Problem sigurnosti i privatnosti u biometrijskoj identifikaciji

Saghir, Tarek

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Tarek Saghir

PROBLEM SIGURNOSTI I PRIVATNOSTI U BIOMETRIJSKOJ IDENTIFIKACIJI

DIPLOMSKI RAD

Varaždin, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Tarek Saghir

Matični broj: 45256/16–R

Studij: Organizacija poslovnih sustava

PROBLEM SIGURNOSTI I PRIVATNOSTI U BIOMETRIJSKOJ IDENTIFIKACIJI

DIPLOMSKI RAD

Mentorica:

Doc. dr. sc. Petra Grd

Varaždin, srpanj 2018.

Tarek Saghir

Izjava o izvornosti

Izjavljujem da je moj diplomski 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

Za početak, u diplomskom radu detaljnije će biti opisano što je to zapravo biometrija, koliko je razvijena do danas te koji su to osnovni pojmovi koje čitatelj mora znati kako bi razumio u cijelosti o čemu se piše u ovom radu.

Svakodnevno, tehnologija nadmašuje očekivanja i standarde koji su postavljeni kod korisnika raznoraznih uređaja. Novosti u tehnologiji javljaju se svakog dana te zbog toga biometrija više ne bi smjela biti strani pojam svakodnevnom korisniku pametnih telefona ili prijenosnih računala. U današnje vrijeme većina novijih uređaja koristi biometrijske karakteristike za verifikaciju korisnika uređaja te pristup uređaju. Najpopularnije biometrijske karakteristike koje uređaji koriste su otisak prsta te prepoznavanje lica korisnika uređaja. Te vrste verifikacije i identifikacije korisniku olakšavaju korištenje uređaja, ali s druge strane pojavljuje se problem privatnosti. Otisak prsta i izgled lica korisnika su osobni podaci koji su vrlo osjetljivi. Ti podaci spremaju se na uređaje korisnika pa se postavlja pitanje koja je razina zaštite osobnih podataka. Ukoliko dođe do neželjenog pristupa uređaju od treće strane, kolika je vjerojatnost da će treća strana moći kompromitirati osobne podatke korisnika.

Iz navedenih činjenica može se identificirati problem sigurnosti i privatnosti biometrijskih podataka koji se koriste za identifikaciju što je ujedno i tema ovog diplomskog rada. Nakon utvrđivanja osnovnih pojmova koji se koriste u biometriji, elaboracije problema sigurnosti i privatnosti koji se javljaju u današnje vrijeme prilikom korištenja biometrije biti će prikazan praktičan rad. Za praktičan rad odabrana su dva operacijska sustava OS X i Android nad kojima će se vršiti istraživanje i analiza sigurnosti i zaštite privatnih podataka. Analizom tih operacijskih sustava doći će se do zaključka koja organizacija više pazi na osobne podatke svojih korisnika. Istražiti će se gdje su osobni podaci spremljeni, kolika je njihova razina sigurnosti te koje su mane i prednosti korištenja operacijskog sustava OS X te operacijskog sustava Android. Na kraju provest će se anketa od deset pitanja gdje će se steći uvid u to koliko korisnici pametnih mobilnih uređaja imaju povjerenja korištenje biometrijskih karakteristika umjesto lozinka te koliko imaju povjerenja u velike organizacije koje čuvaju spremljene njihove biometrijske karakteristike na uređajima.

Ključne riječi: sigurnost, biometrija, privatnost, apple, android

Sadržaj

1. Uvod

U današnje vrijeme više ne postoji privatnost. Nalazimo se u vremenu kada svi koriste društvene mreže i objavljuju informacije i podatke o svojem svakodnevnom životu. Te informacije distribuirane su preko fotografija, opisa osobnih podataka na društvenim mrežama, koji su njihovi privatni interesi i zanimacije, itd. Većina ljudi nije svjesna koliko informacija o svom privatnom životu dijele preko društvenih mreža misleći da ih dijele sa svojim „prijateljima“, a zapravo služe kao golema baza podataka koju koriste veliki marketinški lanci kako bi plasirali svoje reklame. Kako ne bi bilo zabune, društvene mreže imaju određenu politiku o zaštiti podataka, ali zna li se točan broj svakodnevnih korisnika koji detaljno pročitaju svu dokumentaciju uvjeta pružanja usluga? Ta dokumentacija mora biti prihvaćena prilikom registracije i ona je osiguranje pružatelju usluga da sa vašim podacima može činiti sve što je u skladu s prihvaćenim pravilima.

Jednostavnim objavljivanjem svoje slike na društvenim mrežama korisnik narušava svoju privatnost. Osim što je narušio privatnost, otkrio je jednu od svojih biometrijskih karakteristika, izgled lica. Danas, napredniji mobilni uređaji nude mogućnost identifikacije korisnika preko prepoznavanja crta lica. Zamislimo slučaj da osoba od interesa koristi društvene mreže na kojima svakodnevno dijeli svoje privatne fotografije. Ako je ta osoba cilj za kompromitaciju ili otkrivanje nedostupnih informacija, što je sve potrebno da zločinac dođe u posjed mobilnog uređaja te uz pomoć rekonstrukcije izgleda lica dobije pristup privatnim podacima i informacijama.

No ne predstavljaju samo društvene mreže problem sigurnosti i privatnosti. Svakodnevno tisuće korisnika koristi pametne mobilne uređaje za koje se svakodnevno izrađuje tisuće mobilnih aplikacija. Prilikom instalacija mobilnih aplikacija korisnik mora dati svoju suglasnost da dopušta pristup aplikacije privatnim podacima koji se nalaze na mobilnom uređaju. Ovdje se također postavlja pitanje koliko je zapravo korisnika pročitalo uvjete pružanja usluga i na što je sve korisnik pristao prilikom davanja suglasnosti. Jesu li te aplikacije malicioznih namjera ili postoje sigurnosni propusti? Kao što je već spomenuto, noviji pametni mobilni uređaju nude mogućnost identifikacije pomoću biometrijskih karakteristika. Može li treća strana malicioznim namjerama kroz mobilne aplikacije doći do privatnih podataka korisnika mobilnih uređaja te njegovih biometrijskih karakteristika koje su spremljene na mobilnim uređajima? Nadalje, 2017. godine u Kini se pojavljuje način plaćanja za naručenu hranu pomoću biometrijske karakteristike, izgleda lica.

Ali babin[1] suradnik *Ant Financial* je pokrenuo *'smile to pay'* servis u Hangzhou u jednom od KFC[2] restorana. U tekstu se navodi, kada klijent obavi svoju narudžbu plaćanje može obaviti jednostavnim osmijehom na licu. Na blagajni, stoji 3D kamera koja pomoću tehnologije prepoznavanja crta lica potvrđuje identitet osobe, a za dodatnu sigurnost identifikacija se može potvrditi preko verifikacije broja telefona. [1]

Takva mogućnost plaćanja pojednostavljuje i ubrzava proces. Nestaje potreba za radnikom, odnosno, blagajnikom što znači smanjenje troškova za vlasnika. S druge strane, postavlja se pitanje sigurnosti i privatnosti podataka klijenata. Garantira li vlasnik za sigurnost podataka klijenata, garantira li da se prilikom verifikacije identiteta njihov identitet ili biometrijske karakteristike ne spremaju u bazu podataka?

Navedeni primjeri, pitanja i problemi predstavljaju i sam naziv teme diplomskog rada, a to je problem sigurnosti i privatnosti u biometrijskoj identifikaciji. U ovome radu bit će identificirani osnovni pojmovi vezani uz biometriju te će se detaljno proučiti koja je povezanost sigurnosti i privatnosti s biometrijskom identifikacijom te kakvi se sve problemi mogu pojaviti.

Identifikacija ili verifikacija

Tijekom čitanja rada više puta su će se spominjati pojmovi identifikacije i verifikacije. Na prvi pogled identifikacija i verifikacija, ukoliko se ne stave u kontekst, može se učiniti pogreška misleći da su njihova značenja ista. Oba pojma koriste se kada se trebaju utvrditi biometrijske karakteristike osobe koja izvršava radnju prijave u sustav. Biometrijske karakteristike se uspoređuju sa onima iz baze podataka kod identifikacije i verifikacije, ali proces uspoređivanja podataka se razlikuje.

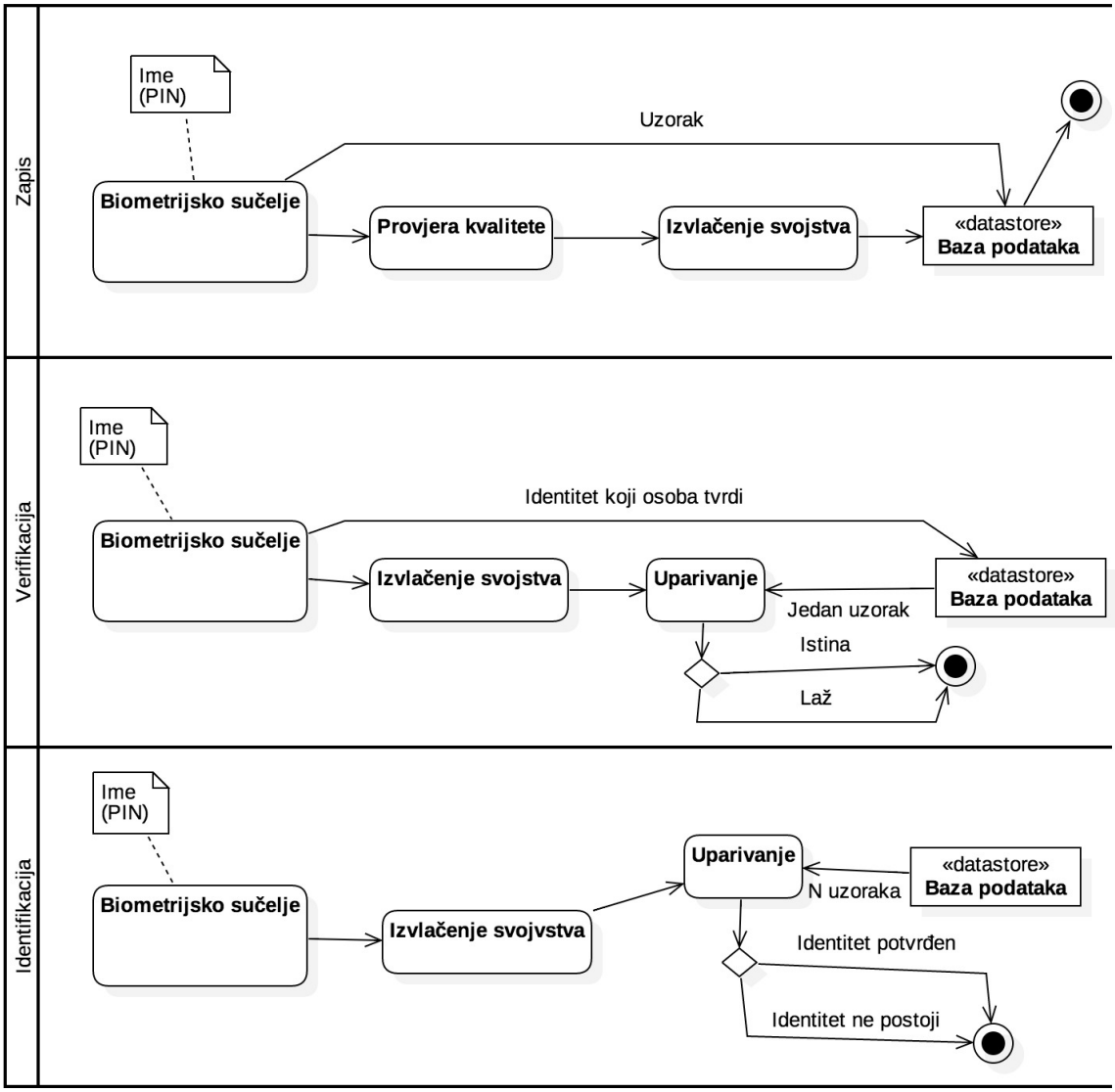
Kada je sustav u načinu verifikacije, tada se identitet osobe validira na način da se uspoređuju zabilježeni biometrijski podaci sa uzorcima tih istih podataka koji su spremljeni u bazi podataka. U takvom sustavu, ukoliko osoba želi biti prepoznata, obično uz PIN, korisničko ime ili pametnu karticu, sustav provodi jedan-na-jedan usporedbu te utvrđuje je li ta osoba ono što tvrdi da jest (npr. „Pripadaju li priloženi biometrijski podaci Ivanu?“). Verifikacija se koristi za pozitivno prepoznavanje, što znači da je cilj sprječavanje korištenja istog identiteta od strane više osoba. [2]

Ako je sustav u načinu identifikacije tada se vrši proces pretraživanja uzoraka svih korisnika u bazi podataka kako bi se utvrdila odgovarajuća osoba. Za razliku od verifikacije ovdje se vrši usporedba jedan-na-više kako bi se utvrdio identitet osobe (ili neizvršenje ako ta osoba nije zapisana u bazi podataka sustava). Ovdje se postavlja pitanje „Čiji su priloženi biometrijski podaci?“. Identifikacija je važna komponenta u aplikacijama negativnog

[1] *Ali baba* – Kineska e-trgovina koje pokriva internacionalno i kinesko tržište
[2] *KFC – Kentucky fried chicken* američki restoran za brzu hranu

prepoznavanje gdje sustav utvrđuje je li osoba (implicitno ili eksplicitno) ono što tvrdi da nije. Svrha sustava negativnog prepoznavanja jest sprječavanje osobe da koristi više identiteta. [2]

Da bi sustav uopće mogao izvršiti identifikaciju ili verifikaciju mora se izvršiti zapis biometrijskih podataka osobe koja se prijavljuje u sustav. Zapis se u pravilu događa samo jednom, a to je prvi puta kada se osoba prijavljuje u sustav jer njezini podaci ne postoje u bazi podataka. Postoje krajnji slučajevi kada sustav odbija podatke zbog slabe kvalitete ili ukoliko su podaci osobe izbrisani iz baze podataka pa mora izvršiti ponovan zapis biometrijskih podataka. Sva tri pojma vizualno su prikazani na slici sedam kao blok dijagram. Slika prikazuje što se događa u sustavu kada osoba vrši zapis svojih biometrijskih podatka te kada osoba prilaže svoje biometrijske podatke, a u sustavu se izvršava identifikacija ili verifikacija.



Slika 1. Blok dijagram zapisa, identifikacije i verifikacije (Izvor: [6], str. 34)

Kao zaključak za sva tri procesa zapisa, identifikacije i verifikacije, koji su prikazani na slici sedam, glasi da zapis osobe u sustav kreira poveznicu između identifikacije i verifikacije. Zapis kreira asocijaciju između identiteta i njegovih biometrijskih karakteristika. Prilikom procesa verifikacije, zapisana osoba tvrdi svoj identitet, a sustav verificira autentičnost tvrdnje koja je temeljena na biometrijskim značajkama. Sustav identifikacije zapisane osobe u bazi podataka identificira prema biometrijskim karakteristikama bez potrebe da osoba tvrdi svoj identitet. [6]

Na kraju, kada se razumije razlika pojmova identifikacije i verifikacije, u daljnjem tekstu biti će spojeni u jedan pojam koji glasi prepoznavanje.

