M	M	VH	M	L	G
L	H	H	M	VVH	H	L	G
L	H	H	M	M	H	L	G
L	H	H	M	L	H	VL	G
L	H	H	L	VL	H	VVL	G
L	H	M	VL	L	H	VVH	G
L	H	M	VL	VL	H	VH	G
VL	VVH	M	L	VH	H	VH	H
VL	VVH	M	L	L	H	VVH	H
VL	VVH	M	M	M	VVH	VVH	H
VL	VVH	M	L	H	VVH	VVH	H
VL	VVH	M	L	VH	VH	VVH	H
VL	VVH	M	VL	VVH	VH	VVH	H
VL	VVH	M	VVL	VVL	H	VVL	H
VL	VVH	M	VVH	VVH	H	VVL	H
VL	VVH	M	VH	VH	M	VVL	H
VL	VVH	M	H	H	L	VVL	H
VL	VH	VH	L	H	VH	VL	I
VL	VH	VH	L	L	VH	VL	I
VL	VH	VH	L	L	H	VL	I
VL	VH	VH	L	M	H	VVL	I
VL	VH	VH	L	H	VH	VVH	I
VL	H	VH	M	VH	VH	VVH	I
VL	H	VH	H	VVH	VH	VVH	I
VL	L	VH	H	VVL	VL	VH	I
VL	L	VH	VH	VVL	VH	VVH	I
VL	L	VH	VVH	VL	VVH	VVH	I
VVL	VVH	VH	VVH	L	VVH	VVL	J

VVL	VVH	VH	VVH	M	VVH	VVL	J
VVL	VVH	VH	VL	H	VVH	VVL	J
VVL	VVH	VH	VL	VH	VVH	VVL	J
VVL	VVH	VVH	VL	VVH	VVH	VVL	J
VVL	VVH	VVH	VVL	VVL	VVH	VVL	J
VVL	VVH	VVH	VVL	L	VVH	VVL	J
VVL	VVH	VVH	VVL	M	VVH	VVL	J
VVL	VVH	VVL	VVL	H	VVH	VVL	J
VVL	VVH	VVL	VVL	VVL	VVL	VVL	J
VVL	VVL	VL	VH	H	VVL	VVL	K
VVL	VVL	VL	VH	VH	VVL	VVL	K
VVL	VVL	VL	VH	VVH	VVL	VVL	K
VVL	VVL	VVL	VVH	VVL	VVL	VVL	K
VVL	VVL	VL	VVH	VL	VVL	VVL	K
VVL	VVL	VVL	VVH	L	VVL	VVL	K
VVL	VVL	VVL	VVH	M	VVL	VVL	K
VVL	VVL	VVL	VVH	H	VVL	VVL	K
VVL	VVL	VVL	VVH	VH	VVL	VVL	K
VVL	VVL	VVL	VVH	VVH	VVL	VVL	K

VII IMPLEMENTACIJA FISHBONE MODELA UPOTREBOM MatLAB

7.1. Rezultati implementacije Fishbone modela primjenom FES alata

Nakon što je postavljen fazi zaključni sistem, sistem je primjenjen za savremene korisničke mobilne metode autentifikacije. Potrebno je istaknuti da je dizajn i implemetacija *Fishbone* modela urađena u hardversko – softverskom okruženju u kojem je korišćen procesor - *Intel(R) Celeron (R) CPU B800 @ 1.5GH, Hard disk 300 GB, RAM memorija: 4.00 GB,* operativni sistem *Windows 7 Profesional 64-bit.* Rezultati implementacije su dati u tabeli 6. Ovi rezultati ukazaju da je predloženi FES alat efektivan u stvaranju numeričke vrijednosti mobilnih metoda autentifikacije.

Tabela 6. Ocjena vrijednosti za savremene korisničke mobilne metode autentifikacije zasnovane na dodjeljenim vrijednostima ekspertskog znanja.

Metod autentifikacije	***FES Ocjena***
PIN	**1.0149**
Password	**1.0161**
OTP generated applications	**2.0207**
OTP using SMS	**3.5013**
Mobile certificate	**5.9678**
Fingerprint	**7.9929**
Face	**8.2071**
Iris	**8.5305**

Voice/Speech	**7.7376**
Keystroke Dynamics	**7.6389**
Gait Recognition	**7.8048**

Rezultati su dobijeni na osnovu dodjeljenih kvantifikacionih vrijednosti mobilnih metoda autentifikacija. Iz dobijenih rezultata, očigledno je da tehnika fazi logike predstavlja dobar alat za postupanje sa nejasnoćama i nepreciznostima koje su prezentovane u mobilnom autentifikacionom području unutar razmatranih SUAPCPC faktora. Da bi se bolje razumijeli rezultati prezentovani u tabeli 6, formalna komparacija rezultata sa statističkim pristupom je data:

Iris 8.5305 < *Face* 8.2071 < *Fingerprint* 7.9929 < *Gait Recognition* 7.8048 < *Voice/Speech* 7.7376 < *Keystroke Dynamics* 7.6389 < *Mobile certificate* 5.9678 < *OTP using SMS* 3.5013 < *A one-time password-OTP* 2.0207 < *Password* 1.0161 < *PIN* 1.0149.

Na osnovu komparacije dobijenih rezultata može se jasno zaključiti da metoda autentifikacije zasnovana na ”*nešto što jesi*”, obezbijeđuje najvišu krisp ocjenu dok metoda autentifikacije zasnovana na ”*nešto što znaš*”, obezbijeđuje najnižu krisp ocjenu. Prema rezultatima iz tabele 6, metod autentifikacije zasnovan upotrebom Iris-a ima najvišu vrijednost 8.5305, dok metod autentifikacije zasnovan upotrebom PIN-a ima najnižu vrijednost ocjene 1.0149. Prednost dizajniranog FES alata je mogućnost zamjene korisničkog prioriteta i na osnovu toga formiranje nove krisp vrijednosti za autentifikaciona rješenja. U slučaju da korisnik ne želi implementaciju nekog od ponuđenih faktora tom faktoru se može dodjeliti nulta vrijednost.

Na osnovu primjene matematičke formule za 2FA rješenja koja je data u prethodnom poglavlju (jednačina 7), formirana je tabela 7 u kojoj je dato svih mogućih 55 rezultata FES ocjena.

Tabela 7. Rezultati ocjene za 2FA rješenja

2FA rješenja	*FES Ocjena*
PIN + Password	**1.0155**
PIN + OTP generated applications	**1.5178**
PIN + OTP using SMS	**2.2581**
PIN + Mobile certificate	**3.4914**
PIN + Fingerprint	**4.5039**
PIN + Face	**4.611**
PIN + Iris	**4.7727**
PIN + Voice/Speech	**4.3762**
PIN + Keystroke Dynamics	**4.3269**
PIN + Gait Recognition	**4.4098**
Password + OTP generated applications	**1.5184**
Password + OTP using SMS	**2.2587**
Password + Mobile certificate	**3.4919**
Password + Fingerprint	**4.5045**
Password + Face	**4.6116**
Password + Iris	**4.7733**
Password + Voice/Speech	**4.3768**
Password + Keystroke Dynamics	**4.3275**
Password + Gait Recognition	**4.4104**
OTP generated applications + OTP using SMS	**2.761**
OTP generated applications + Mobile certificate	**3.9942**

OTP generated applications + Fingerprint	**5.0068**
OTP generated applications + Face	**5.1139**
OTP generated applications + Iris	**5.2756**
OTP generated applications + Voice/Speech	**4.8791**
OTP generated applications + Keystroke Dynamics	**4.8298**
OTP generated applications + Gait Recognition	**4.9127**
OTP using SMS + Mobile certificate	**4.7345**
OTP using SMS + Fingerprint	**6.7574**
OTP using SMS + Face	**6.8645**
OTP using SMS + Iris	**7.0262**
OTP using SMS + Voice/Speech	**6.6298**
OTP using SMS + Keystroke Dynamics	**5.5701**
OTP using SMS + Gait Recognition	**5.6530**
Mobile certificate + Fingerprint	**6.9803**
Mobile certificate + Face	**7.0874**
Mobile certificate + Iris	**7.2491**
Mobile certificate + Voice/Speech	**6.8527**
Mobile certificate + Keystroke Dynamics	**6.8033**
Mobile certificate + Gait Recognition	**6.8863**
Fingerprint + Face	**8.1**
Fingerprint + Iris	**8.2617**
Fingerprint + Voice/Speech	**7.8652**
Fingerprint + Keystroke Dynamics	**7.8159**

Fingerprint + Gait Recognition	**7.8988**
Face + Iris	**8.3688**
Face + Voice/Speech	**7.9723**
Face + Keystroke Dynamics	**7.923**
Face + Gait Recognition	**8.0059**
Iris + Voice/Speech	**8.1341**
Iris + Keystroke Dynamics	**8.0847**
Iris + Gait Recognition	**8.1676**
Voice/Speech + Keystroke Dynamics	**7.6882**
Voice/Speech + Gait Recognition	**7.7712**
Keystroke Dynamics + Gait Recognition	**7.7218**

Na osnovu primjene matematičke formule za 3FA rješenja, date u prethodnom poglavlju jednačina (8), formirana je tabela 8 u kojoj su dati neki od 165 mogućih rezultata ocjene.

Tabela 8. Rezultati ocjene za 3FA rješenja

3FA rješenja	***FES Ocjena***
PIN + Password + OTP generated applications	1.0121
PIN + Password + OTP using SMS	1.5056
PIN + Password + Mobile certificate	2.3278
PIN + Password + Fingerprint	3.0028
PIN + Password + Face	3.0742
PIN + Password + Iris	3.182
PIN + Password + Voice/Speech	2.9177

PIN + Password + Keystroke Dynamics	2.8848
PIN + Password + Gait Recognition	2.9401
Password + OTP using SMS + Mobile certificate	2.7422
Password + OTP using SMS +Fingerprint	3.4172
Password + OTP using SMS + Face	3.4886
Password + OTP using SMS + Iris	3.5964
Password + OTP using SMS + Voice/Speech	3.3321
Password + OTP using SMS + Keystroke Dynamics	3.2992
.....	
.....	
OTP using SMS + Keystroke Dynamics +Face	4.5924
OTP using SMS + Keystroke Dynamics + Iris	4.7002
OTP using SMS + Keystroke Dynamics + Voice/Speech	4.4359
.....	
.....	
Mobile certificate + OTP using SMS + Fingerprint	4.2425
Mobile certificate + OTP using SMS + Face	4.3139
Mobile certificate + OTP using SMS + Iris	4.4217
Mobile certificate + OTP using SMS + Voice/Speech	4.1574
Mobile certificate + OTP using SMS + Keystroke Dynamics	4.1245
Mobile certificate + OTP using SMS + Gait Recognition	4.1798

Iz dobijenih rezultata, prikazanih u tabelama 7 i 8, može se zaključiti da u autentifikacionim pristupima procesi višestruke autentifikacije ostvaruju sinergijski pristup. Pri integrisanju različitih faktora kroz višestruku autentifikaciju, pojedinačni faktori čuvaju njihov izvorni oblik dok dodaju novi sloj zaštite. Stoga, biometrijski metod kao što je *Iris* ili *Face* mogu biti preporučeni kao fundamentalno tehnološko

oružje u borbi za postizanje boljeg zaštitnog faktora. Tabele 7 i 8 pokazuje da je FES alat vrlo efikasan i precizan alat za izračunavanje krisp vrijednosti u nFA rješenjima.

7.1.1. Primjer praktične primjenjivosti

U ovom dijelu rada je urađena implementacija *Fishbone* modela u obliku univerzalni autentifikacioni okvir - UAF upotrebom FES alata za procijenu vrijednosti mobilnih rješenja. FES alat je implementiran i testiran upotrebom MATLAB-a verzija 2015, pri eksploatisanju fazi opisa i procesuiranja napravljenog dostupnim *Fuzzy Sistem Toolbox* [18]. Programski kod za Algoritam 2 (numerička procjena mobilnih metoda autentifikacija u *Fishbone* modelu) koji je urađen u MatLAB-u je dat u prilogu disertacije. Za praktičnu primjenu validnosti i efektivnosti predloženog *Fishbone* modela u obliku UAF, autentifikaciona rješenja iz prakse za 2FA rješenja su uzeta i testirana. Rezultati tih ocjena su dati u tabeli 9.

Tabela 9. Rezultati ocjene za 2FA rješenja iz prakse

2FA rješenja iz prakse	***FES Ocjena***
Face + OTP [174]	5.1139
Password + keystroke dynamic [214]	4.3269
Password + OTP [215]	1.5184
Fingerprint + Password [216]	4.5045
OTP + Fingerprint [217]	5.0068
Face + Voice [218]	7.97235
Face + Passwords [219]	4.6116
Face + Iris [220]	8.3688
OTP + Fingerprint [221]	5.0068

Na osnovu svih gore prezentovanih rezultata u pogledu prema ekspertima i uzimajući u obzir korisničke prioritete SUAPCPC kao kriterijume, moguće je dati preporuku za sljedeće pravilo:

If zaštita je vrlo vrlo visoka AND upotrebljivost je vrlo vrlo visoka AND pristupačnost je vrlo vrlo visoka AND cijena je vrlo vrlo niska AND kompleksnost je vrlo vrlo niska AND privatnost je vrlo vrlo visoka AND pogodnost je vrlo vrlo visoka THEN ocjena je najveća – A.

Preporučeno pravilo predstavlja idealistički šablon u UAF u kojem korisnički prioriteti zadovoljavaju najbolja pojedinačna rješenja za korisnike tj. obezbijeđuje maksimalnu vrijednost za svakog od korisničkih prioriteta. Ovaj šablon predstavlja autentifikaciono rješenje koje ima najveću numeričku vrijednost (ocjena A – 10) u svim autentifikacionim pristupima. Prema tome, ovo pravilo može biti zapisano kao:

$$f_{max} = \{ S_{max} + U_{max} + A_{max} + P_{min} + C_{min} + P_{max} + C_{max} \} \qquad (12)$$

Praktično, programeri treba da teže da stvore metod u kojem će vrijednost takvog metoda biti što je moguće bliža vrijednosti idealističkog šablona. Primjer za ovo je *FIDO U2F* [179] i *HATS* metod [181]. Sa razvijanjem takvih metoda i drugih njima sličnih, biće moguće stvoriti ”*najpogodnije*” nFA rješenje. Takođe, potrebno je napomenuti da, *Fishbone* model može da izgleda kao ograničavajući model ali svaka promjena vrijednosti težinskih koeficijenata generiše novi okvir kao novo rješenje. Uzimajući u obzir korisnička ograničenja poput fizičkih i mentalnih, godina, znanja, i sl., kao i ograničenja pojedinačnih metoda autentifikacija potpuno je jasno da nije moguće razviti jedinstveno nFA rješenje koje bi predstavljalo najbolje korisničko rješenje u mobilnim autentifikacionim pristupima. Da bi se ublažio ovaj problem predloženi *Fishbone* model u obliku UAF daje korisniku mogućnost šireg izbora nFA rješenja. Prema *Fishbone* modelu, “*najpogodniji*” šablon za nFA rješenja prema izdiferenciranim SUAPCPC faktorima treba da uključuju sljedeće metode autentifikacije:

- *Security – Iris.*
- *Usability – PIN.*
- *Accessibility – PIN.*
- *Pricing – PIN.*

- *Complexity – PIN.*
- *Privacy – PIN.*
- *Pogodnost – PIN.*

Na osnovu svega gore prezentovanog moguće je dati bazične karakteristike *Fishbone* modela kao što su:

- Može biti korišćen kao procijenjivajući alat jer daje krisp vrijednost u autentifikacionim pristupima.
- Daje dizajnerima mogućnost dizajniranja nFA rješenja prema odabranim korisničkim prioritetima.
- Implementacijom modela može se prikazati konačan skup rješenja koji su predstavljeni u obliku okvira (f_i).
- Implementacijom modela daje se UAF kao jedno od mogućih rješenja iz skupa konačnih rješenja.
- Daje "*generalizovan*" šablon u UAF čijoj realizaciji i primjeni treba da teže dizajneri.
- Daje mogućnost promjene težinskih koeficijenata za pojedinačne korisničke kriterijume.

