Sigurnosne smjernice za izradu biometrijskih sustava

Borovac, Bruno

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Bruno Borovac

SIGURNOSNE SMJERNICE ZA IZRADU BIOMETRIJSKIH SUSTAVA

ZAVRŠNI RAD

Varaždin, 2023.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Bruno Borovac

Matični broj: 0016133208

Studij: Primjena informacijske tehnologije u poslovanju

SIGURNOSNE SMJERNICE ZA IZRADU BIOMETRIJSKIH SUSTAVA

ZAVRŠNI RAD

Mentor/Mentorica:

Izv. prof. dr. sc. Petra Grd

Varaždin, rujan 2023.

Bruno Borovac

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Biometrija, tehnologija koja koristi fizičke ili bihevioralne karakteristike pojedinca za autentifikaciju, postala je neizostavan dio mnogih aplikacija, uključujući kontrolu pristupa, mobilne uređaje i financijske transakcije. Međutim, s povećanjem upotrebe biometrije, pojavljuju se i izazovi u pogledu zaštite podataka i sigurnosti.

Glavne teze ovog rada uključuju potrebu za rigoroznim sigurnosnim smjernicama u razvoju biometrijskih sustava kako bi se zaštitili osjetljivi biometrijski podaci, osigurala točnost autentifikacije i spriječile prijetnje poput prijevara i neovlaštenog pristupa. Rad se bavi istraživanjem etičkih aspekata prikupljanja biometrijskih podataka te naglašava važnost pridržavanja relevantnih standarda i zakona o zaštiti privatnosti.

Kroz konkretni primjer iz prakse - sustav kontrole pristupa - rad ilustrira kako se sigurnosne smjernice primjenjuju u stvarnom scenariju. Zaključci naglašavaju da pravilna primjena sigurnosnih smjernica može značajno povećati sigurnost biometrijskih sustava te ističu važnost kontinuirane edukacije, testiranja sigurnosti i ažuriranja smjernica kako bi se odgovorilo na dinamičke izazove sigurnosti u biometriji. Rad pruža osnovu za daljnje istraživanje i razvoj sigurnih biometrijskih rješenja koja će osigurati pouzdanu autentifikaciju i zaštitu privatnosti korisnika.

Ključne riječi: biometrija; sigurnost; identifikacija; autentifikacija; smjernice; ranjivosti; podaci;

Sadržaj

1. Uvod

U ovom završnom radu govorit će se o sigurnosti i pouzdanosti biometrijskih sustava te navesti kojih bi se smjernica trebalo držati prilikom izrade istih.

Biometrija je kao tehnologija identifikacije i autentifikacije koja se temelji na fizičkim i ponašajnim karakteristikama danas prisutna u raznim područjima informatike i poslovanja i koristi se u sektorima poput medicine i financija te se u takvim sustavima bavi kontrolom pristupa i raznim sigurnosnim kontrolama. Primjer primjene biometrijskih sustava može biti kontrola pristupa računalnim sustavima, sigurnost kod obavljanja financijskih transakcija i slično. Međutim, s porastom upotrebe biometrije, pojavljuju se i izazovi u pogledu zaštite privatnosti, sigurnosti podataka te izbjegavanja zloupotreba. Ovo istraživanje, fokusirat će se na identificiranje ključnih sigurnosnih rizika i potencijalnih prijetnji koje mogu utjecati na biometrijske sustave. Razmotrit će se kako se biometrijski podaci prikupljaju, pohranjuju, obrađuju i koriste te kako se može osigurati njihov integritet, povjerljivost i dostupnost. Također će se istražiti najbolje prakse i smjernice koje su razvijene kako bi se minimizirali rizici i osigurala adekvatna zaštita biometrijskih sustava od potencijalnih napada. Uzimajući u obzir brzi tehnološki napredak i rastuću važnost biometrije u svakodnevnom životu, cilj ovog istraživanja je pružiti dublji uvid u sigurnosne izazove s kojima se biometrijski sustavi suočavaju te istražiti načine kako razviti i implementirati robustne biometrijske sustave. Kroz analizu relevantnih studija slučaja, propisa i industrijskih standarda, nastojat će se identificirati ključne preporuke za dizajn, implementaciju i upravljanje sigurnim biometrijskim sustavima.

U nastavku rada, detaljnije će se istražiti osnovne biometrijske tehnike, obraditi primjere prijetnji i napada na biometrijske sustave te predstaviti moguće strategije i tehnologije za zaštitu tih sustava od napada i zloupotreba. Kroz integraciju teorijskog okvira i praktičnih primjera, cilj rada je pružiti sveobuhvatan pregled sigurnosnih smjernica koje treba primijeniti pri izradi i upravljanju biometrijskim sustavima kako bi se osigurala njihova učinkovita i sigurna primjena.

2. Metode i tehnike rada

Za izradu ovog završnog rada korištene su različite metode i tehnike kako bi se područje istraživanja što bolje shvatilo i teme koje se obrađuju budu kvalitetno objašnjene. Na samom početku su definirani ciljevi rada i ključna pitanja koja se žele obraditi. Zatim je proveden temeljan pregled literature kako bi se dobio što širi pregled o sigurnosnim aspektima biometrije. Istraživani su radovi, knjige i članci koji se bave biometrijskim sustavima i njihovim sigurnosnim izazovima. Analizirani su i relevantni standardi i smjernice koji se odnose na biometrijske sustave te kako oni definiraju sigurnosne zahtjeve. Napravljeno je ispitivanje tehnologija i metoda sigurnosti koji se koriste u biometrijskim sustavima, a odnose se na enkripciju, zaštitu podataka i otpornost na napade. Za prikupljanje informacija o primjeni biometrije u različitim sektorima radila su se istraživanja na praktičnim primjerima. Analizom izazova sigurnosti identificirani su specifični izazovi s kojima se susreću biometrijski sustavi. Na samom kraju napravljena je i studija etičkih aspekata koji govore o problemu privatnosti pojedinaca koji koriste biometrijske sustave i koje su etičke smjernice za njihovu izradu.

3. Biometrija

Biometrija je znanstvena disciplina koja se bavi proučavanjem jedinstvenih karakteristika koje posjeduju ljudi ili drugi živi organizmi. Jain i Ross [1, str. 1] navode da se biometrija kao znanost bavi određivanjem identiteta pojedinca, a za temelj uzima njegove fizičke, kemijske i ponašajne karakteristike. Temelj svega toga je da svaki pojedinac sadrži jedinstvene fizičke i ponašajne karakteristike koje ga razlikuju od drugih, a zatim se pomoću tih karakteristika vrši identifikacija i autentifikacija.

Fizičke karakteristike pojedinca mogu biti na primjer geometrija lica, šarenica oka ili otisak prsta, dok u ponašajne karakteristike spada način na koji osoba hoda, potpis ili dinamika tipkanja na tipkovnici [1, str. 16]U današnje vrijeme s razvojem tehnologije dogodio se i velik porast u upotrebi biometrije, pa tako danas gotovo svatko otključava mobitel otiskom prsta ili skeniranjem lica, no povijest biometrije seže u dosta daleku prošlost jer su se ljudi i u prošlosti oslanjali upravo na te jedinstvene karakteristike koje posjeduje pojedinac kako bi neku osobu prepoznali odnosno identificirali. Biometrija donosi velik značaj i onda kada je u pitanju sigurnost i igra ključnu ulogu u sprječavanju krađe osobnih podataka ili identiteta, ali se koristi i podržava razne sektore poput zdravstva, financija i pravosuđa.