2. Metode i tehnike rada

Diplomski rad je napisan tako da se prikupljala i analizirala za odabranu temu relevantna literatura. Većina literature su knjige u digitalnom obliku, a mogu se pronaći neke web stranice, zakonodavna uredba (GDPR) te službena izvješća od velikih organizacija kao što su Apple i Google (Android).

Za praktičan dio rada koristila su se službena izvješća o sigurnosti Apple i Android operacijskih sustava. Analizom dokumentacije izdvojili su se najvažniji dijelovi koji se odnose na biometriju te sigurnost podataka i privatnost samog korisnika.

Na kraju, izradila se online anketa u kojoj su bila postavljena osam pitanja povezana s biometrijom i općenitim znanjem korisnika na koji način se čuvaju njihovi biometrijski podaci te vjeruju li operacijskih sustavima da sigurno čuvaju njihove podatke. Odgovor na pitanje se mjeri brojevima od 1 do 5 gdje ispitanik odabire slaže li se sa odgovorom ili ne slaže. Rezultati su prikazani u obliku dijagrama gdje se vidi postotak ispitanika koji su dali za pojedini odgovor. Rezultati ankete su korišteni kako bi napravila usporedba na koji način ljudi percipiraju korištenje biometrijske karakteristike u zamjenu za lozinki, koliko su upoznati sa sigurnošću, odnosno, na koji način su njihovi biometrijski podaci zaštićeni.

3. Što je biometrija?

Svaka osoba ima svoje određene karakteristike. Te karakteristike mogu biti ponašanje, izgled, osobnost, način kretanja, govorne mane, glas, gestikulacije, navike. Karakteristike svaku osobu čine posebnom te na taj način čini njezin identitet. Pomoću tog identiteta osoba može biti identificirana ili verificirana. Identifikacija se koristi kako bi se utvrdio ili ovjerio identitet osobe koja želi pristup sigurnom sustavu ili izvršiti neku radnju kao što je izvršavanje transakcije, prijelaz državnih granica, legitimacije, pristup zatvorenom i osiguranom sustavu, itd.

Kako se postiže sigurnost? Korištenjem tri vrste ovjeravanja autentičnosti: [3]

1. Nešto što znaš
    - Lozinka, PIN, dio osobne informacije (majčino srednje ime)
2. Nešto što imaš
    - Ključ kartica, *smart* kartica, *token*
3. Nešto što jesi
    - Biometrija

Biometrija mjeri individualnu jedinstvenost fizičkih ili bihevioralnih karakteristika osobe kako bi se prepoznao ili autenticirao njezin identitet. Fizička biometrija se odnosi na otiske prstiju, ruke, geometriju dlanova, očnu mrežnicu ili obrise i crte lica. S druge strane, bihevioralna biometrija odnosi se na potpis osobe, glas (koji ujedno ima i fizičke karakteristike), hod te kakvim potezom pisala se osoba potpisuje. [3]

Biometrija je znanost utvrđivanja identiteta osobe. Utvrđivanje identiteta bazirano je na fizičkim, kemijskim ili bihevioralnim atributima osobe. Uloga biometrije u modernom društvu ojačana je zbog pojave potrebe sustava upravljanja identitetom velikih razmjera. Funkcionalnost takvih sustava oslanja se na ispravno utvrđivanje identiteta jedinstvene osobe u odnosu na ostale osobe koje se prijavljuju u sustav. Primjeri takvih sustava su dijeljenje mrežnih resursa, odobravanje pristupa strogo čuvanim ustanovama, izvršavanje financijskih transakcija ili ukrcavanje na let aviona. Krajnji zadatak sustava upravljanja identitetom je utvrđivanje ili verifikacija identiteta osobe. [2]

Također, kako bi se spriječile neovlaštene prijave u sustave, odnosno, kako bi se spriječili neovlašteni ulasci u prostorije strogo čuvanih ustanova, koriste se sustavi upravljanja identitetom. Korištenjem sustava povećava se sigurnost, a implementacija biometrije kao znanost utvrđivanja identiteta sigurnost podiže na sljedeću razinu. Biometrija sa sigurnošću može odrediti identitet osobe u sustavu te se dalje može koristiti za izvršavanje radnji. Razlog

toga je sve učestalije korištenje biometrije u aplikacijama i na uređajima. Sa strane korisnika korištenjem biometrije olakšava se proces korištenja uređaja, plaćanja računa pa čak i pristupa osiguranim ustanovama. Više nije potrebno koristiti ključeve, pamtiti lozinke i email za prijavu u aplikaciju, već se za prijavu u sustav, potvrdu plaćanja ili otvaranje vrata koristi, na primjer, otisak prsta. Nadalje, iz navedenih primjera možemo zaključiti da pristup na kojima se koristi biometrija može biti virtualan ili fizički.

3.1. Karakteristike

Svaki sustav koji koristi biometriju za verifikaciju i identifikaciju osobe ima svoju bazu podataka u kojoj su spremljeni podaci sa kojima se radi usporedba. Da bi se mogla vršiti usporedba u bazi podataka moraju biti spremljene karakteristike koje su jedinstvene.

Brojne biometrijske karakteristike mogu biti prepoznate u prvoj fazi procesiranja. S druge strane, ako se koristi automatsko prepoznavanje te automatska usporedba sa podacima koji su spremljeni u bazi podataka, bitno je da biometrijske karakteristike zadovoljavaju sljedeće karakteristike: [4]

1. **Univerzalnost**
   Svaka osoba mora posjedovati atribut ili karakteristiku koja je prepoznatljiva isključujući bolest ili nesreću.

2. **Invarijentnost svojstava**
   Karakteristika treba biti konstanta u smislu da je nepromjenjiva iako prođe duži period vremena. Takav atribut ne smije biti baziran prema godinama ili prema nekoj bolesti.

3. **Mjerljivost**
   Svojstva trebaju biti prepoznata bez vremena čekanja te moraju biti jednostavna kako bi se moglo vršiti pasivno prikupljanje podataka.

4. **Jedinstvenost**
   Svaki izraz atributa mora biti jedinstven individualnoj osobi. Karakteristika treba imati jedinstvena svojstva kako bi se osobe mogle razlikovati. Visina, težina, kosa te boja očiju su atributi koji su jedinstveni u smislu mjerenja, ali ne nude dovoljno razlike koje bi se mogle koristiti za bilo što drugo osim kategorizacije.

5. **Prihvatljivost**

   Zapažanje karakteristike mora biti primjenljivo na veliki postotak populacije. Isključene su invazivne tehnologije, odnosno tehnologije koje zahtijevaju dio tijela kao primjerak ili koje krnje ljudsko tijelo.

6. **Reducibilnost**

   Preuzeti podaci karakteristike moraju biti u mogućnosti svesti se na razinu datoteke kako bi bilo lakše koristiti te podatke.

7. **Pouzdanost i otpornost na promjene**

   Atributi ne bi smjeli dopustiti mogućnost maskiranja ili manipuliranja. Proces treba osigurati visoku pouzdanost i obnovljivost.

8. **Privatnost**

   Proces preuzimanja podataka karakteristike ne smiju narušavati privatnost osobe.

9. **Usporedivost**

   Atribut mora imati mogućnost da na digitalnoj razini bude usporediv sa ostalima.

10. **Neponovljivost**

    Atribut ne smije biti ponovljiv u bilo kojem smislu. Što je manja mogućnost reprodukcije atributa to je veća šansa da je karakteristika autoritativna.

Navedene karakteristike postoje kao izravne smjernice određivanja biometrijske karakteristike koja će biti primjenljiva na većinu populacije. Za tu biometrijsku karakteristiku postoji sigurnost da će biti jedinstvena, neće moći biti promijenjena, biti će pouzdana i sigurna za korištenje u aplikacijama ili za pristup osiguranim prostorijama. Ono što je najbitnije jest da postoji sigurna usporedba sa ostalim biometrijskim karakteristikama na digitalnoj razini. To omogućuje sigurnu verifikaciju i identifikaciju osobe. Karakteristika broj osam navodi da privatnost osobe od koje se preuzimaju podaci ne smije biti ugrožena. S druge strane, s povećavanjem infrastruktura koje koriste sustav za automatsku identifikaciju raste i zabrinutost narušavanja privatnosti osobe u smislu da svaka osoba ima pravno na anonimnost.

3.2. Biometrijske karakteristike

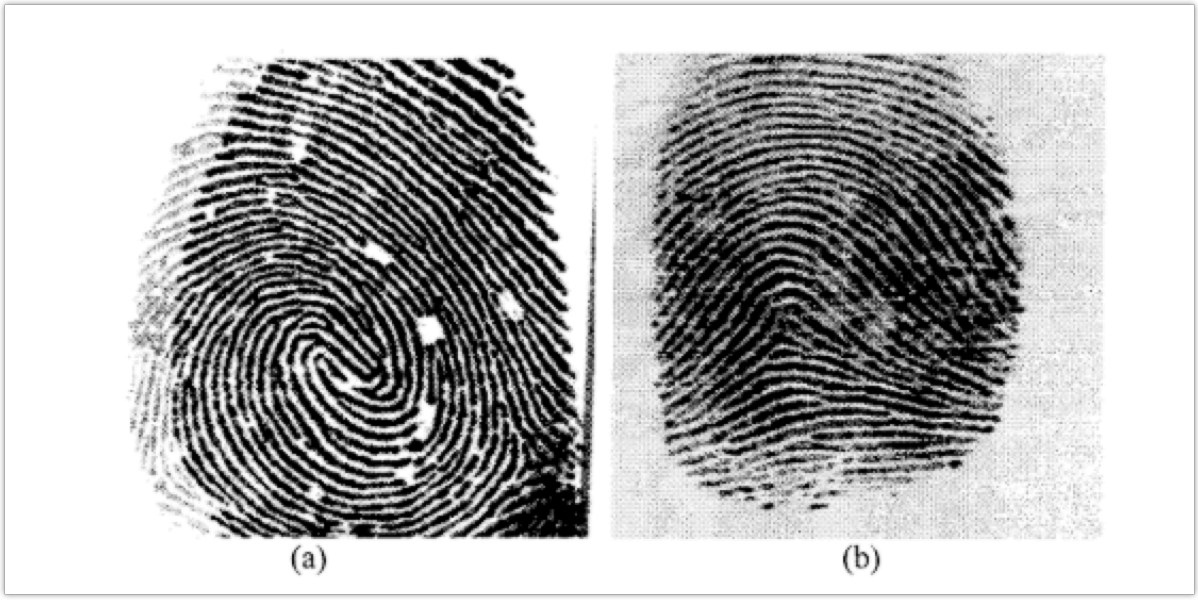
Nakon utvrđivanja smjernica za određivanje biometrijskih karakteristika, one su prepoznate kao jedinstvene te primjenjive na većinu populacije. Time, moguća je verifikacija i pouzdana identifikacija osobe.

3.2.1. Otisak prsta

Najpoznatija biometrijska karakteristika široj javnosti, dio je čovjekova tijela, a nalazi se na prstima ruke. Razvoj otiska prsta ovisi o početnim uvjetima embrijskog stadija razvoja. Vjeruje se da je svaki otisak jedinstven za svaku pojedinu osobu. Uzimanje uzorka otiska prstiju najstarija je biometrijska tehnologija koja se koristi u forenzici. Najviše se koristi u kriminalnim istragama pa dolazi do povezanosti sa kriminalom. [5]

Otisak prsta uzima se na dva načina: [5]

1. Skeniranje utiska prsta od tinte na papiru
2. Uređaj za trenutačno skeniranje otiska prsta



Slika 2. Primjer otiska prsta (Izvor: [5], 2006.)

Ovim tvrdnjama može se postaviti teza da svaki čovjek kada je rođen, na svojim prstima dobiva jedinstvenu oznaku (otisak prsta) preko koje može biti identificiran. Takva biometrijska karakteristika, kada se prebaci u digitalni oblik služi kao pouzdano svojstvo za izvršavanje identifikacije osobe. Uzimajući u obzir da osoba stari ili postoji mogućnost događaja ozljede na

prstu, identifikacija neće biti potvrđena sa sto postotnom sigurnošću. Otisak prsta je toliko jedinstven da su samo glavna svojstva otiska prsta dovoljna da u većim postocima potvrde podudarnost sa primjerom u bazi podataka s kojim se uspoređuje.

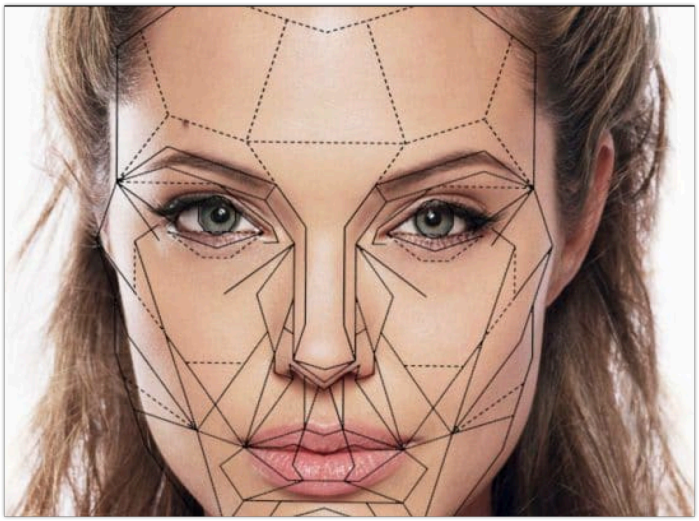
Postoji velik broj uređaja koji koriste otisak prsta kao biometrijsku karakteristiku za verifikaciju korisnika, više od bilo koje druge biometrijske karakteristike. Kroz vrijeme cijena takvih uređaja pada te njihovo korištenje postaje sve prihvatljivije. Verifikacija otiska prsta može biti dobar odabir kod kućnih sustava te sustava u kontroliranim uvjetima. Takvo korištenje ima smisla samo kada se korisnicima prije korištenja pojasne pravila korištenja. Nije iznenađujuće da takav sustav koriste aplikacije radne stanice zbog relativno niskih troškova korištenja, malih dimenzija uređaja te lakog integriranja. [3]

Autori [3] su tvrdili da će korištenje otiska prsta kao verifikacija korisnika biti sve više raširena. Zbog niskih troškova takvi uređaji mogu biti pronađeni kao primjer u bolničkim ustanovama, nuklearnim ustanovama, odnosno ustanovama posebnog pristupa. U komercijalne svrhe, takvi uređaji su postupno bili integrirani u prijenosna računala, ali nisu bili toliko prepoznati. U današnje vrijeme, pojavom pametnih mobilnih uređaja, Internet bankarstva, e-trgovina aplikacija, verifikacija korisnika usporedbom otiska prsta postaje glavno svojstvo koje se koristi svugdje.