Takođe, neophodno je napomenuti da svako odabrano rješenje mobilnog metoda autentifikacije treba da odgovara misiji i ciljevima organizacije. U ovom dijelu rada različite ocjene mobilnih rješenja sa različitim kombinacijama korisničkih faktora su proučene upotrebljavajući fazi zaključni sistem za procijenjivanje mobilnih rješenja. Izlazna 3-D površina fazi zaključnog sistema omogućava analiziranja uticaja i trendova korisničkih faktora sa različitim ocjenama mobilnih rješenja. Neki primjeri tih odnosa su dati na slici 25. Iz prostornih dijagrama datih na slici 25, vidljivo je da se za bilo koja dva izabrana korisnička faktora traži maksimum funkcije, kako bi se dobila najviša ocjena mobilnog rješenja.

Slika 25a. prikazuje uticaj korisničkih faktora, upotrebljivost i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu gornjeg dijela dijagrama, u kojem oba faktora imaju izrazito maksimalne vrijednosti. Međutim, uzimajući u obzir da se u praksi odnos faktora upotrebljivosti i zaštite često nalaze u određenom balansu, poboljšanjem bilo kog faktora narušava se njihov odnos. Sa druge strane, teoretski posmatrano prostorni dijagram ukazuje da je postizanje

maksimalne ocjene nekog mobilnog rješenja moguće postići u slučaju kada oba korisnička faktora imaju maksimalnu vrijednost (*HATS* metod i *FIDO* standard).

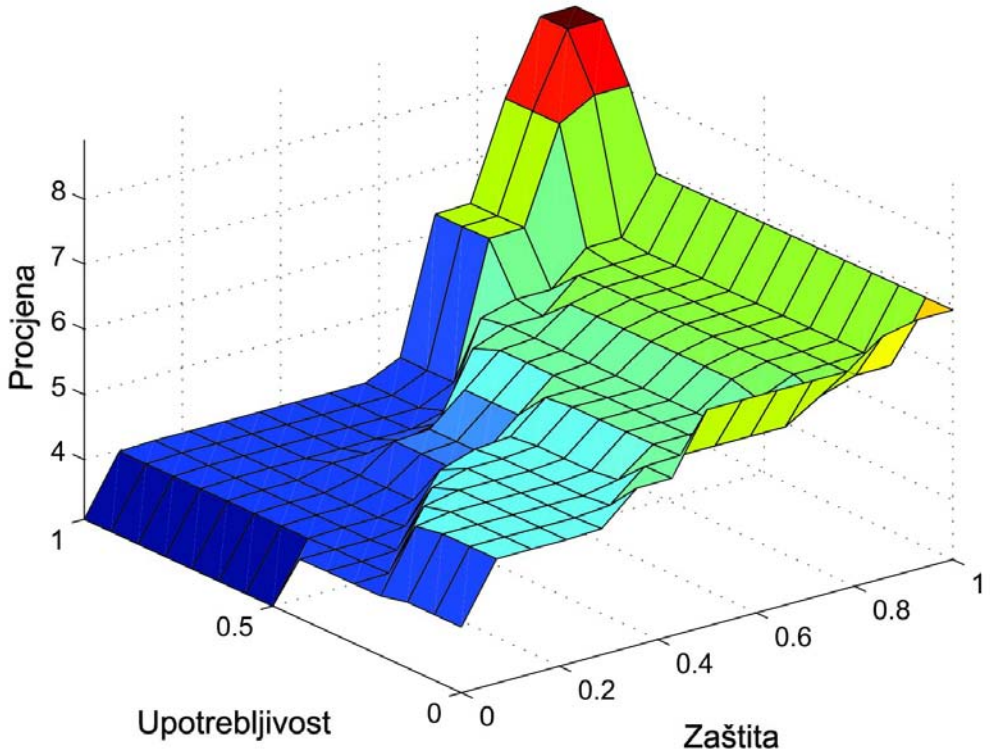
Slika 25b. prikazuje uticaj korisničkih faktora, imenovano pristupačnost i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu gornjeg dijela dijagrama, u kojem faktor pristupačnosti ima varijabilnu vrijednost koja se kreće u granicama neznatno iznad srednje vrijednosti do izrazito maksimalne vrijednosti, dok faktor zaštite ima varijabilnu vrijednost koja se kreće u granicama neznatno iznad srednje vrijednosti do izrazito maksimalne vrijednosti. Kao što može biti primjećeno iz dijagrama, postoji određena sličnost između faktora pristupačnosti i upotrebljivosti. Na osnovu sličnosti karakteristika ovog dijagrama sa prethodnim dijagramom može se zaključiti, zašto autori poput Thatcher-a *et al.,* [194] navode faktor pristupačnosti kao podskup faktora upotrebljivosti.

Slika 25c. prikazuje uticaj korisničkih faktora, privatnost i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu gornjeg dijela dijagrama, u kojem faktor zaštite ima varijabilnu vrijednost koja se kreće u granicama neznatno iznad srednje vrijednosti do izrazito maksimalne vrijednosti, dok faktor privatnosti ima izrazito maksimalnu vrijednost.

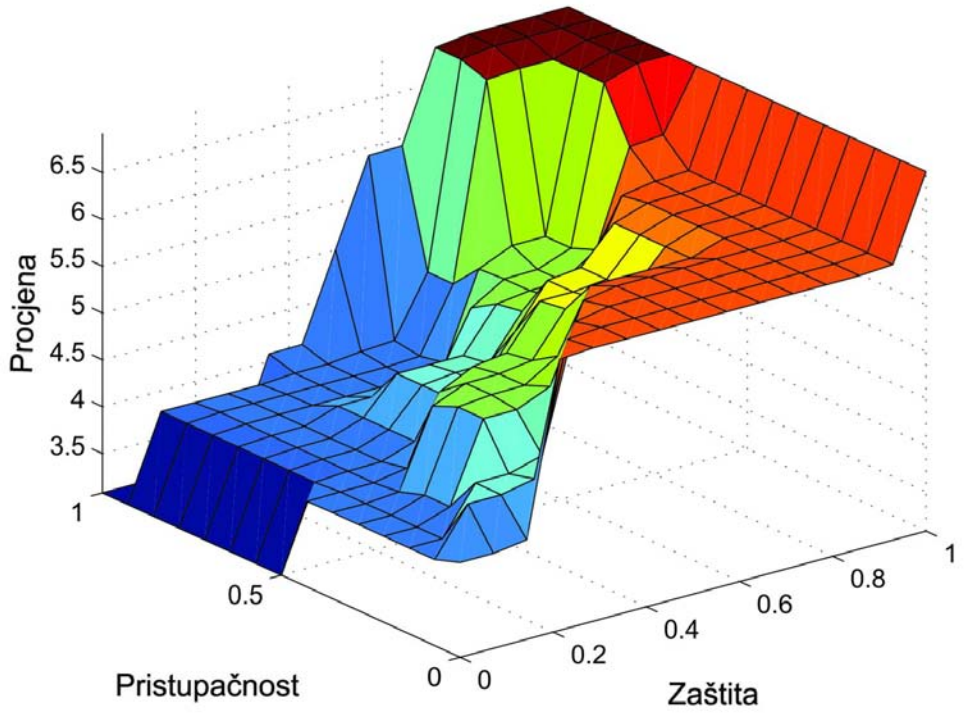
Slika 25d. prikazuje uticaj korisničkih faktora, cijena i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da je maksimum funkcije pokriva površinu gornjeg dijela dijagrama, u kojem faktor zaštite ima izrazito maksimalnu vrijednost, dok faktor cijene ima varijabilnu vrijednost koja se kreće u granicama od izražene minimalne vrijednosti do maksimalne vrijednosti.

Slika 25e. prikazuje uticaj korisničkih faktora, privatnost i cijena, na ocjenu mobilnog rješenja. Na slici se može vidjeti da oba faktora imaju izrazito maksimalne vrijednosti.

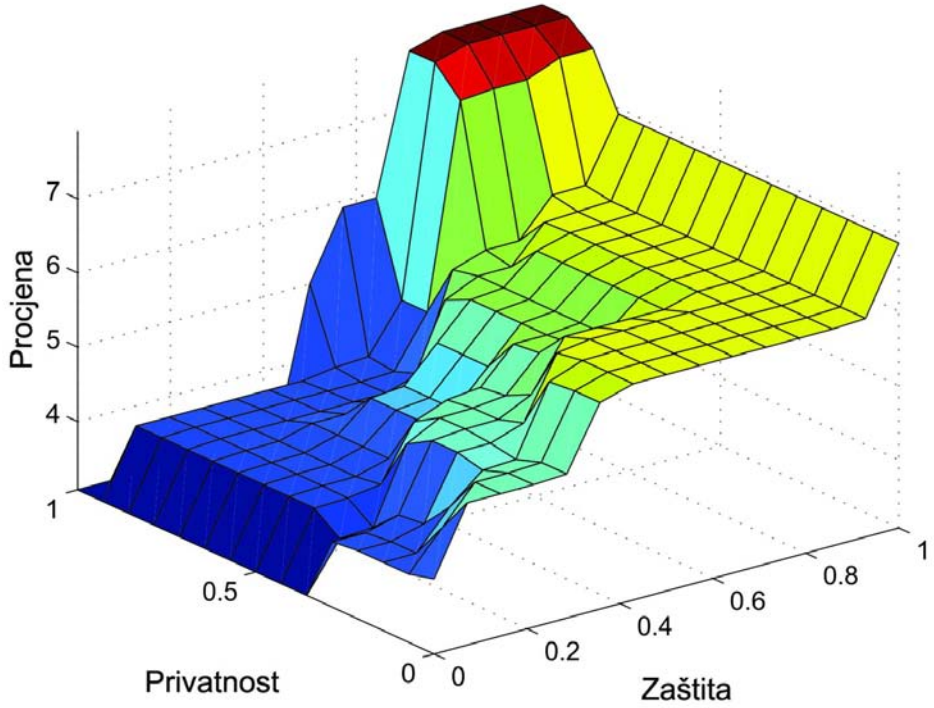
Slika 25f. prikazuje uticaj korisničkih faktora, pogodnost i kompleksnost, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu u kojem faktor kompleksnosti ima izrazito maksimalnu vrijednost, dok faktor pogodnosti ima varijabilnu vrijednost koja se kreće u granicama od srednje do izrazito maksimalne vrijednosti.



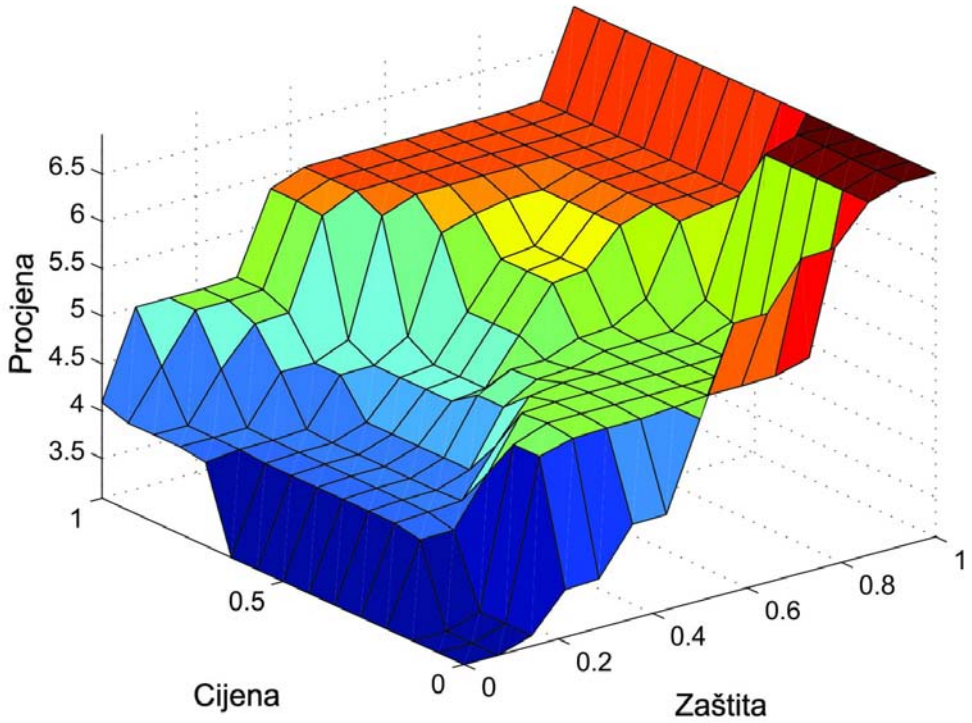
Slika 25a. Izlazna 3-D površina korisničkih faktora upotrebljivosti i zaštite na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



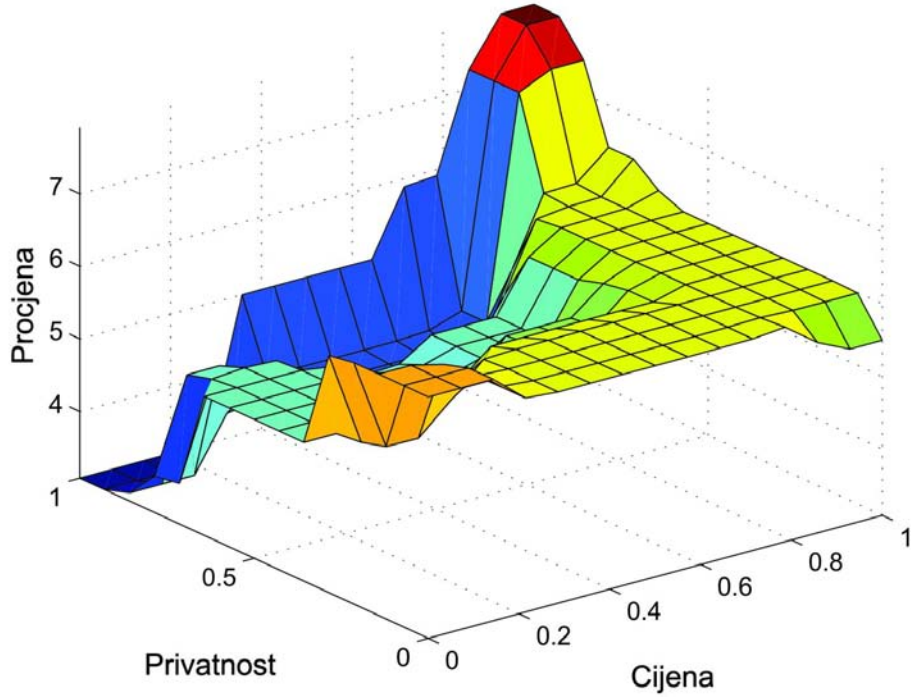
Slika 25b. Izlazna 3-D površina korisničkih faktora pristupačnosti i zaštite na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



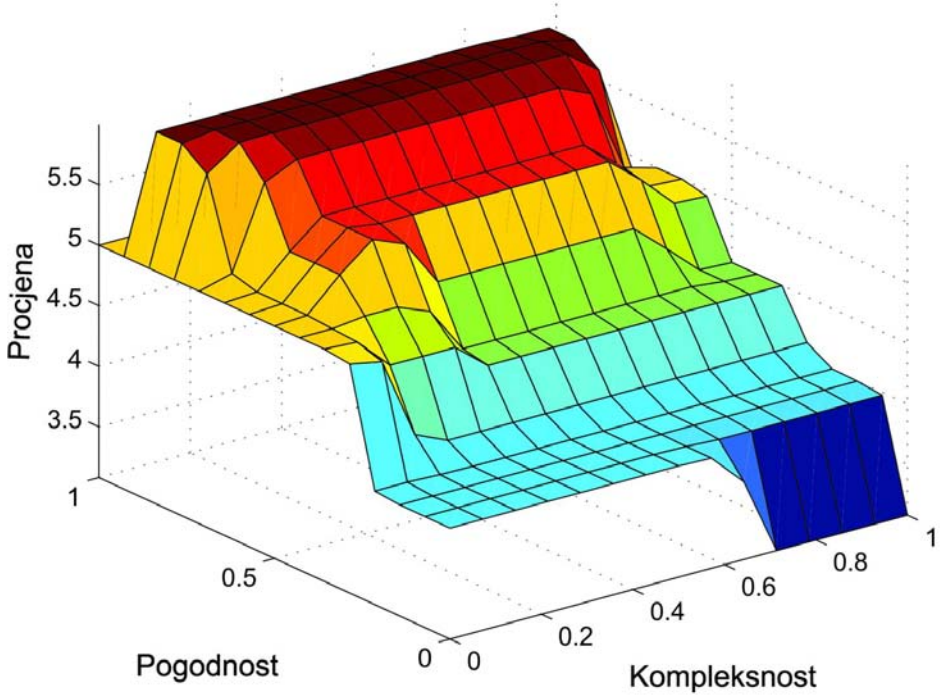
Slika 25c. Izlazna 3-D površina korisničkih faktora privatnosti i zaštite na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 25d. Izlazna 3-D površina korisničkih faktora cijena i zaštita na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 26e. Izlazna 3-D površina korisničkih faktora privatnost i cijena na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 25f. Izlazna 3-D površina korisničkih faktora pogodnost i kompleksnost na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.