Biometrija ima izuzetan značaj u identifikaciji i autentifikaciji. Jedan od ključnih faktora koji tome doprinosi jest visoka pouzdanost koja je osigurana time što svaki pojedinac ima različite karakteristike, a falsificiranje takvih karakteristika u praksi je dosta teško i upravo zbog toga je biometrija vrlo pouzdana u utvrđivanju identiteta. Osim što je vrlo pouzdana biometrijska identifikacija i autentifikacija prilično je jednostavna i praktična. Najveći značaj biometrija pridonosi sigurnosti i upravo zbog tog razloga prilikom izgradnje biometrijskih sustava vrlo je važno predvidjeti moguće propuste i napade te pažljivo pratiti standarde i određene smjernice kako bi se povećala sigurnost samog sustava. Biometrijski sustavi u današnjem društvu su sveprisutni i imaju jako velik utjecaj na život pojedinca pa se zbog toga prilikom izgradnje sustava također treba pozabaviti i etičkim i pravnim pitanjima koja proizlaze iz uporabe biometrije. U nastavku će biti rečeno nešto više o vrstama fizičkih i ponašajnih biometrijskih karakteristika te o njihovim osobinama.

3.1. Vrste biometrijskih karakteristika

Ovisno o vrsti biometrijskog sustava i za koju namjenu se isti koristi potrebno je odabrati biometrijsku karakteristiku koja najviše odgovara tom slučaju. Postoji sedam različitih faktora koji određuju je li određena biometrijska karakteristika pogodna za korištenje u nekom biometrijskom sustavu i to su univerzalnost, jedinstvenost, stalnost, prikupljivost, performanse, prihvatljivost i otpornost na nadmudrivanje (*eng. Circumvention*) [2].

- Univerzalnost: podrazumijeva se da svaka osoba koja pristupa sustavu mora posjedovati tu karakteristiku.
- Jedinstvenost: biometrijska karakteristika ne smije biti jednaka kod dvije različite osobe.
- Stalnost: karakteristika mora biti stalna kroz određeni vremenski period.
- Prikupljivost: karakteristika se mora moći prikupiti i mora biti mjerljiva.
- Performanse: osobina mora biti u skladu sa zahtjevima sustava, ako sustav zahtjeva veliku preciznost i karakteristika mora zadovoljavati tu osobinu.
- Prihvatljivost: osobe koje koriste sustav i daju svoje biometrijske karakteristike moraju s time biti suglasne i voljne dati istu.
- Otpornost na nadmudrivanje: odnosi se na to koja je mogućnost da se neka karakteristika imitira pomoću drugih stvari kao na primjer silikonski otisak prsta.

3.1.1. Fizičke biometrijske karakteristike

Geometrija lica fizička je biometrijska karakteristika koja se dosta često koristi za identifikaciju i autentifikaciju pojedinaca. Temelji se na jedinstvenim značajkama lica svakog pojedinca kao što su oblik lica, razmak između očiju, oblik usana, duljina nosa i slično. Primjena prepoznavanja lica može se izvoditi u statičkom okruženju gdje postoji slika lica ili i dinamičkom okruženju na primjer skupina ljudi na nekom mjestu. Danas su sustavi za prepoznavanje lica rasprostranjeni i često u uporabi, no bitno je napomenuti da kod takvih sustava postoje ograničenja kako će se slike lica prikupljati i slike se uglavnom prikupljaju u točno određenim uvjetima osvjetljenja i položaja lica [2].

Neke od prednosti korištenja geometrije lica kao biometrijske karakteristike su jednostavnost korištenja jer ne traži posebnu interakciju korisnika, brza autentifikacija i visoka pouzdanost budući da su karakteristike lica svake osobe drugačije. Nedostatci ove karakteristike su promjena izgleda lica osobe, ovisnost o vanjskim uvjetima odnosno osvjetljenju te privatnost jer se radi o osobnoj karakteristici.

Otisak prsta je jedna od najpoznatijih i najčešće korištenih fizičkih biometrijskih karakteristika za identifikaciju i autentifikaciju. Radi se o jedinstvenim uzorcima otisaka prstiju koji se nalaze na vrhu prsta svake osobe.

Otisak prsta temelji se na analizi jedinstvenih crta i karakteristika otiska koje uključuju vijuge, razdjeljke kao i druge detalje poput točaka, zakrivljenosti i granica. Upravo zbog takvih sitnih detalja koji se uspoređuju podacima u sustavu postoje razne klasifikacije otiska prsta i kako bi se osigurala učinkovitost prepoznavanja često se koriste algoritmi koji poboljšavaju kvalitetu slika otisaka prstiju [3].

Otisak prsta koristi se u mnogim situacijama od otključavanja mobilnih uređaja sve do pristupa sigurnosnim sustavima banaka ili čak vojske. Prednosti ove karakteristike su zasigurno pouzdanost pri identifikaciji i autentifikaciji jer svaka osoba ima različit otisak prsta i također skeniranje otiska prsta je brzo i jednostavno. Naravno postoje i ograničenja ove biometrijske karakteristike, a ona se ogledaju u tome da kvaliteta otiska može biti loša, sustav se može prevariti lažnim otiskom i na samom kraju to je također osobna karakteristika pa može doći do narušavanja privatnosti.

Šarenica oka ima posebne karakteristike i razlikuje se po svom obliku, šarama, prstenovima i ostalim detaljima. Za identifikaciju i autentifikaciju koristi se sustav za skeniranje šarenice oka koji najčešće koristi infracrvenu ili vidljivu svjetlost i zatim stvara digitalnu sliku šarenice [4].

Šarenica se koristi u situacijama kada je potrebna visoka pouzdanost identifikacije iz razloga što je ovu biometrijsku karakteristiku teško krivotvoriti i to je jedna od njenih najvećih prednosti. Osim što ju je teško krivotvoriti šarenica oka također je jedinstvena i jednostavno se koristi na način da se pogleda u skener očiju koji tada dobivene podatke uspoređuje s podacima u bazi. Naravno ni ova biometrijska karakteristika nije u potpunosti savršena i do problema može doći ako su loši vanjski uvjeti odnosno kvaliteta skeniranja osjetljiva je na osvjetljenje. Kao i kod drugih biometrijskih karakteristika i ova je karakteristika osobna i može doći do povrijede privatnosti pojedinca. Osobe se moraju osjećati sigurno u vezi s tim kako se njihovi biometrijski podaci koriste i štite.

3.1.2. Ponašajne biometrijske karakteristike

Ponašajne biometrijske karakteristike odnose se na osobine koje se zasnivaju na načinu na koji se osoba ponaša ili kako izvodi određene aktivnosti. U nastavku će biti objašnjene neke od ponašajnih biometrijskih karakteristika koje se često koriste u biometrijskoj identifikaciji i autentifikaciji, a to su glas, potpis, dinamika tipkanja i hod.

Analiza glasa je ponašajna biometrijska osobina koja se koristi za identifikaciju i autentifikaciju osoba na temelju njihovog glasovnog obrasca. Radmilović [5] govori o tome da kada je riječ o identifikaciji osobe temeljem glasa, radi se o karakteristikama glasa poput boje glasa, modulacijama, frekvencijama, specifičnostima izgovora određenih glasova, govornim manama i drugo. Ovo područje identifikacije zove se fonoskopska identifikacija i u takvim slučajevima radi se sa snimljenim glasovima osobe koji se kasnije uspoređuje s drugim uzorcima.

Potpis kao ponašajna biometrijska karakteristika se temelji na načinu na koji osoba piše određena slova i oblike. Svaki potpis ima neka svoja obilježja i Radmilović [5] navodi da su opća obilježja opći izgled rukopisa, stupanj ispisanosti, raspored teksta, odnos prema liniji pisanja, veličina rukopisa, razmaci, vezanost i nevezanost slova, rastavljanje riječi, brzina pisanja, pritisak na papir, nagib rukopisa, ukrašavanje i dr.

Dinamika tipkanja je biometrijska karakteristika koja se koristi za identifikaciju ili autentifikaciju osobe na temelju načina tipkanja po tipkovnici.