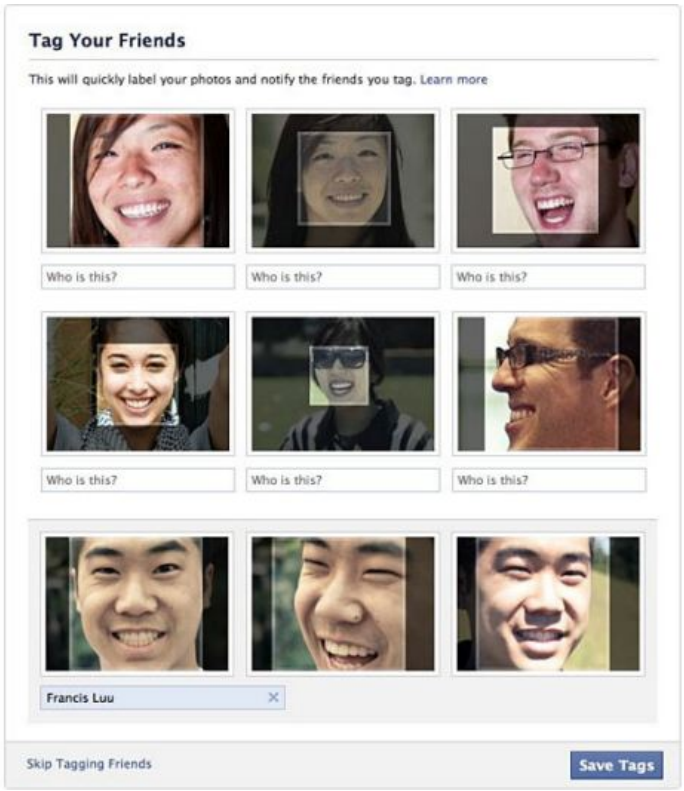
3.2.2. Lice

Lice je jedna od najprihvatljivijih biometrijskih karakteristika jer je jedna od uobičajenijih metoda identifikacije kod ljudskih vizualnih interakcija. Također, metoda prikupljanja slike lica nije nametljiva. [5]

Prepoznavanje lica se izvršava tako da se uspoređuje statički, kontrolirani, cijeli portret lica sa prednje strane. Dva glavna zadatka kod prepoznavanja lica su: (1) lokacija lica, (2) prepoznavanje lica. Budući da je pozadina kontrolirana lokacija lica ne predstavlja problem. Prepoznavanje lica pronalazi sličnosti lociranog lica sa spremljenim predlošcima kako bi se utvrdio identitet [5]. Aplikacija koja prepoznaje lica analizira karakteristike lica. Za to je potrebna digitalna kamera kako bi se razvila digitalna slika korisnika za autentikaciju, odnosno identifikaciju. [3]



Slika 3. Biometrijska karakteristika lica (Izvor: http://lifescodes.com/the-golden-ratio-in-human-face/, 2017.)



Slika 4. Primjer prepoznavanja lica prilikom učitavanja slika na društvenu mrežu Facebook (Izvor: http://www.dailymail.co.uk/sciencetech/article-1339112/Facebook-facial-recognition-software-suggest-friends-tagging-new-photos.html , 2010.)

Lice kao biometrijska karakteristika u zadnje vrijeme postaje sve više popularna. Danas, skoro svugdje nalaze se kamere, sigurnosni video nadzori, kamere na pametnim mobilnim uređajima. Za te uređaje postoje funkcionalnosti, softver ili aplikacije koje omogućuju prepoznavanje lica. Prepoznavanje se vrši usporedbom digitalnih slika na kojima je locirano lice sa digitalnim slikama koje su spremljene u nekoj bazi podataka. Primjeri korištenja prepoznavanja lica za širu javnost, u komercijalne svrhe, među prvima počela je koristiti društvena mreža *Facebook.* Na učitanim slikama na profilima svojih korisnika softver prepoznavanja lica vrši analizu i usporedbu crta lica sa slikama iza baze podataka. Tako, kada bi korisnik učitao novu sliku, mehanizam bi locirao sva lica na slici te bi predložio označavanje[3] svih profila kojima to lice ima najveći postotak sličnosti. S jedne strane, ta funkcionalnost je vrlo korisna kod učitavanja veće količine slika. Na učitanim slikama, ako postoji sličnost osoba sa slika sa bazom podataka spremljenih slika, korisnik će kao prijedlog dobiti sve pronađene profile. S druge strane, pojavljuje se problem privatnosti. Zbog toga, *Facebook* s pravne strane mora svojim korisnicima osigurati da će se taj softver prepoznavanja lica koristiti u ispravne svrhe, odnosno da ga on ili treća strana neće iskorištavati u zlonamjerne svrhe.

Nadalje, zbog sve razvijenijih softvera prepoznavanje lica pojavljuje se primjenjivanje istih na mjestima od sigurnosne važnosti. Zračna luka je jedna od tih mjesta. U zračnim lukama svakodnevno prolazi veliki broj ljudi kojima bi se znatno skratio red u čekanju kada bi se tim osobama automatizmom prepoznavanja lica mogao utvrditi identitet. Također, u najnovijim pametnim mobilnim uređajima tvrtke kao što su Apple i Samsung upotrebljavaju prepoznavanje lica korisnika kao način identifikacije korisnika te otključavanje uređaja za korištenje. Naime, kod uređaja obiju tvrtki znaju se javljati problemi prilikom identifikacije korisnika.

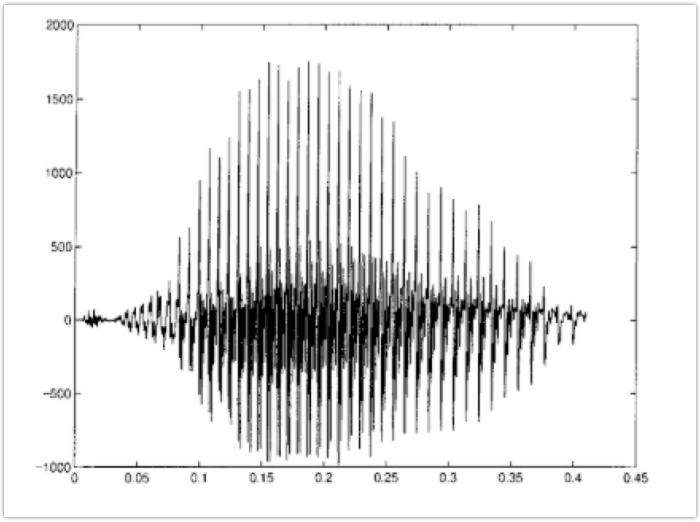
Ta forma biometrijske identifikacije je značajnije nepouzdanija od npr. otiska prsta ili skeniranja šarenice. Analiza slike se vrši na cjelokupnoj strukturi lica što funkcionira u blizini, ali što se više korisnik udaljava točnost analize se progresivno gubi. Prepoznavanje lica je veoma interesantno sa strane korisnika pa će zbog toga vrlo vjerojatno uskoro postati primarna biometrijska karakteristika. [4]

[3] Označivanje, tzv. *Tagging* – funkcionalnost na *Facebook* društvenoj mreži koja korisnicima omogućuje „označavanje“ drugih korisnika na mreži stvarajući poveznicu prema njihovim profilima.

3.2.3. Glas

Glas je individualna karakteristika pojedine osobe. Međutim, ne smatra se dovoljno jedinstvenim kako bi se izvršila sto postotna identifikacija korisnika u velikoj bazi podataka identiteta. Nadalje, glas za identifikaciju ovisi o vrsti i kvaliteti mikrofona koji snima glas, komunikacijskom kanalu, digitalizatoru karakteristika. [5]

Prepoznavanje glasa ili autentikacija glasa nije bazirana na samom prepoznavanju glasa individualne osobe već na pretvorbi zvukova u tekst kompleksnom tehnologijom. Problem kod verifikacije može se javljati prilikom lošeg zvučnog okruženja, lošoj kvaliteti mikrofona ili ne razgovijetnom govoru same individue. Prema trendovima u tehnologiji i umjetnoj inteligenciji postoji sve veća vjerojatnost da bi verifikacija osobe preko glasa postala dodatak ili zamjena za već postojeće Pinove, lozinke i korisničke račune. [3]



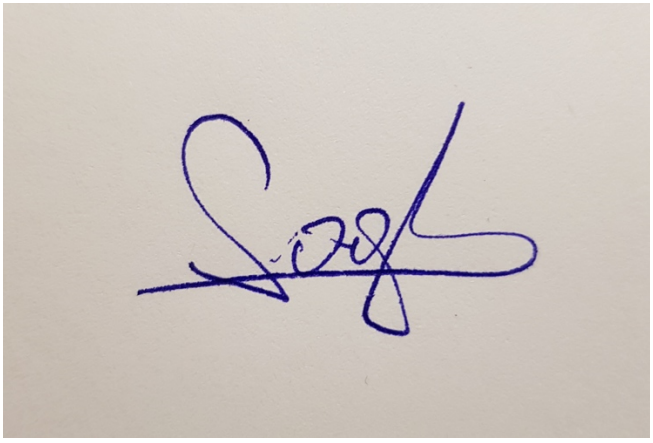
Slika 5. Signal glasa koji predstavlja primjer izgovora broja sedam na engleskom jeziku (Izvor: [5], 2006.)

3.2.4. Potpis

Čovjek od ranih godina počinje učiti čitati i pisati. Za pisanje, potrebno je puno vježbe i ispisanog teksta. Uz toliko prakse i vježbe, počinje se razvijati poseban način pisanja slova, riječi i rečenica koje može postati prepoznatljiv te se može koristiti kao biometrijska karakteristika pojedine osobe. Na temelju te biometrijske karakteristike može se izvršiti identifikacija ili verifikacija određene osobe. Kod plaćanja računa kreditnom karticom, potpisivanju ugovora ili davanju izjava, potreban je potpis. Potpisom osoba garantira za napisane stavke na dokumentu i da će, ukoliko dođe do nesuglasica, pravno odgovarati.

Verifikacija potpisa vrši se tako da se identificira način na koji osoba potpisuje svoje ime. Način pisanja kao što su brzina, pritisak pisala, oblik slova oblikuju jedinstvenost potpisa. [3]

Postoje dva pristupa kod verifikacije potpisa: (1) statički i (2) dinamički. Kod statičke verifikacije potpisa uzima se u obzir oblik i geometrija potpisa. Tipično, potpis je normaliziran na određenu veličinu te na sastavne dijelove poteza pisalom. S druge strane, kod dinamičke verifikacije potpisa uzima se u obzir brzina pisanja, brzina poteza i putanja profila potpisa. [5] Zbog navedenih atributa, potpis može spadati u kategoriju biometrijske karakteristike. Potpis se analizira u sustavu, programskim algoritmom koji provjerava sve navedene atribute. Ako netko želi krivotvoriti potpis mora znati točnu putanju potpisa, brzinu pisanja, tiskanja pisala te oblik slova, što je veoma teško.



Slika 6. Primjer vlastoručnog načina potpisa

3.2.5. Šarenica

Sljedeća po redu biometrijska karakteristika su oči. Osim što postoje različite boje očiju, ono što čini jedinstvenost oka jesu šarenice. Šarenica u optičkom smislu služi za otvaranje i zatvaranje zjenice za propusnost svjetla. Fleksibilnost omogućuju skup mišića koji čine šarenicu. Izgled šarenice je jedinstven pa kao takva spada u kategorije biometrijske karakteristike.

Identifikacija se vrši na način da se analiziraju karakteristike u tom skupu mišića koji okružuju zjenicu. Skeniranje očiju jedna je od biometrijskih karakteristika koja spada u nenametljivu skupinu. Zahtjeva kameru koja će za slikati fotografiju šarenicu, a s druge strane ne zahtjeva bliski kontakt sa osobom nad kojom se vrši identifikacija. [3]

Iako se u literaturi spominje da se očekuje napredak tehnologije i uređaja koji obavljaju verifikacija i identifikaciju preko šarenice, tehnologija nije išla u tom smjeru. Postavljanje uređaja i implementacija sustava nije zaživjela u komercijalne svrhe. Sustavi koji koriste šarenicu kao biometrijsku verifikaciju koriste se na mjestima visoke sigurnosti. Razlog korištenja na tim mjestima jest zato što je šarenica toliko jedinstvena da mogućnost pogreške iznosi jedan u deset slučajeva na sedamdeset i osmu. Također, nude preko dvjesto točaka referenca za usporedbu. Ako radimo usporedbu sa otiskom prstiju broj točaka iznosi između 60 ili 70. Izgled šarenice se ne mijenja tokom vremena, a ukoliko se odradi operacija očiju same oči ostaju nepromijenjene. [4]

3.3. Usporedba biometrijskih karakteristika

U biometrijskoj verifikaciji postoji još nekoliko biometrijskih karakteristika. Ovdje su spomenute samo neke, odnosno, one karakteristike koje su češće primijenjene u komercijalne svrhe i one o kojima najviše ovisi privatnost i sigurnost korisnika. Za lakšu usporedbu i preglednost najpopularnijih biometrijskih karakteristika izrađena je tablica usporedbe. U tablici su u stupcima navedene biometrijske karakteristike, gdje prvi stupac prikazuje po čemu su te karakteristike mjerljive. Mjerne jedinice za većinu navedenih karakteristika su: niska, srednja, visoka, vrlo visoka.

Usporedba biometrijskih karakteristika

Karakteristike	Otisak prstiju	Lice	Glas	Potpis	Šarenica	Geometrija ruke
Jednostavnost korištenja	Visoka	Srednja	Visoka	Visoka	Srednja	Niska
Uzrok pogreške	Suhoća, prljavost, staranje	Osvjetljenje, staranje, naočale, kosa	Buka, prehlada, vrijeme	Promjena potpisa	Slabo osvjetljenje	Ozljeda ruke
Točnost	Visoka	Visoka	Visoka	Visoka	Vrlo visoka	Visoka
Prihvatljivost	Srednja	Srednja	Visoka	Vrlo visoka	Srednja	Srednja
Razina sigurnosti	Visoka	Srednja	Srednja	Srednja	Vrlo visoka	Srednja
Dugoročna stabilnost	Visoka	Srednja	Srednja	Srednja	Visoka	Srednja
Potencijal za zaobilaženje	Niska	Visoka	Visoka	Visoka	Niska	Srednja

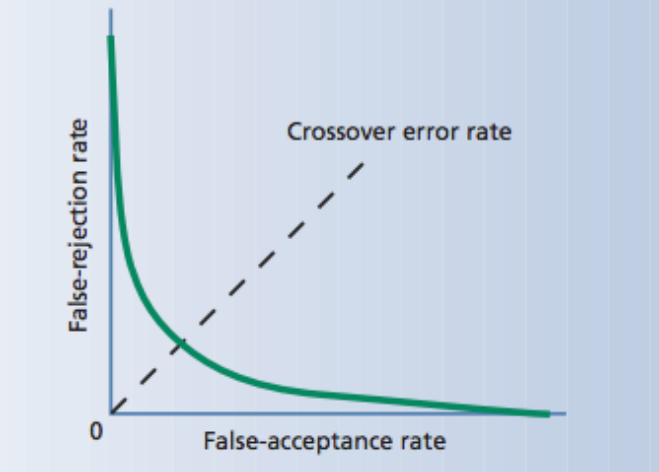
Tablica 1. Usporedba biometrijskih karakteristika (Izvor: [3] 2001., [6] 2003.)