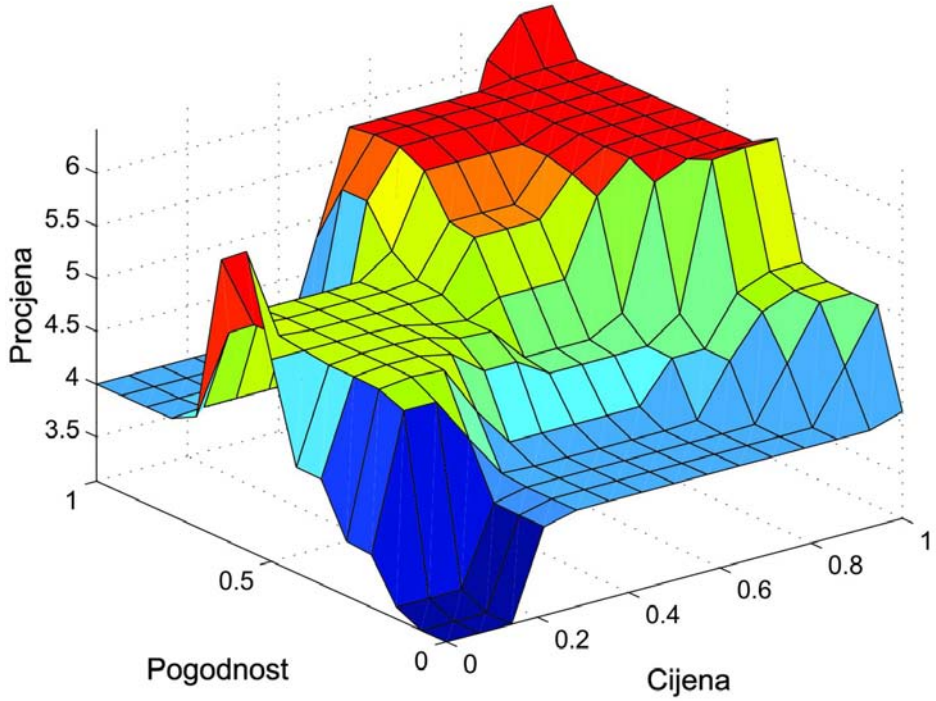
Slika 25g. prikazuje uticaj korisničkih faktora, pogodnost i cijena, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu u kojem faktor pogodnosti ima varijabilnu vrijednost koja se kreće u granicama neznatno ispod srednje vrijednosti do izrazito maksimalne vrijednosti, dok faktor cijene ima varijabilnu vrijednost koja se kreće u granicama od srednje do izrazito maksimalne vrijednosti.

Slika 25h. prikazuje uticaj korisničkih faktora, kompleksnost i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu u gornjem dijelu dijagrama, u kojem faktor kompleksnosti ima varijabilnu vrijednost koja se kreće u granicama od minimalne do maksimalne, dok faktor zaštite ima maksimalnu vrijednost.

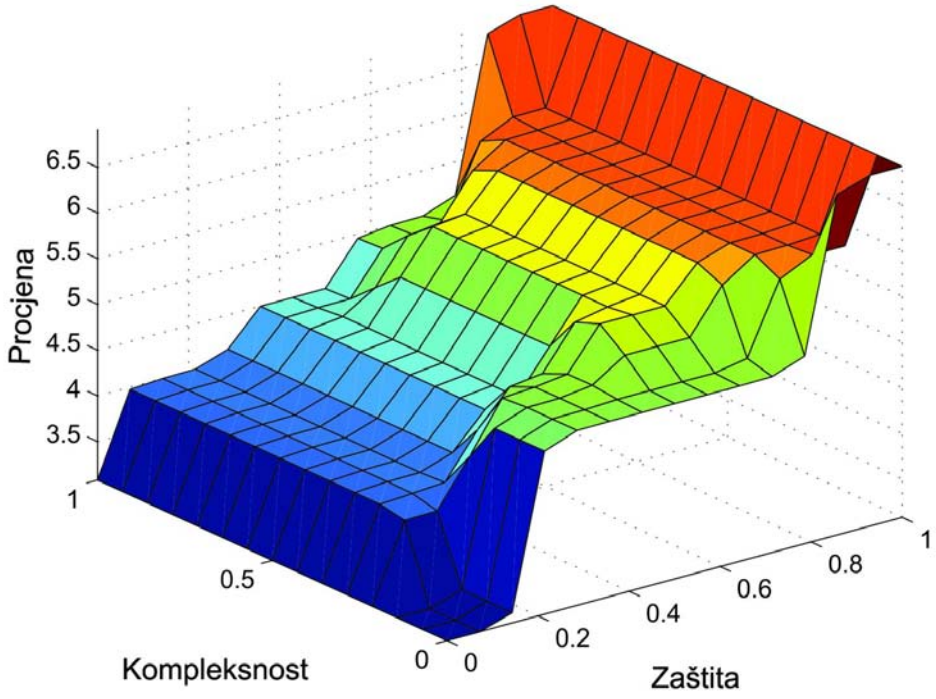
Slika 25i. prikazuje uticaj korisničkih faktora, pogodnost i privatnost, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu u kojem faktor pogodnosti ima varijabilnu vrijednost koja se kreće u granicama neznatno iznad minimalne vrijednosti do izrazito maksimalne vrijednosti, dok faktor privatnosti ima varijabilnu vrijednost koja se kreće u granicama od srednje vrijednosti do izrazito minimalne vrijednosti.

Slika 25j. prikazuje uticaj korisničkih faktora, pogodnost i upotrebljivost, na ocjenu mobilnog rješenja. Na slici se može vidjeti da je maksimum funkcije pokriva površinu u kojem faktor pogodnosti ima varijabilnu vrijednost koja se kreće u granicama neznatno ispod maksimalne vrijednosti do izrazito maksimalne vrijednosti, dok faktor upotrebljivosti ima varijabilnu vrijednost koja se kreće u granicama od neznatno iznad srednje vrijednosti do izrazito minimalne vrijednosti.

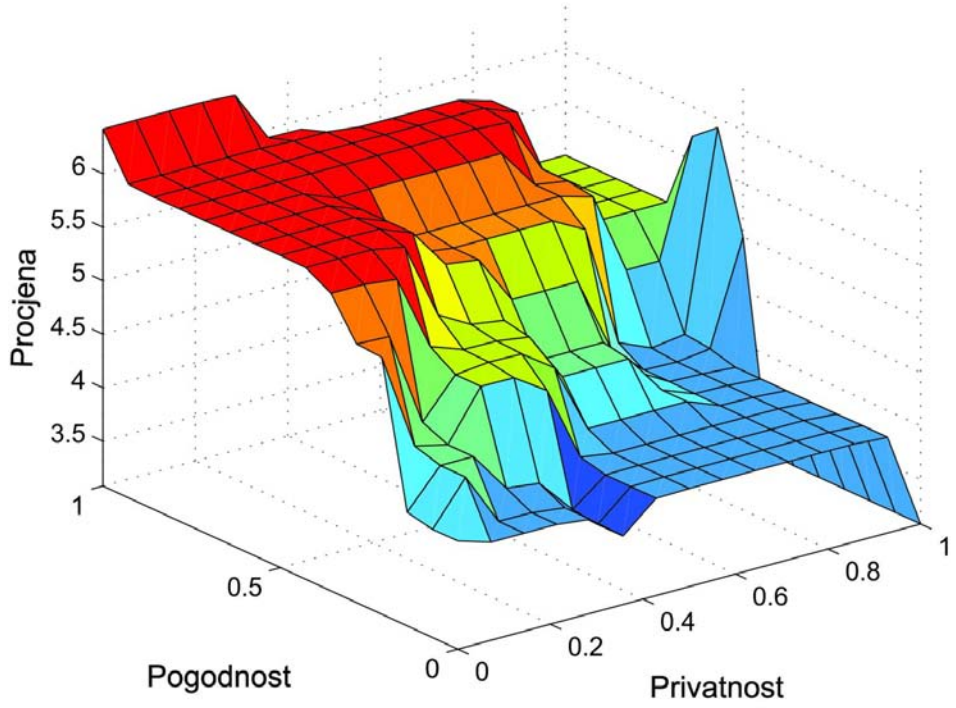
Slika 25k. prikazuje uticaj korisničkih faktora, pogodnost i zaštita, na ocjenu mobilnog rješenja. Na slici se može vidjeti da maksimum funkcije pokriva površinu u kojem oba faktora imaju varijabilne vrijednosti koje se kreće u granicama neznatno iznad srednje vrijednosti do izrazito maksimalne vrijednosti.



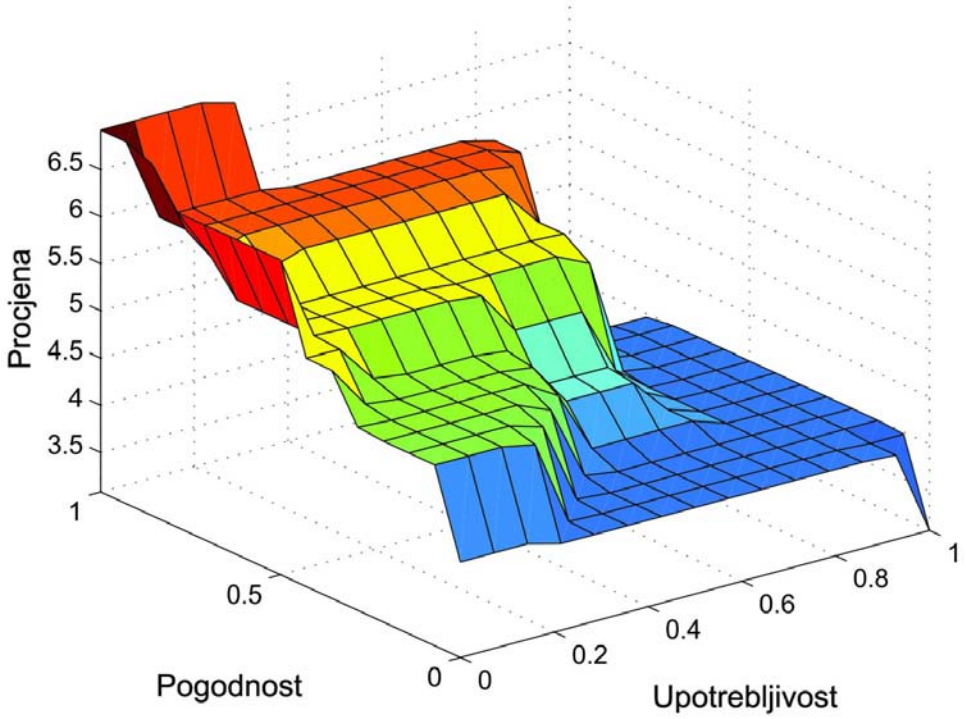
Slika 25g. Izlazna 3-D površina korisničkih faktora pogodnost i cijena na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



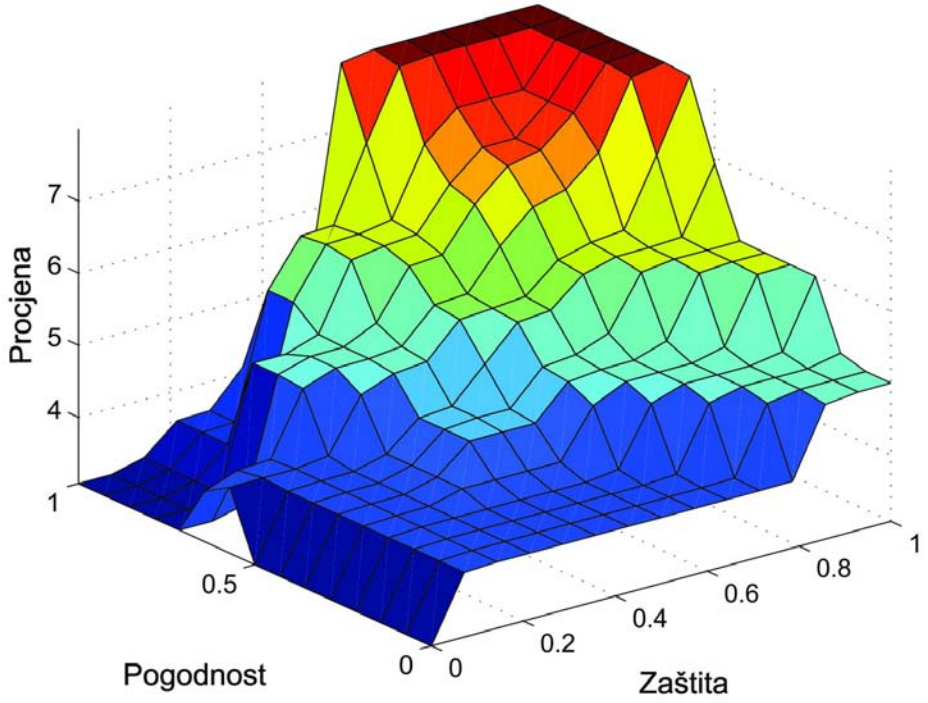
Slika 25h. Izlazna 3-D površina korisničkih faktora kompleksnost i zaštita na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 25i. Izlazna 3-D površina korisničkih faktora pogodnost i privatnost na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 25j. Izlazna 3-D površina korisničkih faktora pogodnost i upotrebljivost na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.



Slika 25k. Izlazna 3-D površina korisničkih faktora pogodnost i zaštita na osnovu fazi ekspertnog sistema za ocjenu mobilnog rješenja.