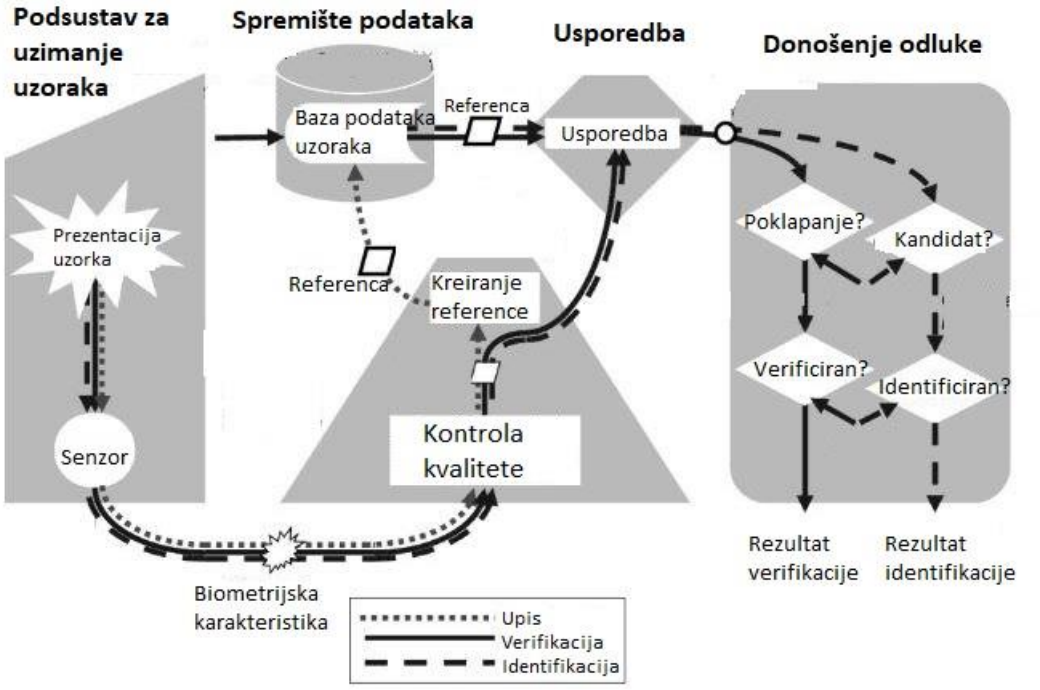
Svaka osoba ima jedinstven način tipkanja kod kojih se razlikuje brzina, vrijeme potrebno da se napravi promjena pritiska između dvije tipke i duljina pritiska na jednu tipku, a sve to analizira informacijski sustav koji te podatke pohranjuje i uspoređuje [5].

Biometrija hodanja ponašajna je biometrijska karakteristika koja se koristi za identifikaciju ili autentifikaciju osobe na temelju njenog načina hodanja. Svaka osoba ima svoj specifičan ritam, brzinu, duljinu koraka i način hodanja koji je karakterističan upravo za tu osobu. Kod svih navedenih ponašajnih karakteristika bitno je napomenuti da su i one, kao i fizičke biometrijske karakteristike, jedinstvene za svakog pojedinca te da i kod njih postoji mogućnost krivotvorenja.

4. Biometrijski sustavi

Biometrijski sustavi predstavljaju revolucionarnu granu tehnologije koja omogućuje identifikaciju i autentifikaciju pojedinaca na temelju njihovih jedinstvenih fizičkih i ponašajnih karakteristika. U suštini, biometrijski sustavi koriste tijelo i ponašanje kao prirodne osobne identifikatore, pružajući izuzetnu preciznost i sigurnost u procesu prepoznavanja. Ova tehnologija donosi sa sobom duboke implikacije u različitim aspektima naših života, od svakodnevne upotrebe pametnih telefona do primjene u sigurnosti, pravosuđu i medicini.

Biometrijski sustav može se opisati kroz podjelu u nekoliko različitih podsustava. Podsustave čine podsustav za prikupljanje, prijenos i procesiranje u svrhu poboljšanja biometrijskih karakteristika, zatim podsustav za pohranu biometrijskih podataka, podsustav za izvođenje usporedbe ulaznih i spremljenih podataka te na kraju podsustav za donošenje odluke [6, str. 16]. Sljedeća slika 1 prikazuje biometrijski sustav podijeljen na prethodno navedene podsustave.



Slika 1. Prikaz komponenti biometrijskog sustava [6, str. 16]

Princip rada biometrijskog sustava sastoji se od nekoliko ključnih koraka. Ulaz u podsustav za prikupljanje podataka jest neka biometrijska karakteristika koja se dobiva preko senzora. Tu se vrši postupak pretvorbe sirove biometrijske karakteristike neke osobe u digitalan oblik.

Primjer senzora za prikupljanje takve vrste podataka može biti kamera na mobitelu za prepoznavanje lica, skener za uzimanje otiska prsta ili pak mikrofon koji snima glas osobe.

Neil i Ted [6, str. 17] navode da kod uzimanja uzoraka, zbog vanjskih smetnji i šumova, pretvorba nikada za rezultat neće dati dva ista digitalna uzorka. Sljedeći korak je procesiranje tako dobivenih biometrijskih karakteristika koje su sada u digitalnom obliku. Procesiranje uključuje uklanjanje šumova, traženje raznih karakteristika koje posjeduje uzorak te na kraju i davanje ocjene o kvaliteti uzetog uzorka. Tako na primjer kod uzorka slike lica u ovom postupku se traže karakteristike poput oblika lica, razmaka između očiju i slično. Zatim, ako je kvaliteta uzorka zadovoljavajuća, šablona uzorka se sprema u mjesto predviđeno za pohranu podataka.

Postoji mogućnost da je takve podatke potrebno zaštititi enkripcijom zbog sigurnosnih razloga i privatnosti korisnika [6, str. 17].

Sljedeći na redu dolazi podsustav za usporedbu koji uzima primjerak spremljene biometrijske karakteristike iz baze podataka gdje su spremljene šablone te uzima i uzorak koji se nalazi na ulazu u sustav uzet preko senzora i ta dva uzorka uspoređuje. Usporedbom sustav pokušava odrediti radili se o osobi čiji uzorak postoji u bazi podataka, a vrlo bitan faktor u ovom postupku je dodjeljivanje ocjene u smislu poklapanja ta dva uzorka. Ovisno o ocjeni podsustav za donošenje odluke zatim prepoznaje osobu koja je dala karakteristiku ili je ne prepoznaje.

4.1. Unimodalni i multimodalni biometrijski sustavi

Unimodalni biometrijski sustavi su sustavi za identifikaciju i autentikaciju koji koriste samo jednu biometrijsku karakteristiku ili osobnu karakteristiku pojedinca za provođenje ovih postupaka. Unimodalni sustavi temelje se na ideji da svaka osoba posjeduje jedinstvene osobne karakteristike koje se mogu koristiti za njihovu identifikaciju [7].

Današnji unimodalni biometrijski sustavi uvelike su poboljšali svoju točnost i pouzdanost, no i dalje se kod ovakvih sustava javljaju određene poteškoće u procesu uzimanja uzoraka. Problemi koji se tu pojavljuju su vezani uz ne univerzalnost biometrijskih karakteristika, lažnog predstavljanja i slabije preciznosti zbog smetnji kod uzimanja uzoraka [7].

Smetnje u uzorcima znaju stvarati poteškoće kada se uzorci uzimaju pomoću starijih senzora ili senzora koji se nisu redovito održavali. Isto tako prilikom snimanja glasa osobe često se znaju pojaviti smetnje u obliku loše kvalitete zvuka. Ne univerzalnost je problem koji se javlja jer nemaju uvijek sve osobe neku biometrijsku karakteristiku, pa tako postoje osobe koje nemaju otisak prsta ili su nijeme i od takvih osoba se ne može uzeti određena biometrijska karakteristika. Kod unimodalnih biometrijskih sustava čak se može pojaviti problem da su dvije

karakteristike različitih osoba vrlo slične na primjer geometrija lica kod ljudi koji su blizanci. Na kraju ovakvi biometrijski sustavi ranjivi su na lažno predstavljanje i moguće ih je prevariti lažiranjem neke biometrijske karakteristike kao na primjer lažiranje otiska prsta na papiru i slično [3]. Za rješavanje problema koji se pojavljuju kod unimodalnih biometrijskih sustava pristupa se izradi multimodalnih biometrijskih sustava.