U tablici se na organiziraniji način mogu vidjeti navedene biometrijske karakteristike koje su već opisane. Neke biometrijske karakteristike nije lako primijeniti pa se može vidjeti usporedba između lakoće korištenja i prihvatljivosti korisnika. Korisnici se većinom mogu prilagoditi ukoliko se navedene biometrijske karakteristike koriste za identifikaciju. Prema izvorima navodi se da je geometrija ruke najteža biometrijska karakteristika za korištenje. Ako se napravi usporedba sa današnjom tehnologijom može se zaključiti da to nije tako. Danas u određenim kamerama postoje senzori koji mogu odrediti osjećaje mjerenjem čovjekovog izraza lica pa tako i izračunati točnu geometriju nečije ruke. Ono što je bitno kod analize uzoraka biometrijskih karakteristika kod identifikacije jest čisti uzorak. Uzrok pogreške prikazuje koji su sve uzroci grešaka prilikom identifikacije ili verifikacije. Za svaku biometrijsku karakteristiku se poprilično sigurno može tvrditi da imaju visoku točnost, ali na točnost utječe njihova dugoročna stabilnost. Budući da čovjek stari može doći do promjene nekih dijelova biometrijskih karakteristika pa su tako najpouzdanije karakteristike za identifikaciju otisak prsta i šarenica oka. Ujedno su te dvije karakteristike i najpouzdanije, odnosno, nije lako zaobići ili

varati sustav koji koristi te karakteristike za identifikaciju. Nadalje, otisak prsta i šarenica se većinom koristi u sustavima u kojima je potrebna visoka razina sigurnosti.

Da bi se odabrala prava biometrijska karakteristika potrebno je uzeti u obzir sve navedene faktore. Na učestalost pogreške u biometrijskim podacima utječu dva faktora: vrijeme i okolišni uvjeti. [3] Kako osoba stari sukladno tome, biometrijska karakteristika se mijenja. Primjer okolišnih uvjeta može biti kada se osoba poreže na prstu ili odradi medicinsku operaciju. Ti uvjeti ne mogu se kontrolirati, a utječu na biometrijsku karakteristiku direktno tako da ostaje ožiljak. Obično, koriste se dvije metode mjerenja stope biometrijske točnosti. Stopa pogrešne prihvatljivosti *(False – acceptance rate* dalje u radu spominjano kao *FAR)* i stopa pogrešnog odbijanja *(False – rejection rate* dalje u radu spominjano kao *FRR).* Obje metode koriste se kako bi se limitirala prijava autoriziranih korisnika. [3]

Budući da su stope *FAR* i *FRR* međuzavisne, grafički su prikazane na suprotnim osima kao što možemo vidjeti na slici šest. Na njihovim osima uspoređuju se sustavi koji koriste biometrijske karakteristike za identifikaciju i verifikaciju. Sa takvim grafičkim prikazom dvije stope se mogu usporediti te odrediti njihovo križanje stope pogreške *(CER – Crossover error rate). CER* je usporediva mjerna jedinica za biometrijske uređaje i tehnologije. Što je niže linija *CERa* na grafu to je točniji i pouzdaniji biometrijski uređaj, biometrijski sustav ili biometrijska tehnologija. [3]



Slika 7. Graf križanja stope pogreški FRR i FAR (Izvor: [3] str. 32)

Na kraju, zadnje četiri karakteristike mogu se evaluirati u skupini jer su međusobno povezane. Organizacija koja bira uređaj, odnosno slaže sustav za identifikaciju temeljen na biometrijskim karakteristikama kao prvo mora uzeti u obzir dugotrajnu stabilnost te biometrijske karakteristike. Ta stabilnost odgovara na pitanja: može li ta karakteristika pratiti tehnologiju koja napreduje svakim danom, ima li zakonsku podršku, postoji li standardizacija. Zrele i standardizirane tehnologije općenito imaju jaču stabilnost. Nadalje, organizacija treba odrediti kakvu razinu sigurnosti će provoditi: nisku, srednju ili visoku. Općenito, bihevioralne

karakteristike su povezane sa niskom razinom sigurnosnih aplikacija, dok s druge strane, za visoku razinu sigurnosti koriste se fizičke biometrijske karakteristike. Uzimajući u obzir prihvatljivost biometrijske karakteristike, organizacija mora odabrati one koje nisu nametljive. Za kraj, kad su sve karakteristike uspoređene ostaje trošak koji organizacija mora platiti kako bi implementirala tu biometrijsku karakteristiku za provođenje sigurnosti. Trošak može sadržati više faktora: [3]

- Hardver za bilježenje biometrijskih karakteristika
- Količina snage za procesiranje podataka koji su spremljeni u baze podataka
- Istraživanje, implementiranje i testiranje biometrijskog sustava
- Instalacija, plaćanje implementacije za instalaciju
- Troškovi ugrađivanja, konekcija, integracija u korisnički sustav
- Gubitak produktivnosti zbog krivulje učenja
- Održavanje sustava

U literaturi [3] autori navode da se fizičke biometrijske karakteristike u većini slučajeva koriste u sustavima gdje je potrebna visoka razina sigurnosti. Ako napravimo usporedbu sa današnjom tehnologijom, kao što je već prije spomenuto, fizičke biometrijske karakteristike se već koriste u osobnim uređajima kako bi se identificirao ili verificirao vlasnik uređaja. Danas postoje uređaji visoke kvalitete koji imaju kvalitetne senzore za bilježenje biometrijskih karakteristika tako da faktor troška kod proizvođača ne smije činiti veliku ulogu jer se već postavljaju standardi. U najnovijim pametnim mobilnim uređajima kao najpopularnija biometrijska karakteristika za identifikaciju vlasnika uređaja koristi se otisak prsta, a odmah iza te karakteristike jest prepoznavanje lica.

3.4. Biometrijski sustavi

Biometrijski sustav je zapravo običan sustav koji prepoznaje uzorke osobe koji su bazirani na specifičnim fiziološkim ili bihevioralnim značajkama koje ta osoba posjeduje. [6]

Sustav prikuplja biometrijske podatke osobe, izvlači glavne značajke iz prikupljenih podataka, uspoređuje prikupljene značajke sa značajkama koje su spremljene u bazi podataka, izvršava akciju na temelju rezultata usporedbe. Prema tome, biometrijski sustav se može promatrati kao sustav s četiri modula: [2]

1. **Modul senzora**
   Kako bi sustav mogao zabilježiti biometrijske karakteristike kao što je to otisak prsta ili crte lica, potreban je senzor u oblicu skenera ili kamere. Modul senzora predstavlja glavno sučelje između osobe i uređaja pa je vrlo bitan za funkcioniranje sustava. Ukoliko je skener nekvalitetan ili kamera ima slabu kvalitetu slike može se prouzročiti pogreška što rezultira pogrešnom identifikacijom ili verifikacijom.

2. **Procjena kvalitete i izvlačenje podataka**
   Nakon što senzor zabilježi karakteristiku, procjenjuje se kvaliteta te se ocjenjuje prikladnost podataka za daljnje procesiranje. Obično, podaci su podvrgnuti algoritmima za poboljšanje kvalitete. Međutim, u nekim slučajevima podaci znaju biti toliko loši da osoba mora ponoviti akciju prezentiranja biometrijskih karakteristika. Nakon toga, biometrijski podaci se obrađuju. Prilikom pristupanja osobe biometrijskom uređaju prvi puta, taj proces se naziva *upis*, a prvi spremljeni podaci su *uzorak* kao temelj za usporedbu prilikom identifikacije ili verifikacije.

3. **Uparivanje i donošenje odluke**
   Izvučeni podaci značajki uspoređuju se sa spremljenim uzorcima te se generiraju rezultati uparivanja. Rezultati mogu biti ograničeni ukoliko su podaci biometrijske karakteristike loše kvalitete. Prema dobivenim rezultatima modul odluke potvrđuje identitet osobe ili pruža ocjenu sličnosti upisanih osoba kako bi se osoba mogla identificirati.

4. **Modul baze podataka**
   Baza podataka služi kao repozitorij biometrijskih informacija. Prilikom početne faze upisa osobe, izvučene značajke iz biometrijskih podataka spremljene su u bazu

podataka. Uz te podatke upisuju se i biografske informacije (ime, prezime, PIN, adresa) koje karakteriziraju osobu.

3.5. Primjena biometrijskih sustava

U literaturi [6] koja je starija od desetljeća spominju se biometrijski sustavi koji se koriste u organizacijama, aerodromima, tvrtkama, odnosno, tamo gdje je potrebna visoka razina sigurnosti. Danas to više nije tako. Ukoliko je netko više informatički obrazovan, može sam kupiti uređaje i izgraditi svoj biometrijski sustav te za njega napraviti potrebnu aplikaciju. Također, jedan od prvih aplikaciju koje su koristile biometrijske karakteristike u biometrijskim sustavima su forenzičke aplikacije. Aplikacije koje mogu identificirati otiske prstiju, odraditi rekonstrukciju crta lica te usporediti sa primjerima iz centralne baze podataka te aplikacije koje su se koristile na mjestima javnog prijevoza od kojih najintenzivnije na aerodromima. Nadalje, u trenutcima ratnih zbivanja pojavljuje se masa ljudi koja bježi od sukoba. Ti ljudi prelaze granice drugih država, a te države koriste biometrijske aplikacije kako bi najlakše prepoznali ljude koji ulaze u njihovu državu te dobili odgovore na prijašnje postavljena pitanja.

Navedeni primjeri biometrijskih aplikacija mogu se kategorizirati u tri glavne grupe koje prikazuje tablica 2. [2]

Forenzičke aplikacije	Aplikacije za potrebe vlade	Komercijalne aplikacije
Identifikacija tijela	Osobna iskaznica, putovnica	Bankarske aplikacije
Kriminalne istrage	Vozačka dozvola	Pametni mobilni uređaji
Utvrđivanje roditeljstva	Socijalna pomoć	Prijenosna računala
Nestala djeca	Prelazak granica	Poslovanje e-trgovina

Tablica 2. Primjeri gdje se koriste aplikacije biometrijskih sustava za prepoznavanje osoba (Izvor: [2], 2008.)

Na kraju, mogu se usporediti prednosti i nedostaci biometrije iz navedenih kategorija. U kategoriji komercijalnih aplikacija potrebno je pozitivno prepoznavanje osoba i biometrijski sustav se može koristiti u svrhu verifikacije ili identifikacije. S druge strane, aplikacije za potrebe vlade te forenzičke aplikacije sadrže aplikacije za negativno prepoznavanje gdje je potrebna identifikacija. [6]

3.5.1. Pozitivno prepoznavanje

U zadnje vrijeme neke aplikacije nude mogućnost prepoznavanje korisnika preko biometrijskih karakteristika otiska prsta, a primjer toga je mobilna bankarska aplikacija. Ukoliko korisnik ima pametni mobilni telefon koji sadrži senzor za prepoznavanje otiska prsta, može dodatno osigurati prepoznavanje prilikom prijavljivanja. Aplikacija zahtjeva od korisnika da prisloni prst na senzor više puta te se uzorak sprema u bazu podataka. Prilikom sljedećeg prijavljivanja u aplikaciju korisnik može birati hoće li se prijaviti u aplikaciju preko lozinke ili preko otiska prsta.

Biometrijska karakteristika u aplikacijama nudi razinu sigurnosti koju nije lako probiti. Ne postoji laki način na koji haker može falsificirati biometriju kako bi izveo napad, a s druge strane postoji vrlo mala šansa da se odbije biometrijska karakteristika osobe koja je spremljena u bazi podataka [6]. Biometrija olakšava korištenje aplikacije gdje korisnik sve što mora napraviti jest izvršiti prijavu preko biometrijske karakteristike. Korisnik više ne mora pamtiti više izbora lozinke, ne mora pamtiti duge fraze svojih lozinka te izvršavati česte promjene lozinka.

Biometrijski sustavi nisu neprobojni, na njih se također mogu izvršavati napadi na njihove module i komunikacijske kanale. Zaštita od takvih napada vrši se korištenjem osnovnim temeljem kriptografskih tehnika. Također, postoji rizik od krađe biometrijskih karakteristika. Kao protumjera koriste se sva načina zaštite: 1. vitalni detekcijski mehanizmi u hardveru i softveru prepoznavanje biometrijskog sustava, 2. multimodalni biometrijski sustav koji spaja više biometrijskih karakteristika kao na primjer lice, prst i geometrija dlana. [6]

Nadalje, kao zaštita od napada može se koristiti kombinacija onoga što korisnik zna i biometrijske karakteristike. Tako na primjer, neki pametni telefoni koji nude mogućnost pristupa uređaju preko prepoznavanja neke biometrijske karakteristike, nakon nekog vremena od korisnika zahtijevaju PIN koji je ono što korisnik zna.

3.5.2. Negativno prepoznavanje

Aplikacije povezane sa zakonodavnim sustavima i forenzičke aplikacije koje imaju funkciju kao pozadinska provjera zaposlenika, sprečavanje terorista da se ukrcaju na avion, identifikacija tijela, moraju izvršavati pojedinačno prepoznavanje osobe na način identifikacije. Za razliku od verifikacije, identifikacije je mnogo teža jer identifikacijski sustav mora izvršavati veliki broj usporedba. Nadalje, biometrijski sustav negativnog prepoznavanja koji radi u poluautomatskom načinu rada sa stručnjakom koji provjerava prijetnje i donosi finalne odluke vrlo je efektivan. Na primjer, ako je potrebno sto agenata na aerodromu da pojedinačno identificiraju sumnjivce sa liste od sto najtraženijih, s druge trebalo bi pet agenata da provjerava dvjesto dnevnih upozorenja prijetnji koje generira biometrijski sustav. U takvim aplikacijama sa

polu automatskim načinom rada biometrijski sustav generira upozorenje koje poziva stručnjaka na dodatnu analizu. [6]

Ostale aplikacije, kao što su pozadinske provjere te kriminalna identifikacija sumnjivca također mogu raditi u poluautomatskom načinu rada. Na primjer, kada se policijski organi bave kriminalističkim istraga, obično se koriste aplikacije za automatsku identifikaciju otiska prsta kako bi se suzio broj sumnjivaca. [6]

4. Privatnost i sigurnost biometrijskih podataka u sustavu

Svaka osoba ima pravo na privatnost. Osobne informacije kao što su adresa stanovanja, OIB, broj osobne iskaznice, datum rođenja, ime i prezime su osjetljivi podaci. Ako netko ne želi da te informacije budu pristupačne javnosti ima svako pravo zadržati ih za sebe.