7.2. Pravci daljeg istraživanja

U ovoj disertaciji, kao pravci budućih istraživanja diskutovani su istraživački pravci u skladu sa širinom okvira predložene teme tj. definisanja metričkog pristupa u širem smislu riječi u dijelu rizika u EMDI dok u užem smislu riječi definisanja proširivanja n-torki korisničkih prioriteta u *Fishbone* modelu. Nesumnjivo, budući značaj mobilne autentifikacije najbolje je istakao Al-Khouri ”*buduće mobilne autentifikacije u informacionoj eri će odrediti konkuretnost država i njihovu spremnost da prežive buduće izazove*” [222]. Dakle, pored ostvarenih naučnih doprinosa ova disertacija ima za cilj da otvori novi set pitanja za buduća istraživanja u kojima bi se napravio iskorak prema proširivanju n-torki korisničkih prioriteta gdje “n” predstavlja dimenziju prostora u kojem je UAF smješten. Takođe, budući pravac istraživanja je analiza proširivanja mobilnih metoda autentifikacija prema kojima bi bilo izvršeno numeričko vrednovanje u *Fishbone* modelu. U širem smislu riječi, ovaj rad ima za cilj da otvori novi set pitanja za buduća istraživanja u kojima bi se napravio iskorak prema stvaranju metričkog rizika u EMDI koji bi omogućio mjerenje implementacija modela, a stim i mogućnost njihovog poboljšanja. U prilogu potvrde navedenom govori i rad [223] koji naglašava

"*Ako vi ne možete nešto izmjeriti (implementirani model), vi ne možete ni poboljšati to*". U ovoj disertaciji, otvoreno pitanje rizika predstavlja izazovan koncept koji je zasnovan na mogućnosti upotrebe metrologije (nauke o mjerenju) i metrike (numeričke vrijednosti) u EMDI za procjenu rizika. Ovaj pristup otvara novi set pitanja u vidu identifikovanja i drugih korisničkih prioriteta koji imaju uticaj na specifikaciju zahtjeva zaštite, a mogu biti korišćeni kao osnovni set metrike za kvantifikaciju rizika u EMDI. Pristup zasnovan na metrici za procjenu rizika u EMDI zahtijeva sagledavanje svih njegovih procesa. Kako su procesi u EMDI jasno izdiferencirani sa svim podprocesima tako ovaj model daje mogućnost dekompozicije rizika. Sa funkcionalnom dekompozicijom rizika sveobuhvatni problemi mogu biti analizirani nezavisno, što omogućava bolje određivanje sveukupnih zahtjeva po pitanju zaštite.

Na osnovu date jednačine (11) u prethodnom poglavlju VI, ukupni rizik pridružen EMDI je suma svih pojedinačnih vrijednosti rizika svih mogućih neželjenih događaja (R_i) prema posmatranim procesima u životnom ciklusu ovog modela. Ipak, bazično pitanje u konceptu rizika je kvantifikacija odnosno određivanja bazičnih komponenti koje doprinose stvaranju rizika. Prijedlog za bolje definisanje zahtjeva zaštite u EMDI prvenstveno treba da obuhvati sve ključne korisničke faktore i kao takvi treba da budu razmatrani na pristupu zasnovanom na metrici. Taj pristup zahtijeva izradu i upotrebu detaljne taksonomije u EMDI. U ovom modelu, taksonomija treba da posluži kao referentni okvir za bolje razumijevanje procesa u EMDI i identifikovanju različitih aspekata koji treba da budu uzeti u obzir pri specifikovanju zahtjeva zaštite i analiziranju mogućih rizika. Stoga, cilj taksonomije treba da pomogne u klasifikovanju svih dekompozicioniranih rizika na osnovu kojih je moguće predložiti rješenja za ublažavanje ranjivosti i prijetnji prisutnih u modelima menadžmenta identiteta. Na ovaj način može se pomoći u identifikovanju rizika uključenih u svaki proces koji može biti korišćen kao ključni dio u definisanju metričkog rizika koji su relevantni za kvantifikaciju. Svaki izdiferencirani ključni prioritet u taksonomiji bio bi nazvan kategorijom rizika i predstavljao bi skup inicijalnih metrika, na primjer rizik zaštite, rizik upotrebljivosti, i sl. Uvođenjem ovakvog skupa inicijalnih metrika generalno bi doprinijeli preciznijoj procjeni rizika u EMDI. Na taj način bi ukupni rizik integrisao sve kategorije rizika u jednu cjelinu. Obuhvatajući sve kategorije rizika zahtjevi zaštite bi donijeli mnogo detaljnije rezultate. Bazični cilj metrologije u EMDI treba da bude identifikovanje svih nezavisnih pojmova koji doprinose procjenu ukupnog rizika. Sa ovim pristupom se obezbijeđuje semantičko značenje definicije metrika i dodjeljuju

lingvističke skale za svaki od kategorija rizika. To podrazumijeva da se svakoj kategoriji rizika dodjeljuju opisne jedinice primjera radi, nizak, srednji i visok (tri lingvističke skale). Deskriptivni termin bio bi korišćen da ukaže u kom obimu određeni rizik ugrožava posmatrani proces. Kako deskriptivne ocjene na lingvističkoj skali nemaju mogućnost izražavanja konkretne numeričke vrijednosti potrebno je iste dovesti u određeni relacioni odnos sa numeričkim vrijednostima. To bi bilo moguće postići uvođenjem funkcije pripadnosti gdje se deskriptivne ocjene mogu matematički izraziti stepenom pripadnosti koja ima vrijednost iz jediničnog intervala [0,1].

S obzirom da napadači mogu pristupiti i ekploatisati slabostima u bilo kom procesu ili podprocesu menadžmenta identiteta, oni time mogu narušiti osnovna načela zaštite informacija kao što je povjerljivost, integritet i raspoloživost (CIA). Na osnovu toga, može se zaključiti da EMDI je izložen kontinuiranom riziku od moguće zloupotrebe. Da bi se ublažili ili smanjili rizici u ovom modelu potrebno je specifikovati zahtjeve zaštite. Svrha definisanja zahtjeva zaštite u pogledu menadžmenta identiteta je da poveća povjerenje u procesu stvaranja identiteta i poveća povjerenje da pojedinac koji koristi digitalni identitet je pojedinac za koga je bio i izdat [223]. Međutim, obezbijeđivanje nivoa povjerenja je i uslovljeno poslovnim ciljem i misijom organizacije koji se suštinski mogu razlikovati među organizacijama. Sa ovim uslovom otvara se novi set pitanja u vidu identifikovanja i drugih korisničkih prioriteta koji su bitni za organizacije pri izboru mehanizma zaštite. Stoga, ovaj istraživački izazov se čini još izazovnijim sa identifikovanjem korisničkih prioriteta koji su već naglašeni kod *Fishbone* modela, i određivanja njihovog balansa na osnovu kojeg organizacije prave izbor metode autentifikacije. U EMDI daje se prijedlog za smanjivanje ili ublažavanje identifikovanih rizika specifikovanih za svaki proces odnosno podproces u cilju definisanja boljih zahtjeva zaštite. Međutim, za pravce daljeg istraživanja identifikovani fundamentalni izazov ostaje otvoren za rješavanje u cilju što boljeg upravljanja identitetima. Prema tome, za procjenu rizika u EMDI potrebno je da pravci daljeg istraživanja uključuju određivanje taksonomije za kategorizaciju rizika zasnovanog na metričkom pristupu i definišu inicijalni skup novih metrika sa kojim bi se omogućilo razvijanje novog oblika kvantifikacije rizika u ovom okruženju. To podrazumijeva da budući ciljevi istraživanja treba da budu usmjereni da izvedu širi skup metrika u EMDI i obezbijede ne samo semantičko opisivanje već i detaljnu numeričku vrijednost.

VIII ZAKLJUČAK

Primarni cilj ovog istraživanja predstavlja razvoj modela zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom (IAM), kao i unapređenje postojećih metoda zaštite. Predmet istraživanja je usmjeren na autentifikacione mehanizme odnosno na nFA metode koje su ključne u procesu menadžmenta identiteta kao najvažnijoj disciplini za upravljanje i zaštiti pristupa informacijama i resursima u organizacijama. U širem smislu riječi, menadžment identiteta predstavlja poseban istraživački izazov koji zahtijeva adekvatan pristup u razumijevanju koncepta digitalnih identiteta. Baveći se ovim pitanjem adresiran je problem ovog rada čijim rješavanjem se daje važan doprinos ove doktorske disertacije. Uzimajući u obzir da su digitalni identiteti od fundamentalnog značaja za modele menadžmenta identiteta, neophodno je da bilo koja strategija bavljenja modelima menadžmenta identiteta bude zasnovana na punom razumijevanju digitalnih identiteta. Povezanost menadžmenta identiteta sa digitalnim identitetima je obostrana jer upravljanje identitetima određuje okruženje i pravila za upravljanje digitalnim idenititetima i njihov cjelokupni proces, dok kroz zaštitu digitalnih identiteta istovremeno se postiže i zaštita menadžmenta identiteta.

U disertaciji je predložen novi edukacioni model digitalnog identiteta - EMDI u sistemima menadžmenta identiteta. Ovaj model, za razliku od svih drugih modela, predstavlja novi prošireni pristup bazičnih modela digitalnog identiteta koji uvodi dva važna procesa planiranja i povratne informacije. Takođe, specifičnost ovog modela čini proces održavanja koji "*zadire*" u proces stvaranja. U ovom radu, EMDI je primjenjen u *Moodle* platformi u obliku novog plagina kao podmodel za filtriranje neaktivnih identiteta. Predloženi plagin ima za cilj da uspostavi izgubljenu komunikaciju između studenta i administratora na mnogo operativniji način. To podrazumijeva da plagin primjenom *feedback* procesa omogućava interaktivnu komunikaciju između administratora i studenta tako da identitet ne može biti obrisan bez prethodnog studentskog znanja. Pored toga, ovaj plagin smanjuje konflikte između aktivnih i neaktivnih digitalnih identiteta, i smanjuje ili ublažava potpunu ili djelimičnu krađu identiteta. Drugim riječima, značaj ovih procesa je u smanjenju mogućnosti stvaranja "*džepova*" u edukacionom sistemu koji ostavlja hakerima mnogo manje prostora za manipulisanje. Time se ublažava djelimična konfuzija prirode koncepta menadžmenta identiteta.

Pored gore navedenog, u EMDI su identifikovani izazovi, pridruženi rizici kao i prijedlozi rješenja sa kojim se mogu smanjiti ili ublažati ti rizici. Identifikovani izazovi i rizici su holistički razmatrani kroz funkcionalnu dekompoziciju procesa koji su detaljno opisani i integrisani kroz životni ciklus EMDI. Na osnovu izvršene analize arhitekture i procesa EMDI može se zaključiti da je svaki proces jednako važan u smislu postizanja pouzdanijeg, fleksibilnijeg, efektivnijeg i efikasnijeg funkcionisanja edukacionog sistema menadžmenta identiteta. Nedostaci u bilo kom procesu EMDI vode ka slabostima u cijelom sistemu što značajno doprinosi stvaranju plodnijeg tla za razvoj krađe identiteta. U ovoj disertaciji, dat je dijagram toka podataka digitalnog identiteta sa napisanim pseudo kodom za specifični proces održavanja u životnom ciklusa digitalnih identiteta. Ovaj pseudo kod algoritma 1 pisan je u formi PL/SQL programskog koda, i pokazuje praktičnu izvodljivost opisanog modela u pogledu stvaranja veb aplikacija u modernim softverskim sistemima. U tom kontekstu, veoma je bitno naglasiti da ovaj model je važan u rješavanju pitanja zaštite u *e-learning* okruženju.

Da bi se u užem smislu riječi došli do modela zaštite informacija u IAM, disertacija daje komparativni pregled savremenih metoda autentifikacije zasnovane na korisničkim SUAPCPC faktorima sa svim njihovim izdiferenciranim prednostima i nedostacima. U ovom radu je predložen *Fishbone* model za procjenu postojećih i dizajniranje novih autentifikacionih rješenja. Pored toga, u radu je urađena fazifikacija *Fishbone* modela odnosno razvijen je FES alat. Konačno, na osnovu dobijenih rezultata urađena je implementacija i verifikacija *Fishbone* modela. Dakle, ova disertacija je dala pregled, klasifikaciju i komparaciju dosadašnjih istraživanja i analiza naučnih radova iz oblasti savremenih metoda autentifikacije namjenjenih za mobilne uređaje, čime je dobijena precizna slika o trenutnim dostignućima u ovoj oblasti. Ono što je ključno, prethodni radovi ukazuju da ne postoji rad za numeričko procijenjivanje metoda autentifikacije odnosno ne postoji metodologija pronalaženja krisp vrijednosti u autentifikacionim pristupima. Sa nepostojanjem krisp vrijednosti u autentifikacionim pristupima nije ni moguće sagledati kvalitetan izbor odgovarajuće metode autentifikacije u dizajniranju bilo kog nFA rješenja. Takođe, određivanje korisničkih prioriteta je suštinsko pitanje u dizajniranju nFA rješenja. Dakle, u ovoj disertaciji adresiran je suštinski problem nepostojanja krisp vrijednosti i predložen je model za njegovo rješavanje, a čiji je cilj dobijanje krisp vrijednosti u autentifikacionim pristupima prema izdiferenciranim korisničkim prioritetima.

Prema tome, najvažniji doprinos ove doktorske disertacije koja ga izdvaja od svih drugih radova, predstavlja razvoj nove originalne metodologije sa kojom se obezbijeđuje numeričko procjenjivanje mobilnih metoda autentifikacije prema izdiferenciranim korisničkim SUAPCPC faktorima. Na taj način, omogućava se dizajnerima da dizajniraju nova mobilna krisp autentifikaciona rješenja sa kojima se postiže bolji sinergijski pristup u nFA rješenjima. U odnosu na druge dostupne radove, ova disertacija komparativno razmatra holistički širi skup savremenih korisničkih metoda autentifikacija za mobilne uređaje kao i korisničkih faktora sa širim skupom klasifikovanih ulaza *VVL, VL, L, M, H, VH* i *VVH*. U tom pogledu, ovaj predloženi pristup donosi sve korisničke faktore i metode autentifikacije integrisane u jednu cjelinu. Metod komparacije mobilnih metoda autentifikacija zasnovanih na sveobuhvatajućim SUAPCPC faktorima daje mnogo detaljnije rezultate. Dakle, na osnovu analize prethodnih radova kritičkog osvrta na prethodne radove i ostvarenih rezultata u ovom istraživanju *Fishbone* model je predložen.

Za dizajn i implementaciju *Fishbone* modela korišćen je fazi pristup za krisp procjenjivanje i dizajniranje mobilnih autentifikacionih rješenja. Primjenom fazi logike se na pogodan način proširuju funkcije klasičnih relacija integrišući nepreciznosti, neodređenosti i nejednoznačnosti koje se ne mogu zanemariti u autentifikacionim pristupima. Dakle, za implementaciju *Fishbone* modela korišćen je inovativni FES alat, koji je posebno razvijen u ovoj disertaciji, kao krisp alat za procjenu savremenih korisničkih mobilnih metoda autentifikacija. Potrebno je posebno istaknuti da je ovo prvi put u autentifikacionim pristupima u kome je razvijen FES alat zasnovan na fazi logici i fazi skupovima. U ovoj disertaciji je pokazano kako fazi sistemi mogu biti uspješno korišćeni za procjenjivanje mobilnih autentifikacionih rješenja. Implementacija ovog modela je urađena pomoću eksterne aplikacije MATLAB-a za izračunavanje kompleksnih matematičkih izraza.

Prema tome, rezultati primjene predloženog *Fishbone* modela su pokazali opštost *Fishbone* modela tj. da *Fishbone* model obezbijeđuje UAF za kvantifikovanje nFA metoda u mobilnom autentifikacionim pristupima. Pored navedenog, prednosti predloženog modela su:

- Može se koristiti i u slučajevima kada se radi sa nedovoljno preciznim informacijama dobijenih od strane krajnjih korisnika.