Multimodalni biometrijski sustavi predstavljaju napredniju razinu u biometriji jer koriste više od jedne biometrijske karakteristike za identifikaciju i autentifikaciju pojedinaca. Ovi sustavi integriraju podatke iz različitih biometrijskih izvora kako bi povećali preciznost, sigurnost i pouzdanost identifikacije [7].

Tipičan primjer kako multimodalni biometrijski sustav rješava problem ne univerzalnosti koji se javlja kod unimodalnih sustava jest da kada osoba ima oštećene otiske prstiju koje senzor ne može prepoznati, ali to ne utječe na proces identifikacije i autentifikacije jer se sustavu predstavlja još jedna biometrijska karakteristika [7].

Multimodalni sustavi kombiniraju više biometrijskih karakteristika, uključujući otiske prstiju, geometriju lica, šarenicu oka, glasovne uzorke, način hodanja i druge karakteristike. Integracija različitih karakteristika omogućuje veću razinu sigurnosti jer se povećava teškoća za načiniti prijevaru i povećava preciznost identifikacije. Multimodalni biometrijski sustavi mogu se primijeniti u različitim sektorima, uključujući kontrolu pristupa, sigurnosne sustave, e-bankarstvo, putovanja i pravosudne aplikacije. Mogu se prilagoditi različitim potrebama i sigurnosnim razinama. Iako pružaju veću sigurnost, multimodalni sustavi ne nužno kompromitiraju praktičnost. Korištenjem više karakteristika, moguće je postići bržu autentifikaciju, jer osoba može koristiti bilo koju od svojih biometrijskih karakteristika za prijavu. Implementacija multimodalnih biometrijskih sustava zahtijeva složeniji hardver i softver te upravljanje velikom količinom biometrijskih podataka. To može predstavljati tehničke i logističke izazove. Kako multimodalni sustavi prikupljaju više osobnih biometrijskih podataka, pitanja privatnosti postaju važnija. Potrebno je pažljivo upravljati i zaštititi ove podatke.

Multimodalni biometrijski sustavi predstavljaju napredak u sigurnosti i preciznosti identifikacije i autentifikacije. Njihova sveprisutna primjena može značajno doprinijeti smanjenju rizika od krađe identiteta i neovlaštenih pristupa, što je od suštinskog značaja u suvremenom digitalnom društvu.

4.2. Biometrijska identifikacija i verifikacija

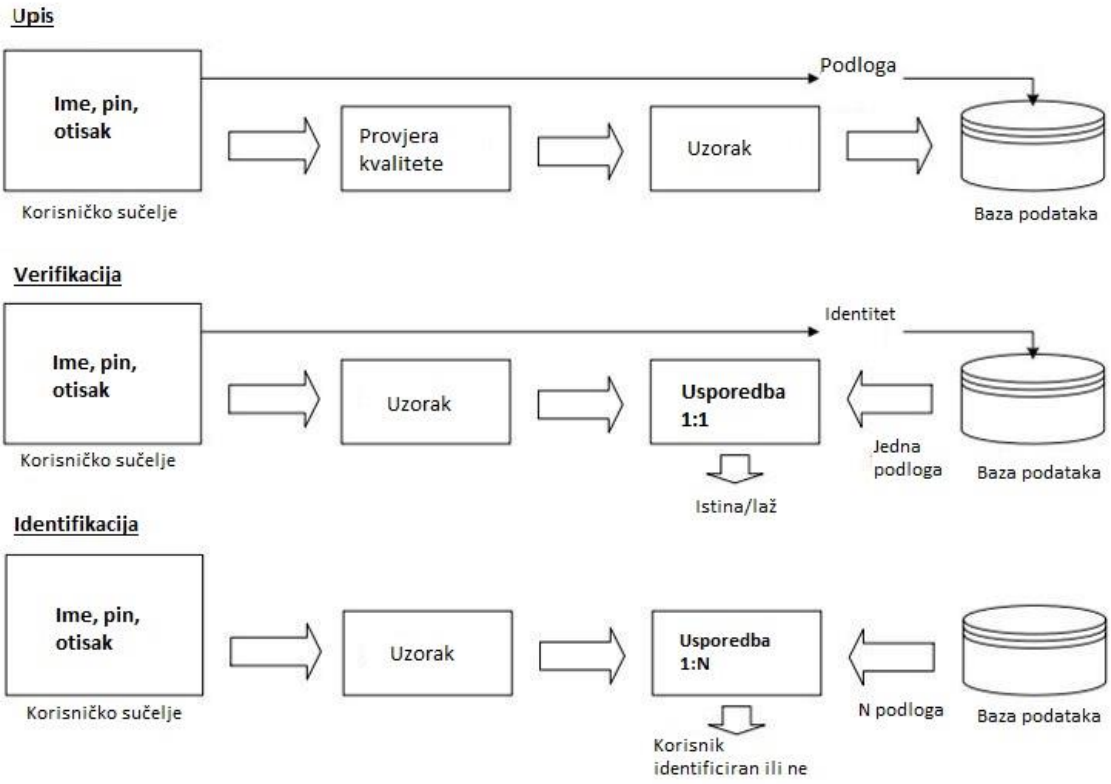
Biometrijska identifikacija i verifikacija su ključni procesi u biometrijskim sustavima za prepoznavanje i autentifikaciju pojedinaca. Ova dva postupka igraju ključnu ulogu u različitim aplikacijama, od otključavanja pametnih telefona do kontrole pristupa područjima visoke sigurnosti.

Biometrijska identifikacija, poznata i kao jednostavno "identifikacija", odnosi se na postupak određivanja identiteta osobe na temelju biometrijskih podataka. U postupku identifikacije, sustav uspoređuje biometrijske podatke osobe s pohranjenim uzorcima u bazi podataka kako bi pronašao najbolje podudaranje. To znači da sustav pokušava utvrditi identitet osobe među svim mogućim korisnicima u bazi podataka [8].

Biometrijska identifikacija koristi se u situacijama gdje je potrebno prepoznati osobu iz velikog broja kandidata, kao što je policijska istraga ili sustav za evidenciju dolaska na posao.

Biometrijska verifikacija, također poznata kao "autentifikacija", odnosi se na postupak potvrde da je osoba ona koja tvrdi da jest na temelju biometrijskih podataka. U postupku verifikacije, osoba tvrdi svoj identitet, obično pružajući biometrijski podatak (npr. otisak prsta, skeniranje lica), a sustav tada provjerava podudara li se taj biometrijski podatak s pohranjenim podacima za taj identitet u bazi podataka [9].

Biometrijska verifikacija koristi se u situacijama gdje je potrebno potvrditi da je osoba ona koja tvrdi da jest, kao što je otključavanje pametnih telefona ili provjera identiteta prilikom plaćanja putem otiska prsta. Sljedeća slika 2 prikazuje proces upisa, identifikacije i verifikacije u biometrijskom sustavu.



Slika 2. Upis, identifikacija i verifikacija u biometrijskom sustavu [10]

Ključne razlike između biometrijske identifikacije i verifikacije uključuju opseg i broj kandidata koji se provjeravaju. Identifikacija traži podudaranje među svim mogućim kandidatima, dok verifikacija provjerava identitet samo u odnosu na jednog kandidata. Oba postupka imaju svoje prednosti i primjene, a izbor između identifikacije i verifikacije ovisi o specifičnim potrebama i sigurnosnim zahtjevima pojedine aplikacije. U mnogim sustavima koriste se kombinacije oba postupka kako bi se postigla veća sigurnost i pouzdanost u autentifikaciji [10].

4.3. Evaluacija biometrijskih sustava

Evaluacija biometrijskih sustava je ključna faza u njihovom razvoju i implementaciji. Ovaj proces se provodi kako bi se ocijenila učinkovitost i pouzdanost sustava u prepoznavanju i autentifikaciji pojedinaca. Evaluacija omogućuje identifikaciju prednosti i nedostataka sustava te pomaže u donošenju odluka o poboljšanjima i prilagodbama.