Postoji više definicija za privatnost, prema autoru [11] navode se tri definicije:

1. **Privatnost znači biti pušten na miru**
   Osoba ima pravo da je se ne prisluškuje, prikupljaju njezine osobne informacije te prate njezine radnje bez naloga zakonodavnih ustanova ili ukoliko ne predstavlja prijetnju prema državi.

2. **Privatnost znači vrsta autonomije nad osobnim stvarima**
   Osoba ima pravo imati kontrolu nad količinom informacija koje mogu biti dostupne javnosti.

3. **Privatnost znači granica pristupa informacija o sebi**
   Ovdje se radi razlika između privatnosti i slobode. Na primjer, ukoliko osoba A prisluškuje osobu B te u nekom trenutku osoba A sazna osjetljive informacije osobe B. Te informacije osoba A ne smije iskoristiti ukoliko ne dobije pravo od zakonodavnih ustanova.

Biometrijske karakteristike se također smatraju kao osobni podaci za koje osoba ima pravo na privatnost. Ali, ukoliko se osoba nalazi na javnom prostoru mora biti svjesna da postoji mogućnost da su njezine biometrijske karakteristike izložene. Na primjer, ako osoba prolazi pokraj video nadzora, postoji mogućnost da će njezina biometrijska karakteristika crta lica biti uhvaćena te spremljena u jednu od baze podataka. Nadalje, neke biometrijske karakteristike spremaju se u državnu bazu podataka prilikom izrade osobne iskaznice ili putovnice. Ukoliko se želi izbjeći manipuliranje nad osjetljivim podacima moraju postojati zakoni i regulative koji reguliraju njihovo korištenje. Jedan od primjera jest nedavno usvojena regulativa GDPR od strane Europske komisije, koja će biti dodatno objašnjena kasnije.

4.1. Sigurnost biometrijskih podataka unutar biometrijskog sustava

Biometrijski sustav je zapravo digitalni sustav koji se sastoji od više komponenata koje mogu činiti ranjivu točku za napad. Senzori, komunikacijski kanali i baze podataka mogu biti izloženi širokom spektru napada pokušaja ponavljanja i drugih napada od treće strane. Kada je biometrijska karakteristika zaprimljena na aplikacijskoj razini od strane senzora, digitalna reprezentacija karakteristike može se presresti preko komunikacijskih kanala te iskoristiti kao nelegitimna autentikacija. Budući da je biometrijska karakteristika reprezentacija žive osobe, nemoguće je ponovno namjestiti drugačije podatke kao što je to moguće kod lozinka ili pametnih kartica. Podaci su jedinstveni za svaku osobu pa nisu promjenjivi. Zaštita biometrijskih podataka u sustavu je najvažniji zadatak kako bi korisnicima sustava osigurali privatnost. [7]

Ukoliko sigurnost podataka u biometrijskom sustavu nije na razini koja zadovoljava njegove korisnike, većina će negodovati pružanju novih ili procesiranih biometrijskih podataka takvom nesigurnom sustavu. Također, korisnici vrlo vjerojatno neće pružati svoje biometrijske podatke centraliziranim i nepouzdanim aplikacijama. Tako će aplikacije s decentraliziranim mogućnostima prepoznavanja biti najprihvatljivije. Decentraliziranost podataka može se postići tako da se biometrijske informacije spremaju na decentraliziranom serveru sa kriptiranom bazom podataka nad kojom korisnik ima potpunu kontrolu. Na primjer, sustav može koristiti pametnu karticu na kojoj je spremljen uzorak otiska prsta korisnika. Uz to, pametna kartica može imati integrirani senzor za otisak prsta te mogućnost izvlačenja i procesiranja značajki kako bi se usporedile sa uzorkom te na temelju toga donijela odluka. [6] Kako bi se postigla dodatna sigurnost biometrijskih karakteristika u bazi podataka, podaci se mogu kriptirati. Kada korisnik sustava zatraži pristup preko biometrijskog senzora njegove karakteristike se uspoređuju sa kriptiranim karakteristikama koje su spremljene u bazi podataka. Uz kriptiranje karakteristika sustav može imati mogućnost autentikacije korisnika preko PIN broja. [7]

4.1.1. Prijetnje sigurnosti biometrijskih sustava

Budući da su biometrijske karakteristike spremljene u digitalnom obliku, svakim danom pojavljuju se nove prijetnje i pokušaji krađe tih karakteristika. Svakim danom hakerski napadi na biometrijske sustave su sve sofisticiraniji te u skoroj budućnosti postoji opasnost od obrnutog inženjeringa spremljenih biometrijskih karakteristika u bazi podataka. Ukoliko se prepoznavanje sve više implementira za korištenje u širim masama, dobra zaštita spremljenih podataka postaje imperativ. Na kraju, korisnička prihvatljivost svodi se na dobru sigurnost biometrijskih sustava, očuvanja privatnosti te jednostavnost korištenja.

Kod biometrijskog sustava mjerna fizička ili bihevioralna karakteristika naziva se biometrijski identifikator. Taj biometrijski identifikator postaje biometrijski uzorak kada korisnik prvi puta pristupi biometrijskom sustavu za prepoznavanje te ga procesira prema postavljenim pravilima i algoritmima koji su definirani u sustavu. Biometrijski uzorak ne sadrži biometrijske podatke u originalnoj formi kao što je slika otiska prsta ili slika lica. Uzorci su definirani kao binarni podaci te nisu čitljivi. Biometrijski uzorci sadrže jedinstvene karakteristike biometrijskih informacija osobe te su glavni primjerci nad kojima će se vršiti usporedba za svaku buduću prijavu korisnika u sustav. [12]

Opće poznato je da se korisničko ime i lozinka koristi za identifikaciju ili autentikaciju korisnika. Glavna razlika korisničkog imena i lozinke od biometrijske karakteristike jest ako dođe do probijanja lozinke ona se vrlo lako može zamijeniti novom lozinkom. Ukoliko se biometrijska karakteristika probije obrnutim inženjeringom, ona se ne može promijeniti jer je to jedinstvena karakteristika koja definira pojedinu osobu. Zbog toga, zaštita biometrijskih podataka u biometrijskom sustavu mora biti na vrlo visokom nivou kako uopće ne bi došlo do probijanja.

Za razliku od ostalih elektroničkih podataka, postoji više razina na koji način se može izvršiti probijanje podataka. Procesirani biometrijski podaci nazivaju se biometrijski uzorci. Budući da se te biometrijske karakteristike zapisuju uz pomoć posebne opreme, vođenje sigurnosti tih biometrijskih podataka mora započeti od biometrijske opreme pa sve do načina spremanja tih podataka u bazu podataka. [12]

Prema navodima Thakkar D. [12], postoji velik broj drugih ranjivosti povezanih s biometrijskim sustavima kao što su:

- Pristupanje uređaju za spremanje biometrijskih karakteristika kako bi se ukrali biometrijski uzorci
- Kreiranje replike biometrijske karakteristike kako bi se koristila kao biometrijski uzorak
- Zamjena uzorka korisnika lažnim uzorkom
- Zaobilazak kompromitiranog uzorka za odgovarajući modul
- Praćenje korisnika na način da se prate njegove ili njezine identifikacijske ili autentikacijske aktivnosti.
- Njuškanje mrežne komunikacije od i do biometrijskog sustava za prepoznavanje

Biometrijski uzorak može biti probijen na lokaciji u kojoj je spremljen pa tako osiguranje skladištenja biometrijskih podataka mora postati prvi sloj sigurnosti. S druge strane, drugi sloj sigurnosti biometrijskog uzorka može se osigurati njegovim kodiranjem. Na taj način uzorak postaje beskoristan za kriminalce. Budući da metode skladištenja biometrijskog uzorka variraju o samoj opremi koja se koristi prema centraliziranoj bazi podataka, moraju se primijeniti drugačije metode za osiguranje skladištenja uzorka.

4.1.2. Strategije sigurnog spremanja biometrijskih karakteristika u baze podataka

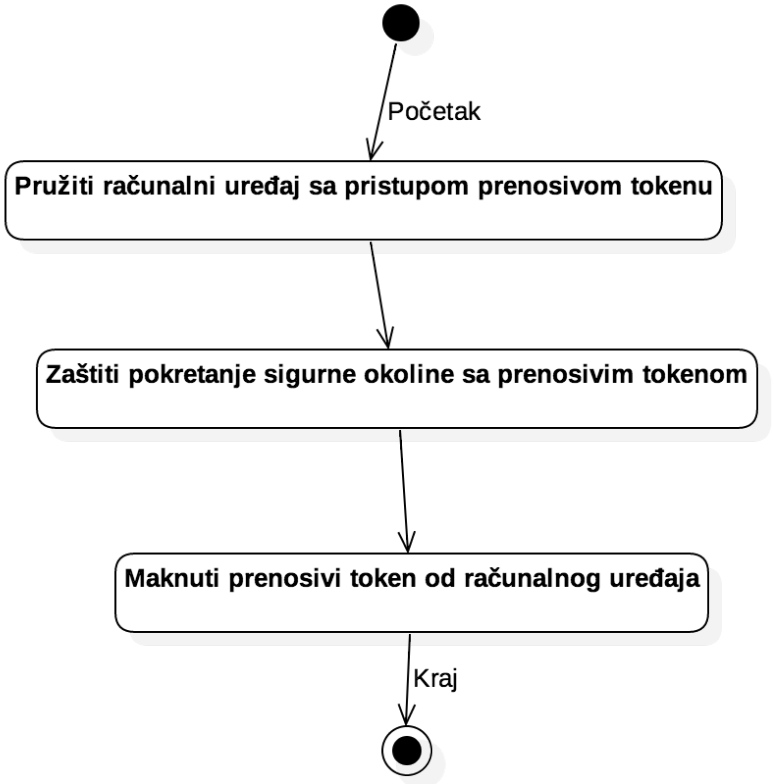
Kako bi sigurno spremile biometrijske karakteristike, obično se implementiraju četiri glavne metode za spremanje podataka. Ovisno o tipu i potrebama navedene su: [12]

1. Prenosivi znak (*token*)
2. Centralizirana biometrijska baza podataka
3. Individualne radne stanice
4. Biometrijski sustav prepoznavanja

4.1.2.1. Prenosivi znak (*token*)

Token se može koristiti kao prenosivi uređaj za lansiranje kontrolirane i provjerene okoline. Treća strana može koristiti prenosivi računalni uređaj s kojim se može uspostaviti razina sigurnosti tako da se koristi mehanizmi ovjeravanja fiksiranog tokena. [13]

Na slici osam prikazan je dijagram slijeda metode koja pokreće sigurnu okolinu koristeći prenosivi token.



Slika 8. Dijagram aktivnosti pokretanja sigurne okoline prenosivim tokenom (Izvor: [13], Fig. 8)

U ovoj metodi, biometrijski podaci osobe su spremljeni na prenosivi token kao što je pametna kartica. Spremanje podataka na pametnu karticu a ne u centralnu bazu podataka znači da nije potrebno koristiti mrežu za verifikaciju te za spremanje biometrijskih podataka. Na taj način izbjegnuti su rizici i ranjivosti koji dolaze sa mrežom i mrežnim podacima. Kada su biometrijski podaci spremljeni na pametnu karticu, korisnici imaju osjećaj kao da su u kontroli svojih privatnih podataka. Na taj način povećava se prihvatljivost korisnika prema toj strategiji spremanja podataka. S druge strane, problem te strategije može biti trošak. Budući da korisnici koriste kartice, mora postojati uređaj koji čita te kartice, što znači da se mora izdvojiti iznos za izradu kartica i kupnju uređaja koji čita te kartice. [12]

4.1.2.2. Centralizirana biometrijska baza podataka

Centralizirana baza podataka se sastoji od procesora koji je povezan sa uređajima za pohranom podataka i ostalom periferijom. Fizičko je zatvorena na jednoj lokaciji. Sustav pruži uslugu obrade podataka korisnicima koji se nalaze na istom mjestu ili preko udaljenih terminala na geografski drugačijim lokacijama. Upravljanje podacima sustava izvršava se sa jedne od centralnih lokacija. Nedostaci ovakvog sustava su da kada sustav padne tada je svaki korisnik blokiran i ne može koristiti sustav sve dok se on ponovo ne digne. Također, postoji trošak komunikacije terminalima do centralne lokacije koji može biti poprilično skup. [14]

Server centralizirane biometrijske baze podataka se koristi kako bi se spremali biometrijski uzorci. Takav pristup nudi financijski prihvatljivije rješenje implementacije biometrijskog ovlaštenja te je prihvatljivo za korisnike koji zahtijevaju multi-lokacijsku autentikaciju. Budući da se podaci korisnika prebacuju preko mreže, ovaj pristup izložen je napadima hakera. Napadač može rekreirati sesiju ovlaštenja i izvršiti transakciju. Ovakvi napadi mogu se zaustaviti enkripcijom. Međutim, enkripcija rješava problema, ali spremanje podataka i pristupna prava enkripcijskim ključevima postaju novi problem. Ukoliko se koristi pristup enkripcije, mora se donijeti odluka gdje će ključevi biti spremljeni te tko će imati pristup tim ključevima. Taj proces može biti vrlo kompleksan. [12]

4.1.2.3. Individualne radne stanice

Spremiti sve podatke na jedno mjesto nije baš najbolje rješenje. Ukoliko se dogodi napad na bazu podataka i podaci budu provaljeni, napadač ima sve informacije od svih korisnika jer je sve spremljeno na jednom mjestu. Zbog toga, spremanje podataka u individualne radne stanice može pomoći u tome da se podaci raširе i da se svi podaci ne nalaze samo na jednom mjestu.