- Obezbijeđuje UAF za kvantifikovanje nFA metoda u mobilnim autentifikacionim pristupima.
- Praktičan i efikasan u dobijanju crisp vrijednosti.
- Fleksibilan i lak za modifikaciju pored toga FES može biti korišćen za nova autentifikaciona rješenja koja budu u bliskoj budućnosti dizajnirana. Eventualne izmjene zahtijevaju samo dodavanje neke druge varijable (mobilnu metodu autentifikacije ili korisničkog prioriteta) ili pravila bez dopunskog razvoja.
- Može se primjeniti za bilo koji informacioni sistem.
- Primjenjiv za nFA rješenja u sistemima koja zahtijevaju istovremenu primjenu dva ili više kriterijuma istih ili različitih težinskih koeficijenata.
- Pomaže korisnicima da izaberu najpogodnije mobilno rješenje za njihov upotrebni scenario.
- Daje mogućnost zamjene korisničkog prioriteta i dobijanje ocjene za izabrano mobilno rješenje prema tom prioritetu.
- Popunjava praznine u trenutnim istraživanjima i pomaže istraživačima da kreiraju najbolji mix mobilnih metoda autentifikacija.
- Ukazuje da nije moguće stvoriti jedinstveno najpogodnije nFA rješenje u praksi jer različiti korisnici imaju različite zahtjeve u pogledu određivanja njihovih prioriteta.
- Daje formalne kvantitativne rezultate savremenih mobilnih metoda autentifikacija.

Teorijsko razmatranje i praktična primjena *Fishbone* modela u obliku UAF pokazali su da u ovom radu važi osnovna istraživačka hipoteza doktorske disertacije:

- Razvojem novog jakog autentifikacionog mehanizma u korisničko-orjentisanom modelu menadžmenta identiteta zasnovanog na principu personalnog autentifikacionog uređaja, može se postići visok nivo zaštite identiteta.

Radi se o razvoju više faktorskih metoda autentifikacije 2FA i 3FA.
Primjer za 2FA je autentifikacioni mehanizam ***Mobile certificate + Iris***.
Primjer za 3FA je autentifikacioni mehanizam ***Pasword + Mobile certificate + Iris***.

Pored osnovne hipoteze istraživanja u doktorskoj disertaciji je potvrđeno da vrijede i sljedeće posebne hipoteze:

- Proces razvoja mehanizma autentifikacije treba biti zasnovan na postojećim iskustvima i modelima.

U poglavljima V i VI opisane su metode autentifikacije, i dat je pregled postojećih modela zaštite informacija i autentifikacionih rješenja. Sva postojeća autentifikaciona rješenja su bila razvijena u pogledu nekog od korisničkih faktora kao što su zaštita, upotrebljivost, pristupačnost, kompleksnost, cijena, privatnost i pogodnost (SUAPCPC). U poglavlju 6.1.2. predstavljena su ograničenja osnovnih modela zaštite informacija. U tom poglavlju je naglašeno da modeli zaštite u trenutku testiranja mogu da potvrde sigurnost sistema, dok već u sljedećem testiranju mogu pokazati određene ranjivosti što ukazuje da proces razvoja mehanizma autentifikacije treba da bude zasnovan na postojećim modelima zaštite informacija. Prosto rečeno, test razvoja novog mehanizma autentifikacije treba da bude implementiran na postojećim modelima zaštite.

- Personalni autentifikacioni uređaji podržavaju višestruke autentifikacione procese uključujući i biometrijske tehnologije.

U poglavlju 4.3. učesnici i zahtjevi u IAM opisan je personalni autentifikacioni uređaj u pogledu podržavanja nFA i biometrijskih tehnologija.

- Analizom i prikazivanjem osnovnih mehanizama autentifikacije može se utvrditi potreba i efikasnost uvođenja jake autentifikacije.

U poglavlju V metode autentifikacija eksplicitno su izdiferencirani nedostaci postojećih metoda autentifikacija na osnovu kojih je utvrđena potreba i efikasnost uvođenja jake autentifikacije.

- Procesom univerzalne jake autentifikacije može se omogućiti sigurnija zaštita identiteta.

U poglavlju 6.2.1. dat je pregled kriterijuma za komparaciju i komparacija, i pregled i opis korisničkih SUAPCPC faktora. U istom poglavlju, istaknuto je da su svi faktori blisko povezani tj. postoji korelacija između njih. U poglavlju 6.3. prijedlog novog *Fishbone* modela zaštite informacija u sistemima za IAM, istaknuto je da korisnici u

mobilnim autentifikacionim pristupima nemaju korisničke kriterijume istog stepena značajnosti. Na osnovu tih činjenica u istom poglavlju je dat univerzalni autentifikacioni okvir - UAF u *Fishbone* modelu sa kojim se može omogućiti sigurnija zaštita identiteta.

Dokazivanjem navedenih hipoteza ostvaren je fundamentalni cilj istraživanja u ovoj doktorskoj disertaciji koji se odnosi na model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom kao i dizajniranjem alata kojim se omogućava izbor metoda autentifikacije u korisničko – orijentisanom modelu IAM sistema sa kojim se postiže visok nivo zaštite identiteta uzimanjem u obzir svih specifičnih vrijednosti SUAPCPC korisničkih faktora.

IX Literatura

1. Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A. SAFETY VS. SECURITY? Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management May 14-18, 2006, Management (PSAM), ASME Press, New Orleans.
2. Kissel R.L. Glossary of Key Information Security Terms. NIST Interagency/Internal Report (NISTIR) 2013.
3. Peltier ,T.R., Peltier, J. and Blackley, J. Formation security fundamentals, Boca Raton, Fl, Auerbach, 2005.
4. Whitman, M.E. and Mattord H.J. Principles of Information Security Fourth Edition, Boston, MA, Course Technology, 2012.
5. Maconachy, W.V., Schou C.D., Ragsdale, D. and Welch, D.A Model for Information Assurance: An Integrated Approach. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June.
6. Krause, M. and Tipton, H.F. Handbook of Information Security Management. CRC Press LLC 1998.
7. Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition. CRC Press LLC 2004.
8. Murphy, G.B. Systems Security Certified Practitioner Study Guide, Indianapolis, Indiana, John Wiley & Sons, Inc., 2015.
9. Harris, S. and Maymí, F. Cissp All-In-One Exam Guide, Seventh Edition (Hardcover), New York Mcgraw-Hill, 2016.
10. Hansche, S., Berti, J., Hare, C. Official (ISC)² guide to the CISSP exam, Boca Raton, Fl, Auerbach Publications, 2003.
11. Tudor, J.K. Information security architecture: an integrated approach to security in the organization. Boca New York Washington, D.C by CRC Press LLC, 2001. Hansche S., Berti J., and Hare C. Official (ISC)² guide to the CISSP exam, Boca Raton, Fl, Auerbach Publications, 2003.

12. Kiljan, S., van Eekelen, M. and Vranken, H. Evaluation of transaction authentication methods for online banking. Future Generation Computer Systems, 80, 430-447, 2018.
13. Ayodele, T., Shoniregun, C.A. and Akmayeva, G. Towards e-learning security: A machine learning approach. *In Information Society (i-Society), 2011 International Conference* (pp. 490-492). IEEE, 2011.
14. Capobianco, B.M., French, B.F., and Diefes-Du, H.A. Engineering identity development among pre-adolescent learners. *Journal of Engineering Education, 101*(4), 698–716, 2012.
15. Windley, P. *Digital Identity*. United States of America: O'Reilly Media, Inc., 2005.
16. Gomi H. A persistent data tracking mechanism for user-centric identity governance. *Identity in the Information Society*, 3(3), 639-656, 2010.
17. La Polla, M., Martinelli, F. and Sgandurra, D. A survey on security for mobile devices. IEEE Communications Surveys and Tutorials, 15(1), 446-471, 2013.
18. Korać, D. and Simic, D, Design of Fuzzy Expert System for Evaluation of Contemporary User Authentication Methods Intended for Mobile Devices, Journal of Control Engineering and Applied Informatics, 19(4), 2017.
19. Kim, S., Oh, H.T. and Kim, Y.G. Certificate sharing system for secures certificate distribution in mobile environment. Expert Systems with Applications, 44, 67-77, 2016.
20. Nuñez, D. and Agudo, I. BlindIdM: A privacy-preserving approach for identity management as a service. *International Journal of Information Security*, Springer Berlin Heidelberg, 13(2), 199-215, 2014.
21. Noëmi Manders-Huits. *Practical versus moral identities in identity management.* Ethics and Information Technology. Springer Netherlands 12(1), 43-55, 2010.
22. Windley, P.J. “Unmasking identity management architecture: digital identity”, O’Reilly, 2005.
23. Wood, P. Implementing identity management security-an ethical hacker’s view, *Network security*, 9, 12-15, 2005.
24. Windley, P. J. Understanding Digital Identity Management. Phillip J. Windley, ”Digital ID and eGovernment”Understanding Digital Identity Management”. Available on: http://www.windley.com/docs/Digital%20ID%20and%20eGovernment.pdf

25. Sullivan, C. Digital Identity: An Emergent Legal Concept. University of Adelaide Press, 2011.
26. Dehing, A.J.M., Baartman, L.K.G. and Jochems, W.M.G., (2011). Mechanisms of students' engineering identity development during workplace learning in the bachelor curriculum. *WEE2011, September 27-30,* 2011, Lisbon, Portugal. Retrieved from http://www.sefi.be/wp-content/papers2011/T7/99.pdf
27. Pfitzman, A. and Hansen, M. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, v0.34. 2010.
28. Hansenu, M., Pfitzmannb, A., and Steinbrecherb, S. Identity management throughout one's whole life. Information Security Technical Report, 13(2), 83–94, 2008.
29. Damiani, E., Vimercati, C.S. and Samarati, P. Managing multiple and dependable identities. *IEEE Internet Computing*, 7(6), 29–37, 2003. doi: 10.1109/MIC.2003.1250581
30. Afzal, M.T., Kulathuramaiyer, N. and Maurer, H. Creating Links into the Future. *Journal of Universal Computer Science,* 13(9), 1234-1245, 2007.
31. Goodstadt, L.F., Connolly, R. and Bannister, F. The Hong Kong e-Identity Card: Examining the Reasons for Its Success When Other Cards Continue to Struggle. *Information Systems Management*, 32(1), 72-80, 2015.
32. Danner, P. and Hein, D.A. Trusted Computing Identity Collation Protocol to Simplify Deployment of New Disaster Response Devices. *Journal of Universal Computer Science,* 16(9), 1139-1151, 2010.
33. Bosworth, K. Gonzalez, M. G. Jaweed S. and Wright, T. Entities, Identifiers and Credentials – what does it all mean? *Bt Technology Journal*, 23(4), 25-36, 2005.
34. Jøsang, A., AlZomai, M. and Suriadi, S. Usability and privacy in identity management architectures. In Proceding Fifth *Australasian Information Security Workshop: Privacy enhancing technologies (AISW 2007), Ballarat, Australia, 2007,* CRPIT, (vol. 68, pp. 143-152x). Australian Computer Society Inc., 2007.
35. Aresta, M., Pedro, L., Santos, C. and Moreira, A. Online identity analysis model. *International Journal of Knowledge Society Research*, 4(3), 89-102, 2013.

36. Guo, L., Zhang, C., F, Y. and Lin, P. A Privacy-Preserving Attribute-Based Reputation System in Online Social Networks. Journal of Computer Science and Technology 30(3), 578–597, 2015. doi: 10.1007/S11390-015-1547-9
37. Bertino, E. and Takahashi, K. Identity Management: Concepts, Technologies, and Systems, London, Artech House Inc, 2011.
38. Korać, D. and Simić, D. Digital Identity in Identity Management Models. Proceeding of the 2014 International Conference on ICT Conference and Exibition, Aranđelovac, InfoTech 2014.
39. Wang, N., Du, H., Xu, B. and Dai, G. Compact Indexes Based On Core Content In Personal Dataspace Management System. Computers & Informatics, 33, 281-302, 2014.
40. Volonino, L., Sipior, J.C. and Ward, B.T. Managing the Lifecycle of Electronically Stored Information. *Information Systems Management*, 24(3), 231-238, 2007.
41. Sabucedo, L.Á. and Rifón, L.Á. Managing Citizen Profiles in the Domain of e-Government: The cPortfolio Project. *Information Systems Management*, 27(4), 309-319, 2010.
42. Whitley, E.A., Gal, U. and Kjaergaard, A. Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, 23, 17–35, 2014.
43. Jøsang, A. and Pope, S. User centric identity management. *In AusCERT Asia Pacific Information Technology*, 1-13, 2005.
44. Koshutanski, H., Ion, M. and Telesca, L. Distributed Identity Management Model for Digital Ecosystems. *IEEE International Conference on Emerging Security Information, Systems and Technologies* (SecurWare 2007). *IEEE Computer Society*, 132-138, 2007.
45. Pfitzmann, A. and Pfitzmann, K.P. Lifelong Privacy: Privacy and Identity Management for Life. *Lifelong Privacy: Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology*, 320, 1-17, 2010.
46. Sullivan, C. Digital identity – The legal person? *Computer Law and Security Review*, 25(3), 227-236, 2009.
47. Capobianco, B.M., Diefes-Dux, H.A. and Habashi, M.M. Generating measures of engineering identity development among young learners. *39th IEEE Frontiers in Education Conference, 200*9, San Antonio, TX, IEEE, (pp. 1-6). IEEE, 2009.

48. Mcnair, L.D., Paretti, M.C. and Kakar, A. Case study of prior knowledge: expectations and identity constructions in interdisciplinary, cross-cultural virtual collaboration. *International Journal of Engineering Education, 24*(2), 386-399, 2008.
49. Koole, M. Identity and the itinerant online learner. *The International Review of Research in Open and Distributed Learning, 15*(6), 52-70, 2014.
50. Nesje, K., Canrinus, E.T. and Strype, J. "Trying on teaching for fit" – Development of professional identity among professionals with multiple career opportunities, Teaching and Teacher Education, Elsevier, 69, 131-141, 2018.
51. Gee, J.P. Identity as an analytic lens for research in education. *Review of Research in Education*, 25(1), 99-125, 2000.
52. Ibarra, H. Provisional selves: Experimenting with image and identity in professional adaptation. *Administrative Science Quarterly*, 44(4), 764-791, 1999.
53. Sheppard, S., Macatangay, K., Colby, A. and Sullivan, W. *Educating engineers, Design for the Future of the Field.* Stanford, CA: The Carnegie foundation for advancement of teaching, 2008.
54. Taylor, T.L. Intentional Bodies: Virtual Environments and the Designers Who Shape Them, *International Journal of Engineering Education*, 19(1), 25-34, 2003.
55. Paci, F., Bauer, D., Bertino, E., Blough.D., Squicciarini, A. and Gupta, A. Minimal credential disclosure in trust negotiations. Identity in the Information Society, 2009.
56. Jensen, J. Identity management Lifecycle – Exemplifying the need for holistic Identity assurance frameworks. Information and Communication technology. Springer, 7804, 343 – 352, 2013
57. Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP," IETF, RFC 2560, 1999.
58. Al-Khouri, A.M. and Bal, I. Digital Identities and Promise of the Tchnology Trio: PKI, Smart Cards, and Biometrics. Journal of Computers Science, 2007.
59. Shute, J. and User, I.D. A Novel of identity Theft. Mariner Books, 2006
60. Marcus, R. and Hasting, G. Identity Theft, inc. Disinformation Company, 2006.
61. Zalud, B. ID Theft tops fraud list again ABA Bank Compliance, 2, p. 5-6, 2003.