Evaluacijski protokoli određuju kako će se testirati sustav, odabrani podaci i kako će se mjeriti učinkovitost. Za evaluaciju biometrijskih sustava, potrebno je koristiti dobro definirane i

reprezentativne skupove podataka. Ovi skupovi trebaju sadržavati biometrijske podatke koji su relevantni za specifičnu primjenu sustava [9].

Za procjenu učinkovitosti biometrijskog sustava potrebno je koristiti odgovarajuće metrike. Najčešće korištene metrike uključuju [8]:

- Stopa neuspjeha upisa: Koliko korisnika ne može uspješno biti upisano u sustav (failure to enroll).
- Vrijeme autentifikacije: Koliko je brzo sustav u procesu autentifikacije.
- Stopa lažnog odbijanja: Koliko često sustav ne prepoznaje osobu (false rejection rate).
- Stopa lažnog prihvaćanja : Koliko često sustav prihvaća neovlaštene korisnike (false acceptance rate).

Formule za računanje false rejection rate (FRR) i false acceptance rate (FAR) izvode se na sljedeći način [8]:

$$FAR = \frac{False_{positive}}{False_{positive} + True_{negative}}$$

$$FRR = \frac{False_{negative}}{False_{negative} + True_{positive}}$$

Evaluacija biometrijskih sustava također uključuje testiranje njihove sigurnosti. To uključuje analizu i testiranje sustava kako bi se utvrdilo koliko je otporan na različite vrste prijevara i napada, uključujući napade kao što su "spoofing" (krivotvorenje) biometrijskih podataka. Evaluacija biometrijskih sustava često uključuje usklađenost s određenim standardima. Važno je analizirati ograničenja sustava i identificirati situacije u kojima biometrijski sustav može izgubiti na učinkovitosti, kao što su promjene u biometrijskim karakteristikama pojedinca zbog starenja ili ozljeda [9].

Evaluacija biometrijskih sustava ključan je korak u osiguravanju njihove pouzdanosti i sigurnosti. Dobro provedena evaluacija omogućuje poboljšanje sustava, donošenje odluka o nadogradnjama te osigurava da se sustav primjenjuje na način koji najbolje odgovara potrebama i sigurnosnim zahtjevima specifične primjene.

4.3.1. Evaluacija biometrijskog sustava prepoznavanja lica

Evaluacija biometrijskog sustava prepoznavanja lica ključna je kako bi se utvrdila njegova pouzdanost i učinkovitost. Postupak evaluacije prepoznavanja lica obuhvaća uporabu standardiziranih metoda i skupova podataka kako bi se testirala sposobnost sustava za točno prepoznavanje i autentifikaciju pojedinaca na temelju njihovih lica.

Između rujna 1996. i ožujka 1997. godine napravljena je evaluacija jednog sustava za prepoznavanje lica [9]. Istraživačke grupe dobile su komplet slika lica osoba kako bi razvile i poboljšale njihov sustav. Evaluacijom se mjerila učinkovitost sustava verifikacije i identifikacije i dobiveni su rezultati učinkovitosti za različite kategorije slika. Prva kategorija su bile slike uslikane isti dan pod istim osvjetljenjem. Od ove kategorije su se očekivali najbolji rezultati učinkovitosti prepoznavanja lica. Svaka sljedeća kategorija trebala je sustavu zadati sve veće poteškoće, pa se tako zadnja kategorija slika sastojala od uzoraka koji su nastali godinu i pol nakon [9]. Na slici 2 prikazani su rezultati evaluacije sustava za prepoznavanje lica.

Kategorija	Stopa lažnog prihvaćanja FAR	Stopa lažnog odbijanja FRR
Prvi dan, isto osvjetljenje	2	0.4
Prvi dan, drugačije osvjetljenje	2	9
Drugi dani	2	11
Drugi dan s razmakom od 1.5 godine	2	43

Slika 3. Rezultati evaluacije [9, str. 61]

Zaključak ovog istraživanja bio je taj da je intenzitet svjetlosti, koji je ovisio o dobu dana kada su slike nastale, uvelike doprinosio padu učinkovitosti sustava za prepoznavanje lica te su se neki rezultati gotovo poklapali s rezultatima dobivenim koristeći slike koje su uslikane godinu i pol nakon.

Evaluacija biometrijskog sustava za prepoznavanje lica pomaže u identifikaciji potrebnih poboljšanja, optimizaciji parametara i osiguranju da sustav radi s visokom pouzdanošću. Ovo je ključno za razvoj i implementaciju sigurnih i učinkovitih biometrijskih rješenja.

5. Sigurnost biometrijskih sustava

Sigurnost u biometrijskim sustavima odnosi se na skup mjera i tehnika dizajniranih za zaštitu biometrijskih podataka i osiguranje pouzdanosti, integriteta te povjerljivosti tih podataka u kontekstu identifikacije i autentifikacije pojedinaca na temelju njihovih biometrijskih karakteristika. Osnovna svrha sigurnosti u biometrijskim sustavima je sprečavanje neovlaštenog pristupa, prijevara i zloupotreba biometrijskih podataka [10].

Ključni aspekti sigurnosti u biometrijskim sustavima uključuju [10]:

- Pouzdanost: Sposobnost biometrijskog sustava da točno prepozna ili autentificira pojedinca na temelju njegovih biometrijskih karakteristika. Visoka pouzdanost znači smanjenje lažnih pozitiva i lažnih negativa.
- Integritet: Osiguravanje da biometrijski podaci ostanu netaknuti i nepromijenjeni tijekom prijenosa, pohrane i obrade. To sprječava napadače da mijenjaju biometrijske podatke kako bi prevarili sustav.
- Povjerljivost: Zaštita biometrijskih podataka od neovlaštenog pristupa i gledanja. Osigurava da samo ovlaštene osobe imaju pristup tim podacima.
- Otpornost na prijevare: Biometrijski sustavi moraju biti otporni na različite vrste prijevara, kao što su pokušaji korištenja lažnih biometrijskih podataka ili uređaja za "spoofing" (krivotvorenje).
- Usklađenost s privatnošću i zakonima: Sigurnost u biometrijskim sustavima treba biti u skladu s relevantnim zakonima i regulacijama koji štite privatnost pojedinaca.
- Sigurnost uređaja: Otpornost samih biometrijskih uređaja na fizičke prijetnje i napade.
- Pravilno upravljanje ključevima: Sigurno upravljanje ključevima za enkripciju i dekripciju biometrijskih podataka.
- Etički aspekti: Razmatranje etičkih pitanja u vezi s prikupljanjem, pohranom i upotrebom biometrijskih podataka.
- Redovito ažuriranje i evaluacija: Kontinuirano ažuriranje sigurnosnih mjera i redovita evaluacija sigurnosti biometrijskih sustava kako bi se identificirali potencijalni rizici i ranjivosti.

Sigurnost u biometrijskim sustavima ključna je kako bi se osigurala pouzdanost i prihvatljivost ovih sustava u različitim sektorima.

5.1. Zaštita biometrijskih podataka

Enkripcija biometrijskih podataka je ključni aspekt sigurnosti u biometrijskim sustavima. Enkripcija se koristi kako bi se zaštitila povjerljivost biometrijskih podataka tijekom prijenosa, pohrane i obrade. Enkripcija je proces pretvaranja čitljivih biometrijskih podataka u nečitljivi format uz pomoć matematičkih algoritama i ključa za enkripciju. Samo osoba koja posjeduje odgovarajući ključ za dekripciju može dešifrirati podatke natrag u čitljiv oblik.

Biometrijski podaci (npr. otisci prstiju, skeniranja lica) prije pohrane ili prijenosa se pretvaraju u nečitljiv format uz pomoć enkripcijskog algoritma i ključa za enkripciju. Tek tada se pohranjuju ili prenose preko mreže. Prilikom pristupa biometrijskim podacima, ključ za dekripciju koristi se za povrat originalnih podataka. Transportna enkripcija primjenjuje se na biometrijske podatke tijekom prijenosa putem mreže, često se koristi za web i mobilne aplikacije. Pohranjena enkripcija, s druge strane, primjenjuje se na biometrijske podatke dok se pohranjuju na uređaju ili u bazi podataka [11].