Takav pristup se čini boljim od spremanja podataka na biometrijski uređaj. Iz radne stanice je puno teže ukrasti biometrijske podatke nego sa biometrijskih uređaja za prepoznavanje. S druge strane, ovaj pristup također može imati negativne posljedice u sigurnosti. Radne stanice mogu imati slabo ili nestandardno osiguranje za razliku od centralne baze podataka. Također, korisnici ne mogu izvršiti autentikaciju identiteta sa više lokacija kao što je to moguće kod centralizirane baze podataka. [12]

4.1.2.4. Biometrijski sustav prepoznavanja

Kada se biometrijski podaci spremaju direktno u sustav za prepoznavanje, otvara se mogućnost brzog davanja odgovora korisniku prilikom autentikacije. Kod centralizirane baze podataka, prilikom izvršavanja prepoznavanja, podaci se dohvaćaju preko mreže te odgovor najčešće ovisi o kvaliteti mreže ili brzini interneta. Kad su podaci spremljeni u biometrijskom sustavu, oni se dohvaćaju iz lokalne baze podataka pa odgovor stiže brzo. Spremanje

biometrijskih podataka na samu opremu znači da korisnik dobiva brz odgovor jer korisnik ne ovisi o vanjskim sustavima koji mogu biti u nepoznatom stanju isto kao što i njihovi komunikacijski kanali. [12]

4.1.3. Tehnike zaštite biometrijskih uzoraka

Za zaštitu biometrijskih uzoraka spominju se dvije kategorije. Prva kategorija se odnosi na transformaciju značajki što znači da se iz postojećih značajki stvaraju nove koje zamjenjuju original. Kao druga kategorija spominje se biometrijski kripto sustav. Prethodno je napomenuto da se biometrijske značajke mogu zaštititi njihovim kriptiranje. Na digitalne uzorke primjenjuju se algoritmi kriptiranja te se takav kriptirani uzorak sprema u bazu podataka. Da bi se takav uzorak mogao dešifrirati potreban je ključ koji je tajan. Na kraju, usporedbom će se utvrditi razlike između te dvije kategorije.

4.1.3.1. Transformacije biometrijskih značajki

Transformacija značajki je grupa metoda koje kreiraju nove značajke. Te metode vrše redukciju dimenzija tako da izračunaju optimalan podskup prediktivnih značajki koje mogu biti mjerljive sa originalnim podacima. Biometrijska baza podataka sprema samo transformirani uzorak. Kada se pojavi zahtjev za tim uzorkom, vrši se transformacija zahtjeva istom metodom kao i kod transformiranja biometrijskog uzorka. Koristi se ključ ili lozinka kako bi se izvukli podaci i parametri iz transformacijske funkcije. [12]

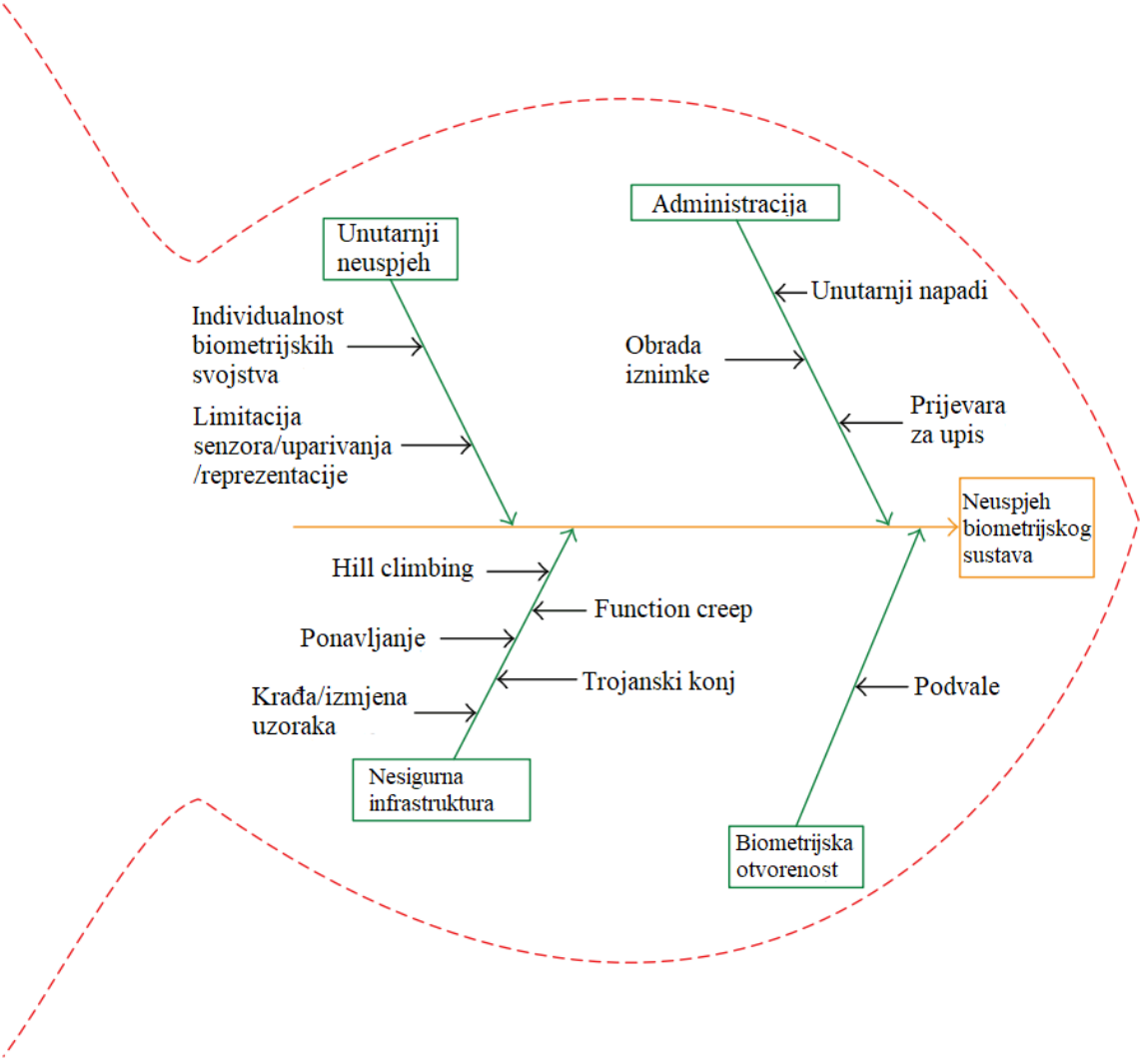
4.1.3.2. Biometrijski kripto sustav

Ovaj pristup koristi pomoćne podatke kako bi se zaštitio biometrijski uzorak. Takva metoda nazvana *„Helper Data Method“* koristi javne dostupne informacije o uzorku. Ne otkrivaju se nikakve značajne informacije o originalnom uzorku. Također, ovaj pristup svrstava se u kategoriju generiranja i vezivanja ključeva. Ako se ključ veže neovisno o biometrijskoj značajki sa biometrijskim uzorkom, to se naziva *„Key binding“* pristup. Ako su s druge strane, pomoćni podaci izvučeni iz uzorka i na njega direktno generiran kriptografski ključ tada se to naziva *„Key generating“* biometrijski kripto sustav. [12]

Čuvanje biometrijskih uzoraka može biti puno izazova s trenutnim stanjem sigurnosti podataka gdje se svakodnevno povećava rizik od napada. Hakerski napadi su sve više sofisticirani, intenzivni i kompleksni. Sa kriptiranim biometrijskih uzorkom ne može previše, ali bitnije je zaštiti biometrijske podatke u bazi podataka da biometrijski podaci uopće ne budu ukradeni. [12]

5. Slabosti biometrijskog sustava

Kao što je već spomenuto, brzim razvojem tehnologija prepoznavanja biometrijski sustavi postaju sve više zastupljeni kao pouzdani sustavi za prepoznavanje. Međutim, kao i svakom sustavu pa tako i ovdje, pojavljuju se pitanja o sigurnosti podataka koji su spremljeni u bazama. Jesu li ti podaci zaštićeni na zakonski način, jesu li dovoljno zaštićeni od hakerskih napada, čuva li se privatnost njihovih korisnika te jesu li pouzdani za korištenje, odnosno, koliki je odnos ispravnih i pogrešnih prepoznavanja.



Slika 9. Model riblje kosti za kategoriziranje ranjivosti biometrijskog sustava (Izvor: [15], str. 4)

Na slici devet prikazan je dijagram uzroka i posljedice koji po izgledu liči na riblju kost. Taj dijagram je koristan za naš biometrijski sustav jer nudi preglednu sliku svih mogućih prijetnji s kojim se može biometrijski sustav sresti ukoliko dođe do njegovog neuspjeha. Dijagram se radi tako da se identificira glavni problem koji čini glavu ribljeg kostura, zatim, identificiraju se barem četiri uzroka koji su povezani sa glavnim problemom. Uzroci se razbijaju tako da se daju

odgovori na pitanja srži uzroka [17]. Na slici osam glavni prikazani problem je „Neuspjeh biometrijskog sustava“ koji čini glavnu riblju kost dok su četiri glavna uzroka „Administracija“, „Biometrijska otvorenost“, „Unutarnji neuspjeh“ te „Nesigurna infrastruktura“.

5.1.1.1. Administracija

Model riblje kosti zorno prikazuje koje su sve moguće situacije u kojima biometrijski sustav može izvršiti neuspjeh.

Administracija biometrijskog sustava je jedan od najvažnijih koraka kako bi se osigurao uspješan biometrijski sustav. Administracija pokriva više područja kao što su: [18]

- integritet prvog upisa,
- kvaliteta uzoraka prilikom prvog upisa,
- konfiguracija sustava,
- rukovanje iznimkama,
- mjere privatnosti

Na modelu slike devet identificirane su prijetnje od unutarnjih napada zaposlenika organizacije na biometrijski sustav za prepoznavanje te prijetnja od prijevare prilikom inicijalnog pristupa osobe biometrijskom sustavu, a da se pritom koristi lažna biometrijska značajka s ciljem da se prevari biometrijski sustav. Obrada iznimke u administraciji se koristi kako bi se izbjegle neugodnosti kod pravog korisnika. Na primjer, kada korisnik ima ozljedu prsta, njemu se može odobriti pristup sustavu alternativnim mehanizmima prepoznavanja bez da se koristi senzor za prepoznavanje otiska prsta [18]. Budući da se takva procedura može lako zloupotrijebiti predstavlja prijetnju da biometrijski sustav može izvršiti neuspjeh prilikom prepoznavanja.

5.1.1.2. Biometrijska otvorenost

Biometrijska otvorenost sustava se odnosi na to koliko je sustav sposoban u prepoznavanju lažnih ili originalnih biometrijskih karakteristika. Moguće je da protivnik ili treća strana prikriveno došla u posjed biometrijske karakteristike nekog korisnika (npr. Otisak prsa s površine) te da ih je iskoristila da izradi fizički predmet (silikonski prst) te biometrijske značajke. Budući da biometrijski sustav nije u stanju razlikovati stvarnu od podvaljene biometrijske prezentacije, korisnik može zaobići sustav tzv. *Spoofing*. [15]

5.1.1.3. Unutarnji neuspjeh

Iako se ne izvrši niti jedan vanjski napad sustav može izvršiti neuspjeh zbog unutarnjih ograničenja. Biometrijski sustav može izvršiti neuspjeh ako senzori ne uspiju uhvatiti primjer biometrijske karakteristike koju je korisnik prezentirao sustavu gdje sustav ne uspije uhvatiti

grešku. Budući da su uzrok tih grešaka unutarnja ograničenja kao što su greške senzora, uređaja za izvlačenje biometrijskih karakteristika ili uređaja za uparivanje značajki, a ne namjernog napada, takav sigurnosni propust naziva se *zero-effort attack*. [19]

5.1.1.4. Nesigurna infrastruktura

Postoji više načina na koje protivnik može manipulirati biometrijski sustav te izvršiti proboj sigurnosti. Napadi koji su uobičajeni za bilo koji sustav su sabotaža i sistemsko preopterećenje također mogu biti primijenjeni i na biometrijski sustav. Primjeri sabotaže su prekid dotoka struje, oštećenje površine senzora ili distribuiranje prekomjerne buke (prema sučelju) kako bi se prekinulo normalno funkcioniranje sustava. Preopterećenje sustava je pokušaj slanja poraznog broja zahtjeva za autentikaciju kako bi se sustav srušio. Motivacija tih napada jest kako bi se stvarnim korisnicima onemogućio pristup sustavu. [19]

U modelu riblje kosti prikazani su ostali napadi koji će detaljnije biti objašnjeni u sljedećem poglavlju, ali ističu se dva koja su na engleskom jeziku.

Napad *Function creep* vrši treća strana kako bi eksploatirala sustav da pruži pristup određenim resursima druge aplikacije što mu zapravo uopće nije namjena. Na primjer, uzorak otiska prsta iz baze podataka može se iskoristiti kako bi se u medicinskoj bazi podataka pretražili zdravstveni kartoni od osobe čiji je otisak prsta. [19]

Napad *Hill climbing* na biometrijski sustav vrši treća strana kada ima mogućnost ubacivanja neobrađenih biometrijskih podataka ili značajki preko trojanskog konja ili *man-in-the-middle* napada te napadač može upariti podatke sa uređajem za uparivanje biometrijskih karakteristika. Ukoliko je to moguće, napadač može pokušati izvršiti *brute-force* napad. Isprobavanjem različitih uzoraka iz velike biometrijske baze podataka postoji veća mogućnost da se izvrši uparivanje biometrijskih karakteristika. [19]

5.2. Ostale ranjivosti biometrijskog sustava

U biometrijskom sustavu postoje pet glavnih komponenti, a to su senzor, uređaj za ekstrakciju značajki, baza podataka s biometrijskim uzorcima, sustav za uparivanje biometrijskih uzoraka s originalom i modul za donošenje odluka. Neuspjeh prilikom prepoznavanja bilo koje od tih komponenti može se kategorizirati u dvije klase: [15]

- Unutarnji neuspjeh
- Neuspjeh prilikom izvršavanja napada treće strane

5.2.1. Posljedice neuspjeha biometrijskog sustava

Ako je biometrijski sustav kompromitiran to znači da je nastupio jedan od dva glavna događaja: [15]

1. **Uskraćivanje usluge (*denial-of-service*)**
   Događaj kada stvarni korisnik nije u mogućnosti koristiti servis koji mu je namijenjen. Napadač ili treća strana može sabotirati infrastrukturu pa na taj način spriječiti korisnika da ima pristup sustavu. Također, administrativna zloupotreba kao što su modifikacija uzoraka ili radnih parametara može prouzročiti uskraćivanje usluge. Ukoliko dođe do unutrašnje pogreške kao što je pogrešno odbijanje, pogrešno skeniranje ili zapisivanje biometrijske karakteristike, također može doći do uskraćivanja usluge.

2. **Upad**
   Odnosi se na situaciju kada varalica dobiva ne legitiman pristup biometrijskom sustavu, što znači da je u sustavu kompromitirana privatnost (npr., neautorizirani pristup osobnim ili zdravstvenim informacijama) te da postoje sigurnosne prijetnje (npr., prelazak terorista preko granice). Na slici devet modela riblje kosti, gdje su prikazani svi uzroci ranjivosti biometrijskog sustava, njihova krajnja akcija može rezultirati upadom u biometrijski sustav.