62. Department of Justice, Identity theft, 2015. Available on: http://www.pcworld.com/article/2986810/security/identity-theft-hit-7-of-us-population-last-year.html
63. Bureau of Justice Statistics, Identity theft, 2015. Available on: https://www.lifelockunlocked.com/hot-topics/17-6-million-experienced-identity-theft-last-year/
64. CIFAS, Identity theft, 2015. Available on: http://www.techworld.com/news/security/uk-identity-theft-affected-125000-people-last-year-says-cifas-3605383
65. Identity theft of business identity, 2015. Available on: https://www.yahoo.com/politics/opm-director-katherine-archuleta-quits-123735134636.html
66. Identity theft of personal information, 2015. Available on: http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888
67. Identity theft of user name and password, 2015. Available on: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0
68. FBI, Identity theft 2015. Available on: https://www.fbi.gov/about-us/investigate/cyber/identity_theft
69. Identity theft of personal information, 2015. Available on: www.redtape.nbcnews.co
70. Vacca, J.R. Computer and Information Security Handbook. Morgan Kaufmann Publishers is an imprint of Elsevier, Burlington, MA 01803, USA, 2009.
71. Prasad, G. and Rajbhandari, U. “Identity Management on a Shoestring”, 2011, Available on: http://www.infoq.com/min/books/Identity-Management-Shoestring.
72. Kent, S.T. and Millett, L.I. *Who Goes There? Authentication Through the Lens of Privacy*, The National Academies Press, Washington, D.C., 2003.
73. Korać, D. and Simić, D. A. Survey of Authentication Methods for Mobile Devices. Proceeding of the 2013 International Conference on ICT Conference and Exibition, Aranđelovac, InfoTech 2013.

74. Stewart, J.M., Tittel, E. and Chapple, M. CISSP: Certified Information Systems Security Professional Study Guide. Wiley publishing, Inc., Canada, 2008.
75. Wong, R., Berson, T. and Feiertag, R. *Polonius: an identity authentication system*, Proceedings of the 1985 IEEE Symposium on Security and Privacy, pp. 101-107, 1985. Available on: http://www.anagram.com/berson/abspolo.html
76. MeT: *Personal Transaction Protocol Version 1.0*, Draft Specification 01-11-2002, Mobile Electronic Transactions Ltd, 2002.
77. Palfrey, J. and Gasser, U. Digital Identity Ineroperability and eInnovation, case study Berkman Publication Series, 2007.
78. Alpár, G., Hoepman, J.H. and Siljee, J. The identity crisis. Security, privacy and usability issues in identity management. *Computer Research Repository (CoRR),* 2011.
79. Zwattendorfer, B., Stranacher, K. and Tauber, A. Towards a Federated Identity as a Service Model, *Technology-Enabled Innovation for Democracy, Government and Governance Lecture Notes in Computer Science,* 8061, 43-57, 2013.
80. Gopalakrishnan, A. Cloud Computing Identity Management. *SET Labs Briefings*, 7(7), 45-55, 2009.
81. Zwattendorfer, B., Zefferer, T. and Stranacher, K. An Overview of Cloud Identity Management-Models. *10th International Conference on Web Information Systems and Technologies (WEBIST),* pp. 82-92, 2014.
82. RFC 2693-SPKI Certification Theory - IETF, 1999. Available on: www.ietf.org/rfc/rfc2693.txt
83. Miyata, T., Koga, Y., Madsen, P., Adachi, S.I., Tsuchiya, Y., Sakamoto, Y. and Takahashi, K. "Asurvey on identity management protocols and standards" IEICE TRANS. INF and SYST 2006.
84. Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J. Design and evaluation of a shoulder-surfing resistant graphical password scheme. *In Proceedings of the working conference on advanced visual interfaces,* ACM pp. 177–184, 2006.
85. Hayday, G. Security nightmare: How do you maintain 21 different passwords. http://tinyurl.com/ silicon-security nightmare.
86. Yan, J., Blackwell, A., Anderson, R. and Grant, A. Password Memorability and Security: Empirical Results. *IEEE Security and Privacy*, 2004.

87. Bonneau, J. Measuring Password Reuse Empirically, February 2011.
88. Corella, F. and Lewison, K.A Comprehensive Approach to Cryptographic and Biometric Authentication from a Mobile Perspective. 2013. Available on: http://pomcor.com/whitepapers/CryptographicAuthentication.pdf
89. Monisha, G., Prabhu, B.B. and Kumar, B.B. Secured Android Mobile Authentication. *International Journal of Research in Engineering and Advanced Technology*, 1(1), 1-7, 2013.
90. Strong password generator 2018. Available on: https://strongpasswordgenerator.com/
91. 10 Most Popular Password Cracking Tools 2018. Available on: http://resources.infosecinstitute.com/10-popular-password-cracking-tools/
92. Clarke, N.L. and Furnell, S.M. Advanced user authentication for mobile devices. *Computers & Security* Elsevier, 26, 109-119, 2007.
93. Dunphy, P., Heiner, A.P. and Asokan, N. A closer look at recognition-based graphical passwords on mobile devices. *In: Proceedings of the 6th symposium on usable privacy and security*, pp. 26-38, 2010.
94. Zezschwitz, E.V., Koslow, A., Luca, A.D. and Hussmann, H. *Making Graphic-Based Authentication Secure against Smudge Attacks.* IUI13, March 19–22, pp.277-278, 2013.
95. Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition. vol. 3. Taylor and Francis Group, 2006.
96. Schneier, B. Biometrics: truths and fictions, Available on: http://www.schneier.com/crypto-gram-9808.html
97. Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. *Handbook of Fingerprint Recognition, cap.1*, New York, 2003.
98. Sheeba, T. and Bernard, M.J. *Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein.* International Journal of Computer Applications (0975 – 8887) volume 51, 2012.
99. Stockinger, T. *Implicit Authentication on Mobile Devices.* Media Informatics Advanced Seminar on Ubiquitous Computing, 2011.
100. Bayly, D., Castro, M., Arakala, A., Jeffers, J. and Horadam, K. Fractional biometrics: safeguarding privacy in biometric applications. *International Journal of Information Security,* Springer Heidelberg, 9, 69-82, 2010. doi: 10.1007/s10207-009-0096-z

101. Damousis, I., Tzovaras, D. and Bekiaris, E. *Unobtrusive multimodal biometric authentication: The humabio project concept.* EURASIP journal on advances in signal processing, 1–11, 2008.

102. Clarke, N., Furnell, S. and Reynolds, P. Biometric authentication for mobile devices. In: *Proceedings of the 3rd Australian Information warfare and security conference*, pp. 61- 69, 2002.

103. Furnell, S., Clarke, N. and Karatzouni, S. Beyond the PIN: Enhancing user authentication for mobile devices. *Computer Fraud and Security*, Elsevier, 12-17, 2008.

104. Tao, Q. and Veldhuis, R. *Biometric Authentification System on Mobile Personal Devices.* IEEE transaction on instrumentation and measurement, 59(4), 2010.

105. Wayman, J., Jain, A., Maltoni, D. and Maio, D. Introduction to Biometric Authentication Systems, Chapter, *Biometric Systems,* Springer London, pp. 1-20, 2005. doi: 10.1007/1-84628-064-8_1

106. Tulyakov, S. Farooq, F., Mansukhani, P. and Govindaraju, V. *Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters,* 28(16), 2427–2436, 2007.

107. Adibi, S. A low overhead scaled equalized harmonic-based voice authentication system. Telematics and Informatics: An Interdisciplinary Journal on the Social Impacts of New Technologies, 31(1), 137-152, 2014.

108. Crawford, H., Renaud, K. and Storer, T. A framework for continuous, transparent mobile device authentication. *Computers & Security,* Elsevier, 39, 127-136, 2013.

109. Iwano, K., Hirose, T., Kamibayashi, E. and Furui, S. Audio-visual person authentication using Speech and Ear images. In: *Proceedings of workshop on multimodal user authentication*, 85-90, 2003.

110. Woo, R.H., Parkm, A. and Hazen, T.J. The MIT mobile device speaker verification corpus: data collection and preliminary experiments. In: *IEEE workshop on speaker and language recognition*, pp. 1-6, 2006.

111. Brunelli, R. and Falavigna, D. Person identification using multiple cues. *IEEE Transactions on pattern analysis and machine intelligence*, 17, 955-966, 1995.

112. Bodei, C., Degano, P., Focardi, R. and Priami, C. Authentication via localized names, in: *Proc. CSFW'99, New York,* IEEE Press, pp. 98–110, 1999.

113. Bowyer, K.W., Baker, S.E., Hentz, A, Hollingsworth, K., Peters, T. and Flynn, P.J. Factors that degrade the match distribution in iris biometrics. *Identity in the Information Society*, 2, 327-343, 2009.
114. Wildes, R.P. Iris recognition: An emerging biometric technology, Proceedings of the IEEE, 85, pp. 1348-1363, 1997.
115. Monrose, F. and Rubin, A. "Authentication via Keystroke Dynamics", *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 48-56, 1997.
116. Clarke, N.L. and Furnell, S.M. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security,* Springer Heidelberg, 6, 1-14, 2007.
117. Kambourakis, G., Damopoulos, D., Papamartzivanos, D. and Pavlidakis, M. Introducing Touchstroke: Keystroke-based Authentication System for Smartphones. *Security and Communication Networks*, Wiley Online Library, 5, 3-14, 2014.
118. Yu, E. and Cho, S. Keystroke dynamics identity verification-its problems and practical solutions. *Computers & Security,* Elsevier, 23, 428-440, 2004.
119. Buchoux, A. and Clarke, N. Deployment of keystroke analysis on a smartphone. In: *Proceedings of the 6th Australian information security management conference*, pp. 40-47, 2008.
120. Saevanee, H. and Bhattarakosol, P. Authenticating user using keystroke dynamics and finger pressure. In: *Proceedings of the 6th IEEE consumer communications and networking conference*, pp. 1-2, 2009.
121. Maiorana, E., Campisi, P., Carballo, N.G. and Neri, A. Keystroke Dynamics Authentication for Mobile Phones. SAC '11 *Proceedings of the 2011 ACM Symposium on Applied Computing*, pp. 21-26, 2011.
122. Monrose, F. and Rubin, A.D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems,* Elsevier, 16, 351–359, 2000.
123. Incel, O.D., Kose, M. and Ersoy, C. A Review and Taxonomy of Activity Recognition on Mobile Phones. BioNanoScience, 3(2), 145-171, 2013.
124. Ailisto, H.J., Lindholm, M., Mantyjarvi, J., Vildjiounaite, E. and Makela, S.M. Identifying people from gait pattern with accelerometers. In*: Proceedings of the SPIE 5779, Biometric Technology for Human Identification II*, Orlando 7, pp. 7–14, 2005.

125. Gafurov, D., Helkala, K. and Soendrol, T. Gait recognition using acceleration from mems. In: *The first international conference on availability, reliability and security*. IEEE 2006.

126. Bujari, A., Licar, B. and Palazzi, C.E. Movement pattern recognition through smartphone's accelerometer. In: *Consumer communications and networking conference (CCNC),* IEEE, pp. 502-506, 2012.

127. Derawi, M. and Bours, P. Gait and activity recognition using commercial phones. *Computers & Security*, Elsevier, 39, 137-144, 2013.

128. Frank, J., Mannor, S. and Precup, D. Activity and gait recognition with time-delay embeddings. In: *Proceedings of the twenty-fourth AAAI conference on artificial intelligence*, pp. 1-6, 2010.

129. He, Z. and Jin, L. Activity recognition from acceleration data based on discrete consine transform and SVM. In: *IEEE international conference on systems, man and cybernetics*, pp. 5041 – 5044, 2009.

130. Kwapisz, J.R., Weiss, G.M. and Moore, S.A. Activity recognition using cell phone accelerometers. *SIGKDD Explorations Newsletter,* 12, pp. 74-82, 2010.

131. Liu, Z, and Sarkar, S. Improved gait recognition by gait dynamics normalization. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28, 863–876, 2006.

132. Han, J. and Bhanu, B. Individual recognition using gait energy image. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28, 316–322, 2006.

133. Derawi, M., Nickel, C., Bours, P. and Busch, C. Unobtrusive user authentication on mobile phones using biometric gait recognition. *In: Sixth international conference on intelligent information hiding and multimedia signal processing 2010*, IEEE Computer Society Washington, DC, USA, pp. 306-311, 2010.

134. Gafurov, D, Snekkenes, E. and Bours, P. Gait authentication and identification using wearable accelerometer sensor. *In 2007 IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 220–225, 2007.

135. Cappelli, R., Ferrara, M., Franco, A. and Maltoni, D. Fingerprint verification competition 2006. *Biometric Technology Today*, 15, 7-9, 2007.

136. Mjaaland, B.B., Bours, P. and Gligoroski, D. Walk the walk: attacking gait biometrics by imitation. In: *Proceedings of the 13th international conference on information*

security, pp. 361-380, 2011.

137. Korać, D. Comparison of Information Security Models. *Info M*, FON, 56(4), 17-24, 2015.
138. Alharby, N. E-government Security: Explaing Main Factors and Analysing Existing Models. World Academy of Science, Engineering and Technology International Journal of Social, Human Science and Engineering 7(9), pp. 1319-1321, 2013.
139. Bell, D.E. and La Padula, L. Secure Computer Systems: Unified Exposition and Multics Interpretation. ESD-TR-75-306, MITRE MTR-2997, MITRE Corporation, 1976.
140. Braghin, C., Sharygina, N. and Barone-Adesi, K. A Model Checking-based Approach for Security Policy Verification of Mobile Systems. *Formal Aspects of Computing*, 23(5), 627-648, 2010.
141. Krause, M. and Tipton, H.F. Handbook of Information Security Management, fifth edition, vol.2, Taylor & Francis Group, 2005.
142. Stamp, M. Information Security Principles and practice. John Wiley & Sons, Inc., Hoboken, New Jersey. 2006.
143. Biba, K.J. Integrity constraints for secure computer systems. Technical Report EST TR-76-372, Hanscom AFB, 1977.
144. Bishop, M. Computer Security: Art and Science, Addison Wesley, Boston, MA. 2003.
145. Balon, I. and Thabet, I. Biba security model comparison. CIS 576, 2004.
146. Sandhu, R.S. and Mason, G. Lattice-based Access Control Models. IEEE, pp. 9-19, 1993.
147. Lipner, S.B. Non-discrentionary controls for commercial applications. In IEEE Symposium on Security and Privacy, pp. 2-10, Oakland, 1982.
148. Lipton, R. J. and Snyder, L. A linear time algorithm for deciding subject security. Journal of the ACM, 24(3), 455-464, 1977.
149. Bishop, M. “Hierarchical Take-Grant Protection System” Proceedings of the eighth ACM symposium on Operating systems principles. Pacific Grove, California, pp. 109-122, 1981.

150. Landwehr, C. “Formal Models for Computer Security”, Computing Surveys, 13(3), 1981.

151. Castano, S., Fugini, M., Martella, G. and Samarati, P. Database Security, Addison Wesley, Harlow, England, 1995.

152. Therialut, M., and Newman, A. Oracle Security Handbook: Implementing a Sound Security-Plan in Your Oracle Environment. McGraw-Hill, Berkeley, CA. 2001.

153. Clark, D.D. and Wilson, D.R. A comparison of commercial and military computer security policies. In IEEE Symposium on Security and Privacy, Oakland, pp. 184-194, 1987.

154. Anderson, M., Montague, P. and Long, B. A Formal Integrity Framework with Application to a Secure Information ATM (SIATM). DSTO Defence Science and Technology Organisation. Commonwealth of Australia 2012.

155. Qingguang, J., Sihan, Q. and Yeping, H. A formal model for integrity protection based on DTE technique, Science in China Series F: Information Sciences 49, pp. 545-565, 2006.

156. Fuglerud, K.S. and Røssvoll, T.H. An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, Springer Heidelberg, 11, 359-373, 2012. doi: 10.1007/s10209-011-0253-9.

157. Grudin, J. Utility and usability: research issues and development contexts. *Interact. Comput*. Elsevier, 4, 209-217, 1992.

158. Kartakis, S. and Stephanidis, C.A. Design-and-play approach to accessible user interface development in ambient intelligence environments. *Computers in Industry*, Elsevier, 61, 318-328, 2010.