Enkripcija je ključna zaštita protiv neovlaštenog pristupa biometrijskim podacima. Ona osigurava da, čak i ako zlonamjerni akteri dobiju pristup pohranjenim biometrijskim podacima, ti podaci ostaju nečitljivi bez odgovarajućeg ključa za dekripciju. Korištenje enkripcije za zaštitu biometrijskih podataka ključno je za osiguranje povjerljivosti i sigurnosti tih podataka u biometrijskim sustavima, posebno u osjetljivim aplikacijama poput sustava za kontrolu pristupa i e-bankarstva.

Osim enkripcije kod zaštite pohrane biometrijskih podataka ključni su i još neki faktori. Potrebno je dobro odrediti prava za pristup tako da samo ovlaštene osobe imaju pristup pohranjenim biometrijskim podacima. Bitna je i fizička zaštita uređaja na kojima su pohranjeni podaci kako bi se zaštitili od krađe i vandalizma. Biometrijski sustavi za pohranu trebaju se redovito ažurirati kako bi se zakrpale poznate ranjivosti. Također je važno kontinuirano nadzirati sustav kako bi se detektiralo i reagiralo na bilo kakve nepravilnosti. Redovito pravljenje sigurnosnih kopija biometrijskih podataka osigurava da se podaci mogu obnoviti u slučaju gubitka ili oštećenja.

5.2. Prijetnje sigurnosti u biometrijskim sustavima

Sigurnost u biometrijskim sustavima suočava se s različitim prijetnjama i ranjivostima koje mogu ugroziti povjerljivost i integritet biometrijskih podataka, kao i samu točnost i pouzdanost autentifikacije pojedinaca.

Procjena ranjivosti biometrijskog sustava je vrlo važna za biometrijsku sigurnost i taj je koncept različit od koncepta biometrijske preciznosti. Naime, savršeno precizan sustav može biti vrlo ranjiv na napad neautoriziranog korisnika, koji može naći alternativne načine da se lažno prijavi na sustav. Ranjivosti biometrijskog sustava se do sada posvećivala manja pažnja nego preciznosti, ali je sve veće korištenje biometrije u praksi natjeralo da se ovom pitanju posveti dužna pažnja [12].

Postoji mnogo točaka ranjivosti u biometrijskim sustavima i u nastavku će biti navedene neke od njih. Biometrijski sustav ranjiv je na mjestu gdje se prezentira određena biometrijska karakteristika u podsustavu za uzimanje biometrijskih uzoraka odnosno senzoru. Isto tako sustav je ranjiv prilikom prijenosa podataka o uzetom biometrijskom uzorku u druge dijelove biometrijskog sustava, bilo to prenošenje prema bazi podataka, podsustavu za obradu i usporedbu biometrijskih uzoraka ili podsustavu za donošenje odluke [13].

U dijelu sustava koji obrađuje biometrijske podatke ranjivost se javlja kod kontrole kvalitete i ekstrakcije biometrijskih značajki te kod kreiranja reference koja se iz ovog djela sustava šalje u bazu podataka [12].

Baza podataka još je jedan ranjivi dio svakog biometrijskog sustava gdje može doći do slanja lažnih zahtjeva, ali i do grešaka kod same administracije baze podataka. Sustav za usporedbu biometrijskih uzoraka najviše je ranjiv na hakerske napade kojima se može manipulirati rezultatima usporedbe. Najviše točaka ranjivosti nalazi se u sustavu za donošenje odluke gdje se mogu mijenjati rezultati usporedbe prilikom prijenosa tih rezultata i u takvoj situaciji sustav može donesti krivu odluku. Promjena definiranog praga za odlučivanje, promjena liste kandidata, politike odlučivanja i na kraju manipuliranje ishoda odlučivanja sve su to točke ranjivosti sustava za donošenje odluka [12].

Osim ovih točaka ranjivosti još jedan bitan ranjivi faktor u biometrijskim sustavima zasigurno su sami administratori tih sustava odnosno zaposlenici koji svakako mogu biti zlonamjerni i samim time povećati ranjivost sustava za kojeg su zaduženi. U nastavku rada će biti opisani konkretni napadi prema određenim točkama napada i biti će predložene mjere zaštite kako do tih napada ne bi došlo.

5.2.1. Napadi lažnim karakteristikama

Napadi lažnima karakteristikama u biometrijskom sustavu odnose se na pokušaj prijevare sustava korištenjem lažnih biometrijskih podataka ili uređaja kako bi se predstavili kao legitimni korisnik. Ova vrsta napada događa se u točki biometrijskog sustava gdje se

prezentira biometrijska karakteristika [13]. U nastavku će biti navedeni neki primjeri napada lažnim biometrijskim karakteristikama u točki prezentacije biometrijskih karakteristika.

U sustavu za prepoznavanje lica, napadač može pokušati prevariti sustav koristeći fotografiju lica osobe umjesto stvarnog lica. Na primjer, napadač može preuzeti fotografiju korisnikovog lica s društvenih mreža ili interneta i pokušati je koristiti kako bi prošao autentifikaciju. Ako sustav nije dovoljno sofisticiran da prepozna razliku između stvarnog lica i slike, napad može biti uspješan.

Biometrijski sustavi koji koriste otiske prstiju mogu biti podložni ovoj vrsti napada. Napadač može pokušati stvoriti lažne otiske prstiju koristeći različite materijale poput gipsa, silikona ili čak želatine [12].

Biometrijski sustavi koji koriste prepoznavanje glasa također su osjetljivi na lažno predstavljanje. Napadač može pokušati imitirati glas korisnika kako bi se prijavio u sustav. Ovo može uključivati pokušaj reprodukcije snimke glasa ili pokušaj glasovnog oponašanja.

Lažno predstavljanje živosti uključuje različite tehnike za prevaru biometrijskog sustava kako bi se prikazalo da je biometrijski uzorak stvaran i živ, umjesto statičkog i lažnog. Ove tehnike mogu uključivati simulaciju pulsa, termičku aktivnost ili drugo ponašanje koje bi sugeriralo životnost uzorka. Da bi se obranili od napada lažnim karakteristikama, biometrijski sustavi trebaju uključivati dodatne sigurnosne mehanizme poput detekcije lažnih uzoraka, provjere života i analize dinamičkih karakteristika (poput dinamičkog ponašanja pri skeniranju otisaka prstiju ili lica) [13].

5.2.2. Hakerski napadi

Ova vrsta napada na biometrijske sustave u najvećoj mjeri iskorištava ranjivosti sustava prilikom prijenosa podataka unutar istog. Hakerski napadi na biometrijske sustave često su sofisticirani i zahtijevaju duboko razumijevanje biometrijskih tehnologija i sigurnosnih propusta [13].

Primjer jednog ovakvog napada prilikom prijenosa uzetog uzorka sa senzora u podsustav za obradu tog uzorka. U ovoj točki napada iskorištavanjem nesigurne veze napadač može sustav ugroziti na dva načina. Prvi primjer je da osoba pokušava pristupiti sustavu tako što senzoru predstavlja svoj otisak prsta, a napadač ukrade njegov otisak prsta iskorištavajući ne sigurnost veze prilikom prijenosa uzorka sa senzora do sustava za obradu podataka. Drugi slučaj je da napadač iskorištava nesigurnu vezu i bez da je itko preko senzora poslao bilo kakav uzorak on šalje sustavu lažni uzorak [12].

Drugi primjer napada ove vrste jest *brute force* napad koji iskorištava ranjivost sustava koji omogućava ponovno preuzimanje uzoraka odnosno da se korisnik neograničen broj puta može pokušati prijaviti u sustav.

Recimo da neki sustav koji kao ulaznu karakteristiku prima geometriju ruke omogućava neograničen broj pokušaja prijava u sustav, tada postoji velika šansa da napadač ovom tehnikom prevari sustav [12].