5.2.2. Točke napada biometrijskog sustava

Napadi na sustav generalno iskorištavaju slabosti sustava na jednom ili više modula. Prema autorima [15] ti napadi grupiraju se u četiri kategorije:

1. **Napadi na korisničko sučelje**
   Kao što je prije napomenuto napadi se izvršavaju direktnim oštećenjem ili varanjem uređaja koji služi za prepoznavanje biometrijskih karakteristika. Ako uređaj ne može prepoznati razliku između lažne i prave karakteristike, napadač može upasti u sustav pod lažnim identitetom. U novije vrijeme, kako se tehnologija razvija pojavljuju se razne hardverske i softverske solucije za sprječavanje takvih vrsta napada.

2. **Napadi na sučelja između modula**

   Treća strana izvršava napada na komunikacijske kanale biometrijskog sustava koji povezuju različite module. Na primjer, napadač može postaviti interferentni uređaj koji će blokirati bežično sučelje. Ako komunikacijski kanal nije osiguran fizički ili kriptografski, napadač može presresti informacije koje putuju tim kanalima te promijeniti njihovo prvobitno stanje. Način na koji se osiguraju takvi kanali jest da se kriptiraju podaci koji se prenose koristeći infrastrukturu javnog ključa. Ali i tada, napadač može izvršiti napad „ponavljanja" da presretne kriptirane podatke pravog korisnika te ih preusmjeri na bilo koji modul biometrijskog sustava u koji želi upasti. Protumjere takvih napada su vremenske marke poslanih zahtjeva pravih korisnika ili korištenje *challange/response* mehanizma.

3. **Napadi na softverske module**

   Kako bi moduli biometrijskog sustava i njihova sučelja mogli funkcionirati koriste se programirane softverske aplikacije. Ukoliko dizajneri softvera nisu pazili na sigurnost izvršnog programa, napadač može modificirati aplikaciju te izvršiti željeni rezultat. Takvi napadi su poznati pod nazivom „Trojanski konj". Ako se dublje analizira kod aplikacije čija sigurnost nije na razini, postoji vjerojatnost pojave nekonzistentnosti u algoritmu koda. Na taj način, napadač izvršava napad na sustav tako da traži takozvani *„loophole"* da upadne i dođe do željenih informacija bez da ga se otkrije.

4. **Napadi na bazu podataka biometrijskih uzoraka**

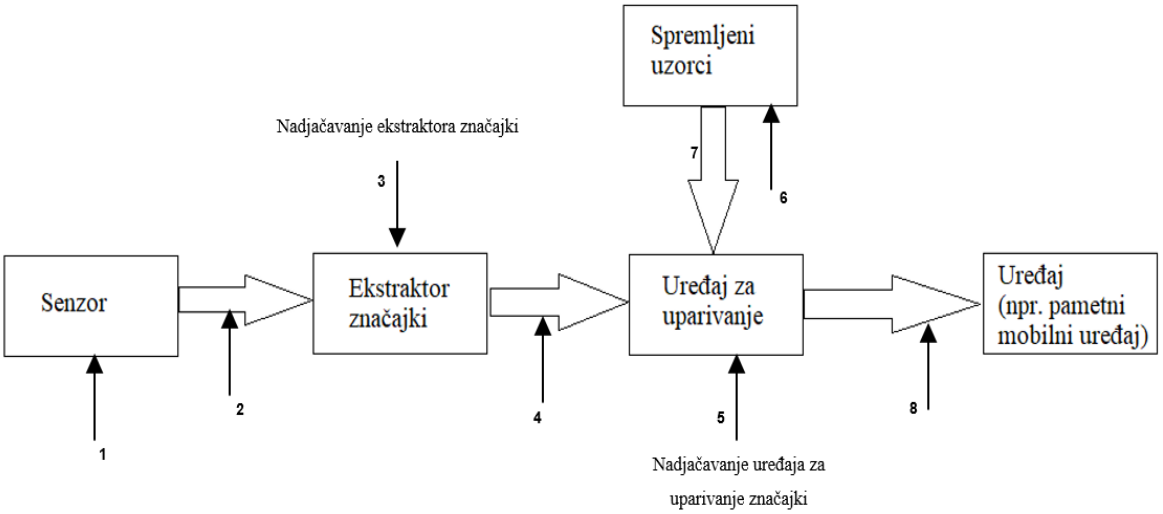
   Potencijalno najizgledniji napad na biometrijski sustav jest napad na bazu podataka gdje su spremljeni biometrijski uzorci. Napadi bazu sa uzorcima, prema autorima [15] mogu prouzročiti tri ranjivosti:

   1. Originalni uzorak može biti zamijenjen sa lažnim kako bi se dobio neautorizirani pristup
   2. Od originalnog uzorka može se kreirati lažna fizička biometrijska karakteristika (gumeni prst) kako bi se pridobila neautorizirana razina pristupa
   3. Ukraden uzorak iz baze podataka može biti ponovo iskorišten na uređaju za uparivanje kako bi se pridobila neautorizirana razina pristupa sustavu

   Također, napadači znaju izvršavati *function creep* napad koji je prije bio detaljnije objašnjen.

Najizravniji način da se osigura biometrijski sustav i uzorak koji drži jest da se svi sustavski moduli i sučelja koja se nalaze između stave na pametnu karticu (sigurni procesor). U takvim sustavima uređaji za izvlačenje značajki i njihovo uparivanje te senzor ovise o tehnologijama koji se nazivaju *match-on-card* ili *system-on-card.* Prednost takvih tehnologija jest da se biometrijske informacije nalaze na kartici i nigdje drugdje. S druge strane takva tehnologija nije prikladna za aplikacije velikog razmjera. Kartice su skupe i mora biti prisutna kod korisnika ukoliko želi pridobiti pristup osiguranom prostoru. [15]

Nadalje, prema autorima [16] na slici deset prikazan je generički biometrijski sustav i njegovi moduli. Na slici su prikazana osam osnovnih izvora napada koji su opisani nakon.



Slika 10. Moguće točke napada biometrijskog sustava (Izvor: [16], str.2.)

1. **Lažna biometrijska značajka kod senzora**

   Ovaj napad spomenut je već više puta, a odnosi se na moguću reprodukciju biometrijske značajke kao lažne koja je na taj način prezentirana sustavu. Primjeri takvog napada mogu biti lažan prst, kopija nečijeg potpisa ili maska za lice.

2. **Ponavljanje slanja digitalno starog biometrijskog signala**

   U ovoj vrsti napada, već zapisani digitalni biometrijski signal se ponavljajući šalje u sustav kako bi se zaobišao senzor. Primjer napada može biti prezentacija stare kopija digitalne slike otiska prsta ili zabilježeni glasovni znak korisnika sustava.

3. **Nadjačavanje ekstraktora značajki**

   Haker izvršava napad na ekstraktor značajki tako da izradi trojanski konj koji prezentira odabrani set biometrijskih značajki po želji napadača.

4. **Neovlašteno mijenjanje reprezentacije biometrijskih značajki**

   U normalnom slučaju, dvije faze odvajanja značajki i njihovo uparivanje nisu odvojene pa je ova vrsta napada za izvesti vrlo teško. Ukoliko se značajke šalju preko udaljenog uređaja za uparivanje (npr., preko Interneta) tada napadač može „prisluškivati“ promet mreže TCP/IP protokola te mijenjati pakete koji se šalju.

5. **Nadjačavanje uređaja za uparivanje značajki**

   Nad uređajem za uparivanje vrši se nadjačavanje tako da direktno mijenja i distribuira umjetan broj visoke ili niske postotne jednakosti između biometrijskih značajki.

6. **Neovlašteno mijenjanje biometrijskih uzoraka**

   Baza podataka u kojoj se nalaze spremljeni biometrijski uzorci može se nalaziti lokalno ili na udaljenom mjestu. Također, ta baza može biti distribuirana preko nekoliko servera. Cilj napadača jest da pokuša promijeniti jednog ili više spremljenih uzoraka što može prouzročiti uspješnu autorizaciju lažnog korisnika ili uskraćivanje usluge korisnika.

7. **Napad na kanal između spremljenih uzoraka i uređaja za uparivanje**

   Kada korisnik koristi biometrijski sustav, uzorci za uparivanje se šalju iz baze podataka do uređaja preko kanala za njihovu komunikaciju. Napadač vrši napad na uzorke tako da ih presretne u kanalu i promjeni njihov sadržaj prije nego što oni stignu do svojeg odredišta.

8. **Nadjačavanje modula za donošenje odluka**

   Koliko god bio dobro biometrijski sustav zaštićen i njegove sigurnosne mjere na vrhuncu, ako napadač ima mogućnost mijenjati ishod rezultata sve ostalo je nebitno. Ukoliko napadač može izmijeniti rezultat modula za donošenja odluka posljedice za taj biometrijski sustav mogu biti katastrofalne.

Postoji više tehnika kako bi se odbili navedeni napadi na biometrijski sustav. Na primjer, ako se kod senzora koristi novija tehnologija koja može osjetiti puls kod prislanjanja prsta na senzor ili koja osjeća vodljivost prsta, može se spriječiti napad kod točke 1. Enkripcijom komunikacijskih kanala mogu se zaustaviti udaljeni napadi na točke 4 i 8. Najjednostavniji način za zaustavljanje napada na točke 5, 6 i 7 jest da se uređaj za uparivanje značajki i baza podataka nalaze na sigurnoj lokaciji. Spomenuto spremanje biometrijskih značajki na pametne kartice koje korisnik nosi sa sobom također može spriječiti napadača da izvrši napad na točku 6. [16]

5.3. Sheme zaštite uzoraka

Idealna shema zaštite biometrijskih uzoraka treba imati četiri glavnih svojstva: [21]

- **Raznovrsnost**

  Ne bi smjela postojati mogućnost da zaštićeni biometrijski uzorci budu upareni sa drugima iz drugih aplikacija. Na taj način zaštićena je privatnost korisnika sustava.

- **Mogućnost poništenja**

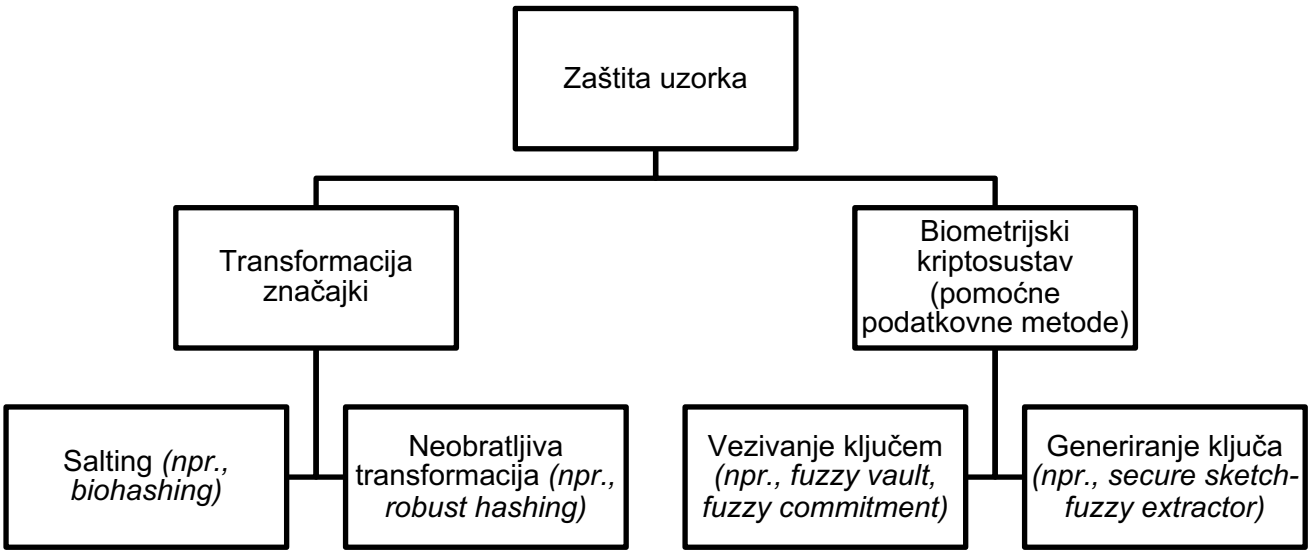
  Ukoliko dođe do kompromitiranja zaštićenog biometrijskog uzorka iz baze podataka, treba postojati mogućnost stavljanja tog uzorka na „listu poništenja“ kako bi se mogao napraviti novi da se zamjeni sa kompromitiranim.

- **Sigurnost**

  Oko zaštićene biometrijske karakteristike treba postojati kvalitetna aplikacijska sigurnost kako napadač ne bi bio u mogućnosti da dospije do originala te od njega napravio fizički lažnjak.

- **Kvaliteta izvođenja**

  Kvaliteta izvođenja se odnosi na sve fizičke i softverske module koje čine biometrijski sustav. Shema zaštite biometrijskog uzorka ne bi smjela narušiti kvalitetu izvođenja biometrijskog sustava u smislu FAR i FRR mjerila.



Slika 11. Kategorizacija shema zaštite uzoraka (Izvor: [21], str. 401)

Glavni izazov prilikom izrade sheme za zaštitu biometrijskih uzoraka jest pokrivanje varijabilnosti prilikom preuzimanja primjera biometrijske karakteristike. Na primjer, karakteristika otiska prsta od korisnika sustava može varirati te imati različite setove značajki ukoliko se prijavljuje u sustav u više navrata. Zbog tog razloga, biometrijski uzorak se ne može kao takav kriptirati standardnim tehnikama (RSA, AES, itd.) i spremiti u bazu podataka. Enkripcija nije jednostavna funkcija pa bi i mala varijabilnost kod preuzete značajke kada se kriptira rezultirala u velikim razlikama. Zbog toga, standardne enkripcijske tehnike su beskorisne. [16]

Prema autorima [16] i kako je prikazano na slici jedanaest, preporučene sheme se mogu kategorizirati u dvije kategorije, a to su:

- Transformacija značajki
- Biometrijski kripto sustav

U tablici tri prikazane su karakteristike shema za zaštitu uzorka.