159. MollahaMd., M.B., Azada A.K. and Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, Elsevier, 84, 38-54, 2017.

160. Shena, W., Yanga, G., Yu, J., Zhanga, H., Kongd, F. and Hao, R. Remote data possession checking with privacy-preserving authenticators for cloud storage, Future Generation Computer Systems, Elsevier 76, 136-145, 2017.

161. Nanz, S. and Hankin, C. A framework for security analysis of mobile wireless networks. *Theoretical Computer Science*, Elsevier, 367, 203-227, 2006.

162. Pribeanu, C., Neszly, P.F. and Patru A. Municipal web sites accessibility and usability for blind users: preliminary results from a pilot study. *Universal Access in the Information Society*. Springer Heidelberg, 13, 339-349, 2014. doi: 10.1007/s10209-013-0315-2.

163. Vapen, A. and Shahmehri, N. Security levels for Web Authentication using Mobile Phones. *Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology*, Springer Heidelberg, 352, pp. 130-143, 2011. doi: 10.1007/978-3-642-20769-3_11.

164. Burr, W.E., Dodson, D.F. and Polk, W.T. Electronic authentication guideline. *Technical Report 800-63, National Institute of Standards and Technology*, 2008.http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Accessed 15 May 2017.

165. O'Gorman, L.: Comparing passwords, Tokens, and Biometric for User Authentication", In Proc. of IEEE, 91, pp. 2019-2040, 2003.

166. Helkala, K. and Snekkenes, E. A Method for Ranking Authentication Products. Proceedings of the Second International Symposium on Human Aspects of Information Security and Assurance, HAISA, 2008.

167. Pond, R., Podd, J., Bunnell, J. and Henderson, R. Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates, *Computers & Security*, 19, 645-656, 2000.

168. Abott, J. Smart cards: How secure are they. www.sans.org/reading_room/whitepapers/authentication/131.php, 2003. (Accessed 30 may 2017).

169. Husemann, D. The smart card: don't leave home without it, IEEE Concurrency, 7, pp 24-27, 1999.

170. Maio, D., Maltoni, D., Cappelli, R., Wayman J. and Jain, A. FVC2000: Fingerprint Verification Competition, Trans. on pattern analysis and machine int., 24, pp. 402-412, 2002.

171. Phillips, P.J., Moon, H., Rizvi, S.A. and Rauss, P.J. The FERET Evaluation Methodology for Face-Recognition algorithms, Trans. on pattern analysis and machine intelligence, 22, 1090-1104, 2000.

172. Mansfield, A. and Wayman, J. Best practices in Testing and Reporting Performance

of Biometric Devices, NPL Report CMSC 14/02, Version 2.01., 2002.

173. Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. Handbook of Fingerprint Recognition. Second Edition, Springer Verlag, London, Limited, 2009.

174. Karovaliya, M., Karedia, S., Oza, S. and Kalbande, D.R. Enhanced security for ATM machine with OTP and Facial recognition features. Procedia Computer Science, 45, 390-396, 2015.

175. Renaud, K. Quantifying the quality of web authentication mechanisms: A usability perspective, J. Web Eng. 3(2), 95–123, 2004.

176. Bonneau, J., Herley, C., Oorschot, P.C. and Stajano, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes.2012 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 553-567, 2012.

177. Mihajlov, M., Jerman-Blazic, B. and Josimovski, S. A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives, in: 2011 5th International Conference on Network and System Security, NSS, pp. 332–336, 2011.

178. Mihajlov, M., Blazic, B., Josimovski, S. Quantifying usability and security in authentication, in: 2011 IEEE 35th Annual Computer Software and Applications Conference, COMPSAC, pp. 626–629, 2011.

179. FIDO standard 2018. Available on: https://fidoalliance.org/aetna-deploys-fido-authentication/

180. Sabzevar, A.P. and Stavrou A. Universal Multi-Factor Authentication Using Graphical Passwords. International Conference on Signal Image Technology and Internet Based Systems, IEEE, pp. 625 – 632, 2008.

181. Zhou, L., Kang, Y., Zhang, D. and Lai, J. Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones, Decision Support Systems, 2016. DOI:10.1016/j.dss.2016.09.007

182. Memon, I., Mohammed, M.R., Akhtar, R., Memon, H., Memon, M.H. and Shaikh, R.A., Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC). *Wireless Personal Communications*, Springer US, 79, 661-686, 2014. doi: 10.1007/s11277-014-1879-8.

183. ISO 9241. *Ergonomics Requirements for Office Work with Visual Display Terminals (VDTs) International Standards Organisation,* Geneva, 1997.

184. Nielsen, J. Usability engineering. *Morgan Kaufmann Pub*., 1994.

185. Harrison, R., Flood, D. and Duce, D. Usability of mobile applications. Literature review and rationale for a new usability model Wireless. *Journal of Interaction Science*, Springer, 1-16, 2013. doi: 10.1186/2194-0827-1-1.

186. Bevan, N. Classifying and selecting UX and usability measures. *In the Proceedings of Meaningful Measures: Valid Useful User Experience Measurement (VUUM), 5th COST294-MAUSE Open Workshop*, Reykjavik, Iceland, 2008.

187. Miao, M., Pham, H.A., Friebe, J. and Weber, G. Contrasting usability evaluation methods with blind users. *Universal Access in the Information Society*, Springer Heidelberg, 2014. doi: 10.1007/s10209-014-0378-8.

188. Parhi, P., Karlson, A.K. and Bederson, B.B. Target size study for one-handed thumb use on small touch screen devices. *In: Proceedings of the 8th Conference on Human–Computer Interaction with Mobile Devices and Services*, New York, NY, USA, MobileHCI' 06, ACM, pp. 203-210, 2006.

189. Zhou, J., Rau, P.L.P. and Salvendy, G. Age-related difference in the use of mobile phones. *Universal Access in the Information Society*, Springer Heidelberg, 13, 401-413, 2014. doi: 10.1007/s10209-013-0324-1.

190. Bevan, N. European Usability Support Centres: Support for a More Usable Information Society. *Proceedings of TAP Annual Concertation Meeting*, Barcelona, 1998.

191. Bevan, N. Claridge, N. and Petrie, H. Tenuta: simplified guidance for usability and accessibility. *In: Proceedings of HCI International 2005*, Las Vegas, 2005.

192. Weir, C.S., Douglas, G., Carruthers, M. and Jack, M. User perceptions of security, convenience and usability for eBanking authentication tokens. *Computers & Security*, Elsevier, 28, 47-62, 2009.

193. Weir, C.S., Douglas, G., Richardson, T. and Jack, M. "Usable security: user preferences for authentication methods in eBanking and the effects of experience." *Computers & Security,* Elsevier, 22, 153-164, 2010.

194. Thatcher, J., Waddell, C.D., Henry, S.L., Swierenga, S., Urban, M.D., Burks, M.,

Regan, B. and Bohman, P. *Constructing Accessible Web Sites*. Glasshaus, San Francisco, 2003.

195. Galvez, R.A. and Youngblood, N.E. e-Government in Rhode Island: what effects do templates have on usability, accessibility, and mobile readiness? *Universal Access in the Information Society*, Springer, Heidelberg 2014. doi: 10.1007/s10209-014-0384-x.
196. Calvo, R., Iglesias, A. and Moreno, L. Accessibility barriers for users of screen readers in the Moodle learning content management system. *Universal Access in the Information Society*, Springer Heidelberg, 13, 315-327, 2014.
197. Emiliani, P.L. and Stephanidis, C. *Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities,* IBM Sys, 44, 2005.
198. Gajos, K.Z., Wobbrock, J.O. and Weld, D.S. Automatically generating user interfaces adapted to users' motor and vision capabilities. In: *UIST'07: Proceedings of the 20th Annual ACM Symposium on User Interface Software and Technology,* ACM, New York, pp. 231–240, 2007.
199. Stephanidis, C. and Savidis, A. Universal access in the information society: methods, tools and interaction technologies. *Universal Access in the Information Society*, Springer Heidelberg, 1, 40-55, 2001.
200. Shaikh, A. and Karjaluoto, H. Mobile banking adoption: A literature review. *Telematics and Informatics*, Elsevier, 32, 129-142, 2015.
201. Friedewald, M.,Vildjiounaite, E.,Punie, Y. and Wright, D. Privacy, Identity and Security in Ambient Intelligence: a Scenario Analysis. *Telematics and Informatics*; Elsevier, 24, 15-29, 2007.
202. Baseri, Y., Hafid, A. and Cherkaoui, S. Privacy preserving fine-grained location-based access control for mobile cloud, *Computers & Security*, Elsevier, 73, 249-265, 2018.
203. Ntalkos, L., Kambourakis, G. and Damopoulos, D. Let's Meet! A participatory-based discovery and rendezvous mobile marketing framework, *Telematics and Informatics*, Elsevier, 32, 539-563, 2015.
204. Bettini, C. and Riboni, D. Privacy Protection in Pervasive Systems: State of the Art and Technical Challenges. *Pervasive and Mobile Computing*; Elsevier, 17, 159-174.

2015.

205. Veeningen, M., Weger, B. and Zannone, N. *Data minimisation in Communication protocols: A Formal Privacy Analysis of Identity Management Systems*. International Journal of Information Security, Springer Verlag, 1-52, 2013

206. Jiang, L., Jiang, N. and Liu, S. Consumer Perceptions of E-Service Convenience: An Exploratory Study. Procedia Environmental Sciences, 11, 406-410, 2011.

207. Dabholkar, P.A., Bobbitt, L.M. and Lee, E.J. Understanding consumer motivation and behavior related to self-scanning in retailing: implications for strategy and research on technology-based self-service, International Journal of Service Industry Management, 14(1), 59-95, 2003.

208. Fournier-Bonilla, S.D., Watson, K., Malaveâ, C. and Froyd, J. Managing Curricula Change in Engineering at Texas A & M University, *International Journal of Engineering Education*, 17(3), 222-235, 2001.

209. OWASP Risk Rating Methodology, 2018. Available on: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

210. Ogbanufe, O. and Kim, D.J. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decision Support Systems, 2017. https://doi.org/10.1016/j.dss.2017.11.003

211. Korać, D. A Comprehensive Overview and Comparison of Contemporary User Authentication Methods for Mobile Devices. *Info M*, FON, 53(2), 48-54, 2015.

212. Mamdani, E. and Assilian, S. An Experiment in Linguistic Synthesis with a Fuzzy Logic Controller. *International Journal of Man-Machine Studies*, 7(1), 1-13, 1975.

213. Mount, C. and Liao, T.W. Prototype of an intelligent failure analysis system, in Proceedings of the 4th International Conference on Case-Based Reasoning (ICCBR ’01), Vancouver, BC, Canada, pp. 716– 731, 2001.

214. Monrose, F., Reiter, M.K. and Wetzel, S. Password hardening based on keystroke dynamics. *International Journal of Information Security*, Springer Verlag, 1(2), 69–83, 2001.

215. Gunson, N., Marshall, D., Morton, H. and Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4), 208–220, 2011.

216. Go, W., Lee, K. and Kwak, J. Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal Intelligent. Manufacturing*, 25, 217–230, 2014.

217. Cha, B.R., Kim, Y.I. and Kim, W.J. Design of new P2P-enabled Mobile-OTP system using fingerprint features. *Telecommunication Systems*, 52(4), 2221-2236, 2013.

218. Tresadern, P., Cootes, T.F., Poh, N., Matejka, P., Hadid, A., Levy, C., McCool, C. and Marcel, S. Mobile biometrics: combined face and voice verification for a mobile platform, IEEE Pervasive Computation, 12(1), 79-87, 2013.

219. Kang, J., Nyang, D.H. and Lee, K.H. Two-factor face authentication using matrix permutation transformation and a user password, Information Sciences, 269, 1-20, 2014.

220. DeMarsico, M.,Galdi, C.,Nappi, M. and Riccio, D. FIRME: face and iris recognition for mobile engagement, Image and Vision Computing, 32(12), 1161-1172, 2014.

221. Cha, B.R., Kim, Y.I. and Kim, J.W. Design of new P2P-enabled Mobile-OTP system using fingerprint features. *Telecommunication Systems*, 52(4), 2221-2236, 2013.

222. Al-Khouri, A.M. *Identity and Mobility in a Digital World.* Technology and Investment, 7-12, 2013.

223. Arias-Cabarcos, P., Almenárez-Mendoza, F., Marin-López, A., Diaz-Sánchez, D. and Sánchez-Guerrero, R. A Metric-Based Approach to Assess Risk for ‘‘On Cloud’’ Federated Identity Management. *Journal of Network and Systems Management*, Springer US, 20(4), 513-533, 2012.

X PRILOG – PROGRAMSKI KOD ZA ALGORITAM 1 I ALGORITAM 2

Programski kod za Algoritam 1

Algoritam 1 Proces održavanja u životnom ciklusa digitalnih identiteta

```
create or replace procedure algoritam_IsIdentityActive (v_broj_dozvoljenih pokusaja integer /*Parametar
                kojim definisemo broj pokusaja za izvrsenje CVORA IsIdentityActive, tj. broj iteracija petlje*/,
tf out boolean /*parametar koji sluzi kao informacija da li se desila neka greska u proceduri, ili je izvrsena
                                                                                    do kraja*/,
                                                odgovor out varchar2 /*opis rezultata izvrsavanja procedure*/) is
/*Napomena: kod je pisan u Oracle proceduralnom jeziku: PL/SQL. Kod obuhvata samo simulaciju petlje
                                                                                    za cvor IsIdentityActive*/
 rezultat_izvrsavanja boolean;  -- parametar koji sluzi za rezultat izvrsavanje poziva procedure za CVOR1
     rezultat_attribute boolean;  -- parametar koji sluzi za rezultat izvrsavanje poziva procedure za CVOR2
       rezultat_service boolean;  -- parametar koji sluzi za rezultat izvrsavanje poziva procedure za CVOR3
         rezultat_serviceSimple boolean; -- parametar koji sluzi za rezultat izvrsavanje poziva procedure za
                                                                                    CVOR4
           --Ugnjezdena procedura u koju su samo izdvojeni koraci nakon CVORA2 jer su identicni, osim
                                                                                    AttributeProofing();
                                                                procedure koraci_OdCredentialIssuance is
begin
    /*Napomena: svaki poziv ove fiktivne procedure treba da ima neku logiku koda u pozadini koja nije
predmet u ovom primjeru algoritma*/
    CredentialIssuance();
    DigitalIdentityFormation();
    Propagation();
    --Dodavanje u Repository
    AddRepository();
    Entity();
    --CVOR3 "Is Service or SSO Reuse"
    rezultat_service:=false;
    rezultat_service:=IsServiceOrSSOReuse();
    if rezultat_service=true then
       IdentityFiltering();
       IdentityChoosing();
          --Dodavanje u Repository nakon koraka Identity Choosing
       AddRepository2();
    else
       --CVOR4 "Is Service Simple Use" - ovaj cvor takodje prouzrokuje izlazak iz petlje i ne ponavljanje
vise ovog koraka
       v_broj_dozvoljenih:=0;
       rezultat_serviceSimple:=false;
       rezultat_serviceSimple:=IsServiceSimpleUse();
       /*ovdje sada treba da ide kod za nastavak dijagrama*/
    end if;
  end;
 end koraci_OdCredentialIssuance;
begin
  tf:=false;
 --ovdje sam predvidio da kao ulaz dobijem broj dozvoljenih pokusaja uspjesnosti koji mora biti veci od
0
 if v_broj_dozvoljenih<0 then
    odgovor:='GRESKA: broj dozvoljenih pokusaja mora biti veci od 0!';
    raise_application_error(-20000, odgovor);
    return;
```

```
  end if;
  loop
    --u slucaju da se pozove procedura bez ijedne iteracije da u tom slucaju izadje iz petlje odmah
    if v_broj_dozvoljenih=0 then
      exit;
    end if;
    rezultat_izvrsavanja:=false;
    --CVOR1 poziv funkcije
    rezultat_izvrsavanja:=IsIdentityActive();
    --ako je rezultat uspjesan prelazi se na fazu SPAssertionAcquisition
    if rezultat_izvrsavanja=true then
      --Nakon ovoga petlja se odmah zavrsava i prelazi se u nastavak dijagrama
      v_broj_dozvoljenih:=0;
      SPAssertionAcquisition();
      /*ovdje sada treba da ide kod za nastavak dijagrama*/
     else
      /*Ako rezultat izvrsavanja IsIdentityActive nije uspjesan  rade se ponovljeni koraci izbora atributa
sledecim redosledom kao u dijagramu toka (simulirano su pozivi funkcija):*/
      AttributeChoosing();
      --CVOR2 "Is AttributeRequested from Subject"
      rezultat_attribute:=false;
      rezultat_attribute:=IsAtributeRequestedFromSubject();
      if rezultat_attribute=true then
        koraci_OdCredentialIssuance();
      else
        AttributeProofing();
        koraci_OdCredentialIssuance();
      end if;
    end if;
   --U slucaju ad je uspjesno zavrsen upit i da se otislo na sledeci korak SPAssertionAcquisition, onda je
potrebno izaci iz petlje
   exit when v_broj_dozvoljenih=0;
   --Umanjenje za jedan prolaz
   v_broj_dozvoljenih:=v_broj_dozvoljenih-1;
  end loop;
  odgovor:='Uspjesno zavrsena simulacija rada procedure!';
  tf:=true;
exception when others then
  odgovor:='GRESKA prilikom izvrsavanje procedure IsIdentityActive: '||sqlerrml;
  raise_application_error(-20000, odgovor);
end algoritam_IsIdentityActive;
```