Postoji velik broj načina na koji hakeri koji imaju podatke o nekom biometrijskom sustavu mogu iskoristiti njegove ranjivosti i najčešće su to ranjivosti vezane uz prijenos podataka unutar sustava. Kao zadnji primjer ovakve vrste napada navest će se napadi vezani uz kreiranje i prijenos referenci.

U podsustavu za obradu podataka nakon što je stigao biometrijski uzorak, nakon što je sustav odredio da je uzorak zadovoljavajući, dolazi do stvaranja reference na temelju tog uzorka. Ovdje haker može unesti novi ili promijeniti postojeći programski kod koji sustav koristi za stvaranje reference i tako omogućiti prijavu lažnim osobama. Referenca koja se ovdje stvara prenosi se prvo u bazu podataka, a zatim iz baze podataka u podsustav za usporedbu kako bi se referenca usporedila s tekućim uzorkom. Ovdje kod prijenosa tako dobivenog predloška napadač može zamijeniti ili predložak koji treba unijeti u bazu ili predložak koji izlazi iz baze i uspoređuje se s tekućim uzorkom i u oba slučaja narušiti sigurnost sustava [12].

Zaštita od ovakvih napada zahtijeva sveobuhvatnu sigurnosnu strategiju koja uključuje enkripciju podataka tijekom prijenosa i pohrane, stroge kontrole pristupa, nadzor aktivnosti korisnika, redovite sigurnosne provjere i testiranje ranjivosti, kao i usklađenost sa sigurnosnim standardima i zakonima o zaštiti podataka.

5.2.3. Napadi na uređaje

Napadi na uređaje u biometrijskom sustavu mogu se odnositi na fizičke ili digitalne prijetnje koje ciljaju uređaje za prikupljanje biometrijskih podataka ili uređaje za pohranu i obradu tih podataka [13]. U nastavku će biti naveden primjer fizičkog napada na uređaj za prikupljanje otisaka prstiju.

Na samom početku napadač identificira uređaj za prikupljanje otisaka prstiju koji se koristi za autentifikaciju pristupa zgradi. Zatim napadač fizički pristupa uređaju za prikupljanje otisaka prstiju. To može uključivati oštećenje uređaja kako bi onemogućio njegovo normalno funkcioniranje ili pokušaj prisilnog otvaranja uređaja kako bi pristupio senzoru otiska prsta. Ako napad uspije, napadač može pokušati ukrasti ili presresti biometrijske podatke koji se

prikupljaju tijekom autentifikacije ili može iskoristiti elektroniku uređaja kako bi poslao signal za otvaranje vrata iako uređaju nije predstavljena biometrijska karakteristika.

Sustav se od ovakve vrste napada može osigurati tako što će se napraviti fizička zaštita uređaja, ugraditi videonadzor te redovito održavati uređaj.

5.2.4. Zloupotreba ovlasti

Napadi osoblja na biometrijski sustav predstavljaju unutarnju prijetnju sigurnosti jer uključuju zloupotrebu ovlasti ili privilegija od strane pojedinaca koji imaju legitimni pristup sustavu. Nekoliko primjera takvih napada navedeno je u nastavku rada.

Zlonamjerni administrator baze podataka mijenja poslovna pravila, lažno označavajući nekoga kao osobu koja se ne mora identificirati na sustav ili zlonamjerni administrator zamjenjuje prag i omogućava napadaču da uđe u sustav [12].

Još jedan primjer zloupotrebe ovlasti je da zaposlenik, koji ima ovlasti za pristup skladištu, koristi biometrijski sustav za autentifikaciju pri ulasku u skladište. Zatim taj zaposlenik zloupotrebljava svoje ovlasti da omogući pristup skladištu osobama koje nemaju ovlasti ili čak kriminalnim subjektima, deaktivira biometrijski sustav kako bi omogućio pristup bez biometrijske autentifikacije ili pak zloupotrebljava biometrijski sustav kako bi pristupio skladištu tijekom neovlaštenih vremena ili krao inventar.

Kako bi se spriječila ova vrsta napada osoblju treba dodijeliti samo one ovlasti koje su im potrebne za obavljanje njihovih zadataka. Dodatno, treba osigurati da osoblje ne može mijenjati postavke biometrijskog sustava ili deaktivirati ga bez odobrenja. Također, osoblje treba biti educirano o etičkim i sigurnosnim aspektima korištenja biometrijskih sustava te svjesno posljedica zloupotrebe pristupa.

5.3. Standardi u biometriji

Biometrija se temelji na različitim standardima i smjernicama kako bi osigurala interoperabilnost, sigurnost i kvalitetu biometrijskih sustava. U nastavku su navedeni neki od ključnih standarda u biometriji.

- ISO/IEC 19794-1 i 19794-2: Ovi standardi definiraju formate za razmjenu biometrijskih podataka, uključujući otiske prstiju i skeniranja lica. Oni osiguravaju konzistentno kodiranje i formatiranje biometrijskih podataka za razmjenu između različitih sustava [13].

- ISO/IEC 19785: Ovaj standard definira općenite koncepte i terminologiju u biometriji te pruža smjernice za upravljanje biometrijskim informacijama [14].
- ISO/IEC 24745: Ovaj standard specifično se odnosi na zaštitu privatnosti i sigurnost biometrijskih podataka, uključujući smjernice za kriptografiju i upravljanje ključevima [14].
- SO/IEC 29109: Ovaj standard definira zahtjeve za upotrebu biometrijskih podataka u elektroničkom identitetu, uključujući smjernice za upravljanje i zaštitu biometrijskih podataka u takvim sustavima [14].
- Biometric Data Interchange Formats (BioAPI): Ovo je međunarodni standard za interakciju između biometrijskih uređaja i aplikacija. Omogućava integraciju različitih biometrijskih uređaja u istu infrastrukturu [14].

Ovi standardi igraju ključnu ulogu u osiguravanju da biometrijski sustavi budu pouzdani, interoperabilni i usklađeni sa zakonima i regulacijama o privatnosti i sigurnosti podataka. Iako se standardi razvijaju i mijenjaju tijekom vremena kako bi odražavali nove tehnološke i sigurnosne izazove, pridržavanje tih standarda od strane tvoraca biometrijskih sustava izuzetno je važno.

6. Sigurnosne smjernice

U prethodnom dijelu ovog rada objašnjeno je što je biometrija te kako funkcioniraju biometrijski sustavi. Velik naglasak stavljen je upravo na sigurnost rada takvih sustava zbog područja i svrhe njihovog korištenja. Pri izradi bilo kojeg biometrijskog sustava potrebno je izraditi sigurnosne smjernice za izradu biometrijskih sustava koje se trebaju se prilagoditi konkretnim potrebama i kontekstu svakog projekta. Na temelju prije navedenih točaka ranjivosti i mogućih napada u nastavku rada biti će navedene sigurnosne smjernice za izgradnju biometrijskog sustava i ideja je da se njihovim korištenjem smanji broj ranjivosti i poveća sigurnost.

- Identifikacija točaka ranjivosti biometrijskog sustava: Potrebno je utvrditi za što će se navedeni sustav koristiti i koji su njegovi elementi te identificirati moguće točke ranjivosti da bi se na samom početku istima posvetilo više pažnje i izradilo više sigurnosnih mjera u tim područjima.
- Zaštita biometrijskih podataka: Biometrijski sustavi često se koriste u razne sigurnosne svrhe, pa su tako i samo podaci koji kolaju unutar sustava vrlo osjetljivi i privatni. Bitan faktor u sigurnosti svakog biometrijskog sustava jest zaštita podataka.
  Za kvalitetnu zaštitu podataka može se koristiti biometrijski kripto sustav koji kombinira biometriju i kriptografiju te koristi prednosti oba područja za što bolju enkripciju podataka. Funkcionira na način da se uz svaki predložak u bazi podataka generira i ključ za enkripciju istog [13].
- Zaštita od lažnih karakteristika: U današnje vrijeme vrlo je lako simulirati ili lažirati razne biometrijske karakteristike te kako bi zaštitili sustav potrebno je ugraditi dodatne sigurnosne mehanizme za detekciju lažnih uzoraka. Takvi mehanizmi mogu uključivati sustave za prepoznavanje živosti i sustave koji analiziraju okolinu i dinamičko ponašanje prilikom uzimanja biometrijskog uzorka.
- Više faktorska autentifikacija: Kako bi se povećala sigurnost sustava preporuča se pristupati izradi multimodalnog biometrijskog sustava kada god je moguće jer ovakvi sustavi koriste više od jedne karakteristike za identifikaciju u autentifikaciju pa samim time i povećavaju sigurnost.
- Zaštita od hakerskih napada: Prilikom izgradnje biometrijskog sustava potrebno je uzeti u obzir da taj sustav može biti meta hakerskih napada. Kako bi se osigurali od ove vrste napada, osim enkripcije podataka prilikom prijenosa i pohrane, potrebno je implementirati dobre kontrole pristupa, nadzirati aktivnosti korisnika sustava te sustav

redovito testirati na moguće hakerske napade i po potrebama raditi zakrpe sustava i česta ažuriranja.

- Zaštita uređaja: Fizički uređaji poput senzora i računala (servera) sastavni su dio svakog biometrijskog sustava i u smislu povećanja sigurnosti njih je također potrebno prikladno zaštititi. Kako bi ovi uređaji bili zaštićeni od neovlaštenog pristupa potrebno ih je, na primjer, postaviti u zaštitne kutije (senzori) i na teško dostupna mjesta (računala). Isto tako učinkovit način zaštite fizičke imovine je instalacija sustava video nadzora. Na kraju, kako bi se osiguralo da ne dođe do kvara uređaja, potrebno je redovito održavati iste.
- Implementacija razina pristupa i uloga: Potrebno je u sustavu odrediti uloge poput administratora, moderatora, korisnika i slično kako bi svaka osoba koja koristi biometrijski sustav imala pristup samo onim podacima koji su joj potrebni i paziti da pristup ključnim podacima imaju samo odgovorne i za to osposobljene osobe. Edukacija svih korisnika sustava je vrlo poželjna kako bi se izbjegao faktor ljudske greške što je više moguće.
- Korištenje biometrijskih standarda: Kako bi se osigurala interoperabilnost, sigurnost i kvaliteta biometrijskih sustava potrebno se pridržavati standarda u biometriji koji opisuju načine komunikacije sustava i razmjene podataka, ali i propisuju etičke smjernice u smislu prikupljanja i korištenja privatnih podataka.

Ove smjernice pomažu u izgradnji biometrijskog sustava koji je otporan na različite napade i osiguravaju sigurnost biometrijskih podataka i korisnika. Važno je pridržavati se najboljih praksi sigurnosti i redovito pratiti promjene u sigurnosnom okruženju kako bi se održala sigurnost biometrijskog sustava.

7. Zaključak

U ovom završnom radu, detaljno su istražene i analizirane sigurnosne smjernice za izradu biometrijskih sustava. Biometrija je postala neizostavna tehnologija u mnogim aplikacijama, od kontrole pristupa i mobilnih uređaja do financijskih transakcija i zdravstvene skrbi. No, s porastom upotrebe biometrije, pojavljuju se i sve veći izazovi u pogledu sigurnosti i zaštite privatnosti biometrijskih podataka.

Kroz ovaj rad, razmotreni su ključni sigurnosti biometrijskih sustava, uključujući zaštitu biometrijskih podataka, kontrolu pristupa, otpornost na prijevare i etičke aspekte. Isto tako, istraženi su relevantni standardi i smjernice koje se primjenjuju u industriji biometrije.

Kroz analizu ovog primjera, dokazano jeda pravilna primjena sigurnosnih smjernica može značajno povećati sigurnost i pouzdanost biometrijskih sustava. Naglašena je važnost kontrole pristupa, enkripcije, praćenja aktivnosti korisnika i redovitog ažuriranja kako bismo se suprotstavili različitim prijetnjama sigurnosti.

Važno je napomenuti da sigurnost biometrijskih sustava nije statička, već dinamička oblast koja se razvija zajedno s tehnološkim napretkom i promjenama u prijetnjama. Stoga je kontinuirana edukacija, testiranje sigurnosti i ažuriranje smjernica ključno za očuvanje sigurnosti biometrijskih sustava u budućnosti.

Kroz ovaj rad, stečeno je dublje razumijevanje sigurnosnih izazova u biometriji i kako ih učinkovito rješavati. Ovaj rad će pružiti korisne smjernice i poticaj za daljnje istraživanje i razvoj sigurnih biometrijskih rješenja koja će osigurati pouzdanu autentifikaciju i zaštitu privatnosti korisnika. Biometrija je neosporno ključna tehnologija budućnosti, ali sigurnost mora biti njezin neodvojivi pratilac kako bi se ostvarile sve njezine prednosti.

Popis literature

[1] Anil K. Jain i Arun Ross, *Handbook of biometrics*. SAD: Springer US. 2008.

[2] A. K. Jain, A. Ross, S. Prabhakar, „An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics,* Vol. 14, No. 1, sij. 2004, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/1262027 [pristupano 29.06.2023].

[3] R. Subban i D. P. Mankame, „A Study of Biometric Approach Using Fingerprint Recognition," *Lecture Notes on Software Engineering,* Vol. 1, No. 2, svib. 2013, [Na internetu]. Dostupno: https://www.academia.edu/ [pristupano 29.06.2023].

[4] R. P. Wildes, „Iris Recognition: An Emerging Biometric Technology," *Proceedings of the IEEE*, vol. 85, no. 9, str. 1348-1363, ruj. 1997, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/628669 [pristupano 02.07.2023].

[5] Ž. Radmilović, „Biometrijska identifikacija," *Polic. sigur. (Zagreb),* broj 3-4, str. 159-180, 2008, [Na internetu]. Dostupno: https://hrcak.srce.hr/ [pristupano 02.07.2023].

[6] Neil Yager i Ted Dunestone, *Biometric System and Data Analysis Design, Evaluation, and Data Mining*. SAD: Springer US. 2009.

[7] M. O. Oloyede i G. P. Hancke, „Unimodal and Multimodal Biometric Sensing Systems: A Review," *Department of Electrical, Electronic and Computer Engineering,* str. 7541-7543, stu. 2016, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/7580649 [pristupano 03.07.2023].

[8] Vandana i N. Kaur, „A Study of Biometric Identification and Verification System," *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, str. 60-64, 2021, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/9404735 [pristupano 07.07.2023].

[9] P. J. Phillips, A. Martin, C. L. Wilson i M. Przybocki, „An Introduction to Evaluating Biometric Systems," *National Institute of Standards and Technology*, str. 56-63, velj. 2000, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/820040 [pristupano 07.07.2023].

[10] P. Ambaktal, „Security of biometric authentication systems," *21st Computer Science Seminar*, 2005, [Na internetu]. Dostupno: https://citeseerx.ist.psu.edu/ [pristupano 12.07.2023].

[11] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov i J. Yearwood, „Protection of Privacy in Biometric Data,“ *IEEE access*, str. 882-889, velj. 2016, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/abstract/document/7420576 [pristupano 12.07.2023].

[12] Z. Sirotić, „Biometrijski sustavi – greške i ranjivosti,“ *Istra informatički inženjering d.o.o., Pula*, [Na internetu]. Dostupno: http://www.istratech.hr/wp-content/uploads/2010/12/hroug2010.pdf [pristupano 23.07.2023].

[13] R. Jain i C. Kant, „Attacks on Biometric Systems: An Overview*,“ International Journal of Advances in Scientific Research,* str. 283-288, 2015, [Na internetu]. Dostupno: https://pdfs.semanticscholar.org/ [pristupano 08.09.2023.]

[14] M. Trikoš, I. Tot, J. Bajčetić, K. Lalović, B. Jovanović i D. Bogićević, "Biometric Security Standardization," *2019 Zooming Innovation in Consumer Technologies Conference (ZINC)*, str. 17-20, 2019, [Na internetu]. Dostupno: https://ieeexplore.ieee.org/document/8769419 [pristupano 25.07.2023].

Popis slika