Programski kod za Algoritam 2

Algoritam 2 Numerička procjena mobilnih autentifikacionih metoda u *Fishbone* modelu

```
clear all;
close all;
clc;

a=newfis('sistem');

%% Unosenje prve varijable, odnosno Security (0, ,1)
a = addvar(a,'input','Security',[0 1]);
a=addmf(a,'input',1,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',1,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',1,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',1,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',1,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',1,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',1,'Very Very High','gaussmf',[0.07078 1]);

%% Unosenje druge varijable, odnosno Usability (0, ,1)
a = addvar(a,'input','Usability',[0 1]);
a=addmf(a,'input',2,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',2,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',2,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',2,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',2,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',2,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',2,'Very Very High','gaussmf',[0.07078 1]);

%% Unosenje trece varijable, odnosno Accessibility (0, ,1)
a = addvar(a,'input','Accessibility',[0 1]);
a=addmf(a,'input',3,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',3,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',3,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',3,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',3,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',3,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',3,'Very Very High','gaussmf',[0.07078 1]);

%% Unosenje cetvrte varijable, odnosno Pricing (0, ,1)
a = addvar(a,'input','Pricing',[0 1]);
a=addmf(a,'input',4,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',4,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',4,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',4,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',4,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',4,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',4,'Very Very High','gaussmf',[0.07078 1]);

%% Unosenje pete varijable, odnosno Complexity (0, ,1)
a = addvar(a,'input','Complexity',[0 1]);
a=addmf(a,'input',5,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',5,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',5,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',5,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',5,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',5,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',5,'Very Very High','gaussmf',[0.07078 1]);
```

```
%% Unosenje seste varijable, odnosno Privacy (0, ,1)
a = addvar(a,'input','Privacy',[0 1]);
a=addmf(a,'input',6,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',6,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',6,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',6,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',6,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',6,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',6,'Very Very High','gaussmf',[0.07078 1]);

%% Unosenje sedme varijable, odnosno Convenience (0, ,1)
a = addvar(a,'input','Convenience',[0 1]);
a=addmf(a,'input',7,'Very Very Low','gaussmf', [0.07078 0]);
a=addmf(a,'input',7,'Very Low','gaussmf', [0.07078 0.1667]);
a=addmf(a,'input',7,'Low','gaussmf', [0.07078 0.3333]);
a=addmf(a,'input',7,'Medium','gaussmf',[0.07078 0.5]);
a=addmf(a,'input',7,' High','gaussmf', [0.07078 0.6667]);
a=addmf(a,'input',7,'Very High','gaussmf', [0.07078 0.8333]);
a=addmf(a,'input',7,'Very Very High','gaussmf',[0.07078 1]);

% Unosenje izlaza, odnosno ocjena metoda
a=addvar(a,'output','Evaluation',[0 10]);
a=addmf(a,'output',1,'K','gaussmf',[0.45 0]);
a=addmf(a,'output',1,'J','gaussmf',[0.45 1]);
a=addmf(a,'output',1,'I','gaussmf',[0.45 2]);
a=addmf(a,'output',1,'H','gaussmf',[0.45 3]);
a=addmf(a,'output',1,'G','gaussmf',[0.45 4]);
a=addmf(a,'output',1,'F','gaussmf',[0.45 5]);
a=addmf(a,'output',1,'E','gaussmf',[0.45 6]);
a=addmf(a,'output',1,'D','gaussmf',[0.45 7]);
a=addmf(a,'output',1,'C','gaussmf',[0.45 8]);
a=addmf(a,'output',1,'B','gaussmf',[0.45 9]);
a=addmf(a,'output',1,'A','gaussmf',[0.45 10]);


%% Dodavanje pravila
ruleList=[ ...
7 7 7 1 1 7 7 11 1 1
7 7 7 1 2 7 7 11 1 1
7 7 7 1 3 7 7 11 1 1
7 7 7 1 4 7 7 11 1 1
7 7 7 1 5 7 7 11 1 1
7 7 7 1 6 7 7 11 1 1
7 7 7 1 7 7 7 11 1 1
7 7 6 3 4 6 7 11 1 1
7 6 6 3 5 6 6 11 1 1
7 5 6 3 6 6 6 11 1 1
7 2 6 3 2 6 6 10 1 1
7 2 6 3 3 6 6 10 1 1
7 2 6 4 2 6 7 10 1 1
7 1 1 7 7 1 7 10 1 1
7 1 6 4 4 6 7 10 1 1
7 1 6 4 5 6 7 10 1 1
7 1 6 4 6 6 7 10 1 1
7 1 1 7 7 1 6 10 1 1
7 1 5 2 3 6 6 10 1 1
7 2 2 6 6 1 7 10 1 1
6 2 2 6 6 1 7 9 1 1
6 2 2 6 2 2 7 9 1 1
6 4 5 5 2 6 6 9 1 1
6 4 4 3 2 2 6 9 1 1
6 4 4 3 3 3 6 9 1 1
```

6 3 5 7 3 6 5 9 1 1
6 3 3 4 3 2 6 9 1 1
6 3 3 4 3 2 6 9 1 1
6 4 4 3 4 2 7 9 1 1
6 4 4 2 2 1 7 9 1 1
6 4 4 2 3 1 7 8 1 1
6 1 2 6 6 1 7 8 1 1
6 1 3 4 3 2 7 8 1 1
6 1 2 4 4 2 7 8 1 1
6 1 2 4 5 2 7 8 1 1
6 1 3 5 6 4 7 8 1 1
6 1 4 5 7 3 6 8 1 1
6 1 4 6 5 3 6 8 1 1
6 1 4 5 3 3 6 8 1 1
6 1 3 4 3 3 6 8 1 1
5 4 3 5 3 3 5 7 1 1
5 4 4 6 4 3 5 7 1 1
5 4 2 5 5 3 5 7 1 1
5 4 2 4 6 3 5 7 1 1
5 4 3 5 7 2 5 7 1 1
5 4 4 4 3 2 5 7 1 1
5 3 3 5 5 4 5 7 1 1
5 3 5 4 3 2 5 7 1 1
5 3 6 4 2 2 5 7 1 1
5 3 6 2 6 2 5 7 1 1
4 6 4 6 6 2 5 6 1 1
4 6 4 3 3 2 5 6 1 1
4 6 4 2 4 2 5 6 1 1
4 6 4 3 5 2 5 6 1 1
4 5 4 5 6 4 4 6 1 1
4 4 4 3 2 4 4 6 1 1
4 4 4 3 3 4 4 6 1 1
4 4 4 3 4 4 4 6 1 1
4 3 4 4 5 4 4 6 1 1
4 3 4 5 6 4 4 6 1 1
3 7 4 4 3 4 4 5 1 1
3 7 4 4 4 4 3 5 1 1
3 6 4 4 5 4 3 5 1 1
3 5 4 4 6 4 3 5 1 1
3 5 5 4 7 5 3 5 1 1
3 5 5 4 4 5 3 5 1 1
3 5 5 4 3 5 2 5 1 1
3 5 5 3 2 5 1 5 1 1
3 5 4 2 3 5 7 5 1 1
3 5 4 2 2 5 6 5 1 1
2 7 4 3 6 5 6 4 1 1
2 7 4 3 3 5 7 4 1 1
2 7 4 4 4 7 7 4 1 1
2 7 4 3 5 7 7 4 1 1
2 7 4 3 6 6 7 4 1 1
2 7 4 2 7 6 7 4 1 1
2 7 4 1 1 5 1 4 1 1
2 7 4 7 7 5 1 4 1 1
2 7 4 6 6 4 1 4 1 1
2 7 4 5 5 3 1 4 1 1
2 6 6 3 5 6 2 3 1 1
2 6 6 3 3 6 2 3 1 1
2 6 6 3 3 5 2 3 1 1
2 6 6 3 4 5 1 3 1 1
2 6 6 3 5 6 7 3 1 1
2 5 6 4 6 6 7 3 1 1
2 5 6 5 7 6 7 3 1 1
2 3 6 5 1 2 6 3 1 1

```
2 3 6 6 1 6 7 3 1 1
2 3 6 7 2 7 7 3 1 1
1 7 6 7 3 7 1 2 1 1
1 7 6 7 4 7 1 2 1 1
1 7 6 2 5 7 1 2 1 1
1 7 6 2 6 7 1 2 1 1
1 7 7 2 7 7 1 2 1 1
1 7 7 1 1 7 1 2 1 1
1 7 7 1 3 7 1 2 1 1
1 7 7 1 4 7 1 2 1 1
1 7 1 1 5 7 1 2 1 1
1 7 1 1 1 1 1 2 1 1
1 1 2 6 5 1 1 1 1 1
1 1 2 6 6 1 1 1 1 1
1 1 2 6 7 1 1 1 1 1
1 1 1 7 1 1 1 1 1 1
1 1 2 7 2 1 1 1 1 1
1 1 1 7 3 1 1 1 1 1
1 1 1 7 4 1 1 1 1 1
1 1 1 7 5 1 1 1 1 1
1 1 1 7 6 1 1 1 1 1
1 1 1 7 7 1 1 1 1 1];


a=addrule(a,ruleList);

% Ulaz = [0.04 0.94 0.94 0.04 0.04 0.97 0.04]; %  ovo je ulaz za pin (1.0149)
% Ulaz = [0.07 0.97 0.97 0.04 0.07 0.97 0.07]; % ovo je ulaz za password (1.0161)
% Ulaz = [0.15 0.85 0.85 0.4 0.4 0.8 0.8]; % ovo je ulaz za OTP generated applications (2.0207)
% Ulaz = [0.35 0.70 0.7 0.5 0.5 0.7 0.75]; % ovo je ulaz za OTP using SMS (3.5013)
% Ulaz = [0.65 0.3 0.3 0.6 0.6 0.45 0.6]; % ovo je ulaz za mobile certificate (5.9678)
% Ulaz = [0.9 0.1 0.1 0.8 0.8 0.06 0.98]; % ovo je ulaz za fingerprint (7.9929)
% Ulaz = [0.94 0.07 0.07 0.94 0.94 0.05 0.94]; % ovo je ulaz za face (8.2071)
% Ulaz = [0.97 0.04 0.04 0.97 0.97 0.04 0.96]; % ovo je ulaz za iris (8.5305)
% Ulaz = [0.77 0.45 0.45 0.2 0.2 0.08 0.92]; % ovo je ulaz za voice speech (7.7376)
% Ulaz = [0.8 0.35 0.3 0.55 0.35 0.2 0.8]; % ovo je ulaz za keystroke dynamics (7.6389)
% Ulaz = [0.85 0.5 0.55 0.3 0.2 0.15 0.85]; % ovo je ulaz za gait recognition (7.8048)


fuzout = evalfis([Ulaz], a)
```

BIOGRAFIJA AUTORA

Dragan (Milan) Korać je rođen 24.09.1974. godine u Prijedoru. Osnovnu školu i srednju mašinsku završio u Sanskom Mostu. Na Mašinskom fakultetu u Banjaluci, smjer – proizvodno mašinstvo, diplomirao 1999. godine na temu *Menadžment informacioni sistem.* Magistrirao je 2009. godine na Fakultetu informacionih tehnologija, Panevropskom univerzitetu Apeiron u Banjaluci gdje je odbranio magistarski rad na temu "*Informacioni sistemi obavještajnih agencija tranzicionih zemalja u kontekstu evropskih integracija"*. Osnovni i postdiplomski studij završio u roku, jedan od najboljih u generaciji. Takođe, radi se o bivšem dugogodišnjem vrhunskom sportisti, karatisti osvajaču mnogih evropskih odličja.

Tokom svog dosadašnjeg naučno-istraživačkog rada, Dragan Korać je objavio, u svojstvu prvog autora rad u časopisu od međunarodnog značaja (SCIe lista sa Impakt faktorom), u svojstvu prvog autora 2 rada u časopisima domaćeg značaja i 2 rada na domaćim konferencijama. Takođe, potrebno je napomenuti da Dragan Korać ima prihvaćen, u svojstvu prvog autora, rad pod nazivom "A mathematical model for evaluation of intelligence products value" za objavljivanje u časopisu Journal of Information and Optimization Science - DOI : 10.1080/02522667.2018.1427027 (Taylor & Francis) kao i još dva rada koja su prihvaćena za recenziju u časopisima međunarodnog značaja (SCIe lista sa Impakt faktorom), i to:

1. A model of digital identity and its application in moodle platform.
2. Fishbone Model: Universal Authentication Framework for Evaluation of Multifactor Authenticationin in Mobile Environment.

Prilog 1.

Izjava o autorstvu

Potpisani-a Dragan Korać

broj indeksa _____

Izjavljujem

da je doktorska disertacija pod naslovom **"Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom".**

- rezultat sopstvenog istraživačkog rada,
- da predložena disertacija u celini ni u delovima nije bila predložena za dobijanje bilo koje diplome prema studijskim programima drugih visokoškolskih ustanova,
- da su rezultati korektno navedeni i
- da nisam kršio/la autorska prava i koristio intelektualnu svojinu drugih lica.

Potpis doktoranda

U Beogradu, _____

_____

Prilog 2.

Izjava o istovetnosti štampane i elektronske verzije doktorskog rada

Ime i prezime autora Dragan Korać

Broj indeksa _____

Studijski program Informacioni sistemi

Naslov rada **"Model zaštite informacija u sistemima za menadžment identiteta i upravljanja pristupom"**

Mentor Prof. dr Dejan Simić

Potpisani/a Dragan Korać

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao/la za objavljivanje na portalu **Digitalnog repozitorijuma Univerziteta u Beogradu**.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis doktoranda

U Beogradu, _____

_____

Prilog 3.

Izjava o korišćenju

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom:

“Model zaštite informacija u sistemima za menadžment identiteta i upravljanje pristupom”

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalni repozitorijum Univerziteta u Beogradu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo

2. Autorstvo - nekomercijalno

3. Autorstvo – nekomercijalno – bez prerade

4. Autorstvo – nekomercijalno – deliti pod istim uslovima

5. Autorstvo – bez prerade

6. Autorstvo – deliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponuđenih licenci, kratak opis licenci dat je na poleđini lista).

Potpis doktoranda

U Beogradu, _____

_____

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo – nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo - nekomercijalno – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo - nekomercijalno – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.