Pristup	Što pruža sigurnost uzorku?	Koji entiteti su spremljeni?	Kako su rukovane *intra* klasne varijacije?
Salting	Tajnost ključa *K*	Javna domena: transformirani uzorak *F (T;K)* Tajna: Ključ *K*	Kvantizacija i uparivanje u transformiranoj domeni *M(F (T;K), F(Q,K))*
Neobratljiva transformacija	Neobratljivost transformacijske funkcije *F*	Javna domena: transformirani uzorak *F (T;K),* ključ *K*	Uparivanje u transformiranoj domeni *M(F (T;K), F(Q,K))*
Kripto sustav vezivanjem ključem	Razina sigurnosti ovisi o količini informacije koju otkrivaju pomoćni podaci *H*	Javna domena: pomoćni podaci *H = F (T;K)*	Ispravljanje grešaka i specifična korisnička kvantizacija *K = M(F (T;K),Q)*
Kripto sustav generiranjem ključa	Razina sigurnosti ovisi o količini informacije koju otkrivaju pomoćni podaci *H*	Javna domena: pomoćni podaci *H = F (T)*	Ispravljanje grešaka i specifična korisnička kvantizacija *K = M(F (T),Q)*

Tablica 3. Karakteristike shema za zaštitu biometrijskih uzoraka (Izvor: [21], str. 401)

U tablici tri prikazane sumirane su različite sheme za zaštitu biometrijskih uzoraka. U njoj *T* predstavlja biometrijski uzorak, *Q* predstavlja upit, i *K* predstavlja ključ koji se koristi kako bi se zaštitio uzorak. U *saltingu* i neobratljivoj transformaciji, *F* predstavlja transformacijsku funkciju, dok *M* predstavlja uparivač koji se izvršava u transformiranoj domeni. U biometrijskim kripto sustavima, *F* predstavlja pomoćne podatke ekstrakcijske sheme, a *M* predstavlja grešku ispravljačke sheme koja dopušta rekonstrukciju ključa *K*. [15]

5.3.1. Transformacija značajki

U pristupu transformacije značajki primjenjuje se funkcija transformacije značajki *(F)* na biometrijski uzorak *(T)* i samo se transformirani uzorak *(F (T;K))* sprema u bazu podataka. Parametri transformacijske funkcije su izvedeni iz ključa *(K)* ili lozinke. Ista transformacijska funkcija se primjenjuje na upit značajki *(Q),* a transformirani upit *(F (Q;K))* se direktno uparuje sa transformiranim uzorkom *(F (T;K)).* Nadalje, ovisno o karakteristika transformacijske funkcije, transformacije značajki se kategoriziraju kao *salting* ili kao neobratljive transformacije. [16]

5.3.1.1. Salting

Salting biometrijske karakteristike otiska prsta ili *biohashing* jest pristup gdje se koristi uzorak otiska prsta da bi se izvršila njegova transformacija preko funkcije čiji su parametri definirani sa vanjskim ključem. Takav pristup koristi *RQM* ili *Random Multispace Quantization* koji obuhvaća tri stanja: [21]

1. Projektiranje vektora značajke otiska prsta u nižu dimenzijsku razinu
2. Projektiranje na slučajan set ortogonalnih vektora koji su izvedeni iz vanjskog ključa
3. Kvantizacija individualnih mapa.

Zaštićeni uzorci nisu reverzibilni ukoliko nisu poznati oba uzorka i ključ u isto vrijeme. Međutim, ako je ključ poznat (ili je dovoljno slab da bi mogao biti probijen napadom rječnika), nasumičnost nestaje, a kvantizacija učinkovito ne sačuva zaštićeni uzorak. Ako se izgubi manji dio informacija prilikom kvantizacije, poprilično većina uzorka može biti oporavljeno. Kako bi se poboljšala sigurnost *biohashinga,* prijedlog je da se ključ ne sprema nego da ga korisnik zapamti što ujedno vraća slabost koja se nalazi u shemama baziranim sa lozinkom što se ovdje želi zaobići. [21]

5.3.1.2. Neobratljive transformacije

U ovom pristupu, biometrijski uzorak se zaštićuje tako da se na njega primjenjuje neobratljiva transformacijska funkcija. To se odnosi na jednostavne funkcije koje se „lagano računaju“, ali se „teško preobrnu“. Parametri transformacijske funkcije su definirani ključem koji mora biti dostupan za vrijeme autentikacije da bi se izvršila transformacija set značajki upita. Glavna karakteristika ovog pristupa jest da iako su poznati ključ i transformirani uzorci, vrlo je teško napadaču izvesti napad kako bi se izračunao originalni biometrijski uzorak. [15]

5.3.2. Biometrijski kripto sustavi

Prema autorima [15] to su sustavi koji su napravljeni sa svrhom kako bi osigurali kriptografski ključ koristeći biometrijske karakteristike ili kako bi direktno generirali kriptografski ključ iz biometrijskih značajki. Međutim, mogu se koristiti i kao uzorak zaštite. U biometrijskom kripto sustavu spremaju se neke javne informacije o biometrijskom uzorku. Te informacije se nazivaju „pomoćni podaci“ pa su po tome biometrijski kripto sustavi poznati kao metode bazirane na pomoćnim podacima. Ti podaci su potrebni prilikom uparivanja kako bi se izvukao kriptografski ključ iz upita biometrijskih značajki. Uparivanje se izvodi indirektno verificiranjem Vrijednosti izvučenog ključa.

Nadalje, biometrijski kripto sustavi mogu se klasificirati kao sustavi *vezanja* ključa i sustavi *generiranja* ključa, ovisno o tome kako su pribavljeni pomoćni podaci.

5.3.2.1. Biometrijski kripto sustavi vezivanjem ključa

Biometrijski uzorak je osiguran monolitnim vezivanjem ključa unutar kriptografskog okvira. Entitet koji veže ključ i uzorak sprema se u bazu podataka kao pomoćni podatak. Taj podatak ne otkriva puno informacije o ključu ili biometrijskom uzorku pa je ključ vrlo teško računalno dekodirati bez znanja o biometrijskim podacima samog korisnika. Pomoćni podaci su općenito povezani sa kodom za ispravljanje grešaka i biometrijskim uzorkom. Kada se biometrijski upit razlikuje od uzorka u određenom okviru tolerancije pogreške, asocirana kodna riječ sa sličnom količinom tolerancije na pogrešku može biti oporavljena. Ta riječ se može dekodirati i izvući ugrađen ključ koji ako je točan pokazuje uspješno uparivanje. [15]

5.3.2.2. Biometrijski kripto sustavi generiranjem ključa

Informacije o granicama kvantizacije se spremaju kao pomoćni podaci koji se koriste tijekom autentikacije kako bi se uočila varijacija između stvarnog korisnika i napadača. Glavni zadatak jest da se direktno generira kriptografski ključ iz biometrijskih podataka. [15]

Dodis [22, 23] u svojim radovima predlaže koncepte *secure sketch (i)* i *fuzzy extractor (ii)* u kontekstu generiranja ključa iz biometrijskih karakteristika. Koncept *(i)* iz biometrijske karakteristike izvlači nasumičnost *R.* Izvučeni podaci su tolerantni na pogreške, u smislu da će *R* ostati isti iako se sljedeće uneseni podaci promijene, bitno je da podaci ostaju čim bliže originalu. Koncept *(ii)* stvara javne informacije o biometrijskim unosima *w*, ali pri tom ne otkriva *w.* Dopušta se izvlačenje i oporavljanje *w* ukoliko su uneseni podaci slični prema *w*. Na taj način stvaraju se pouzdani biometrijski unosi bez rizika sigurnosti prilikom njihovih spremanja u bazu podataka.

U primjerima navedenih sustava postavlja se pitanje stabilnosti i entropija ključa. Stabilnost ključa odnosi se na veličinu opsega ponavljanja generiranog ključa iz biometrijskih karakteristika. S druge strane entropija ključa se odnosi na broj mogućih ključeva koji mogu biti generirani iz biometrijske karakteristike. Iako je moguće izvesti ključ direktno iz biometrijskih karakteristika, teško je postići podjednaku visoku entropiju ključa, a da je pritom stabilan.

6. GDPR (Opća uredba o zaštiti podataka)

Prema Europskoj komisiji [24] u *Povelji EU-a o temeljnim pravima* svaki građanin EU-a ima pravo na zaštitu osobnih podataka. Europa želi biti spremna za trenutno digitalno doba te je više od 90% građana Europske unije reklo da želi imati ista prava na zaštitu podataka gdje god se u Europskoj uniji obrađuju njihovi podaci. Tako se dovodi *Opća uredba o zaštiti podataka* (Uredba EU 2016/679) koja govori o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka. Uredba stupa na snagu 24. svibnja 2016., krenula se primjenjivati 25. svibnja 2018. godine.

Prema članku 8. stavkom 3. Povelje EU-a o temeljnim pravima države članice uspostavljaju nacionalna tijela koja su nadležna za zaštitu osobnih podataka. [24]

1. Europski odbor za zaštitu podataka
   Prema [24], Radnu skupinu osnovanu na temelju članka 29. zamijenit će se Europskim odborom za zaštitu podataka. Taj odbor imam status tijela EU-a s pravom osobnošću te ima neovisno tajništvo. Ovlasti tijela sežu do odlučivanja u sporovima između nacionalnih nadzornih tijela, savjetovanje i davanje smjernica o glavnim konceptima *Opće uredbe o zaštiti podatka i Direktive i o policiji*

2. Zaštita podataka u institucijama i tijelima EU-a
   Prema [24], u *Uredbi (EZ) br. 45/2001* utvrđena su pravila koja institucije i tijela EU-a primjenjuju pri obradi osobnih podataka. Uredbom o zaštiti pojedinaca pri obradi osobnih podataka u institucijama Unije uspostavljen je Europski nadzornik za zaštitu podataka koji je zapravo neovisno tijelo EU-a nadležno za praćenje primjene pravila o zaštiti podataka u europskim institucijama i za istraživanje pritužbi. Nadalje, imenovan je službenik za zaštitu podataka koji je nadležan za praćenje i primjenu pravila o zaštiti podataka u Europskoj komisiji. Taj službenik osigurava internu primjenu pravila o zaštiti podataka u suradnji s Europskim nadzornikom za zaštitu podataka

Prema članku 2. stavkom 1. uredbe opisuje se glavno područje primjene uredbe. U tekstu [25] kaže da se Uredba primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

Prema članku 4. opisane su definicije za potrebe Uredbe. Pod brojem 14. navodi se kako „biometrijski podaci“ znače kao osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.

Prema članku 9. u četiri stavka opisano je na koji način se vrši obrada posebnih kategorija osobnih podataka kao što su to npr. Biometrijski podaci. Prema stavku 1. [25] zabranjuje se obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

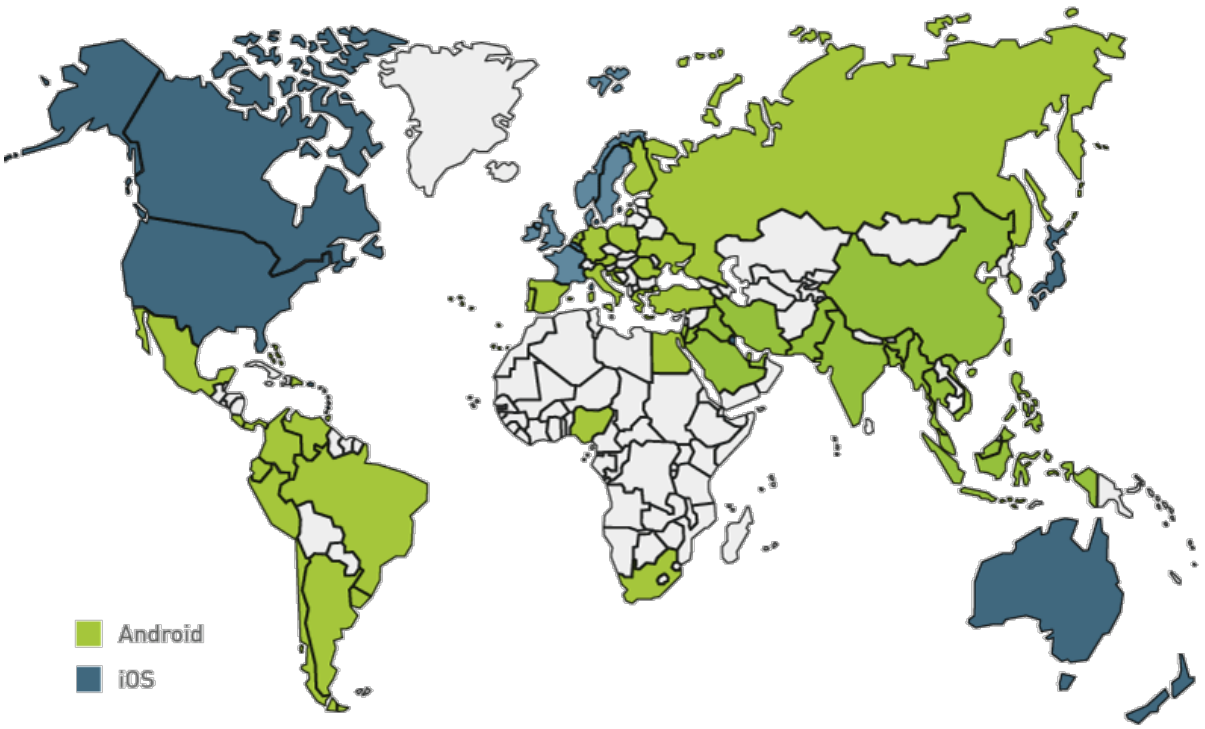
Stavak 1. se ne primjenjuje ako je ispunjen jedan od sljedećih navoda:

1. Ako je ispitanik dao izričitu privolu za obradu tih osobnih podataka
2. Ako je obrada nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava države članice
3. Ako je obrada nužna za zaštitu životno važnih interesa ispitanika
4. Ako se obrada provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela
5. Ako se obrada odnosi na osobne podatke koje je očito da ih je objavio ispitanik
6. Ako je obrada nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva
7. Ako je obrada nužna za potrebe značajnog javnog interesa na temelju prava Unije ili prava države članice koje je razmjerno željenom cilju
8. Ako je obrada nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi
9. Ako je obrada nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju
10. Ako je obrada nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe

Na kraju, države članice mogu zadržati ili uvesti dodatne uvjete, uključujući ograničenja s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje [25]. Uvođenjem ove Uredbe Europska unija uvodi dodatnu sigurnost i zaštitu privatnih podataka za svoje građane. Budući da svakim danom tehnologija napreduje, sve više će se u nju ugrađivati senzori koji prepoznavanju biometrijske karakteristike. Kao što je prije spomenuto, već postoje aplikacije koje omogućuju potvrdu plaćanja verifikacijom oblika lice klijenata, a u budućnosti će možda postojati uređaji koji će prepoznati osjećaje klijenata na obliku lica te im ponuditi proizvod. Svi ti privatni podaci se spremaju u bazu podataka, a ovom Uredbom će se ti podaci dodatno zaštititi. S druge strane, javlja se problem razvijanja takvih aplikacija u kojima je potrebno obratiti posebnu pozornost na zakonske regulative kako ne bi došlo do pravnih nesuglasica. Poduzeća koja se bave razvojem takvih aplikacija morat će ulagati dodatna sredstva u takav način razvoja aplikacija.

7. Analiza sigurnosti i privatnosti Apple i Android organizacija

Današnje stanje na tržištu pametnih uređaja jest da su najpopularnija dva operacijska sustava. Android OS u vlasništvu je Googlea i baziran je na *linux* operacijskog sustavu što znači da je polovično *open source.* iOS je Apple mobilni operacijski sustav koji je u početku bio među prvima koji su se koristili u njihovim pametnim mobilnim uređajima. Kako se tržište razvijalo taj broj se mijenja, ali su ionako dvije organizacije stvorile duopol na tržištu. Prema [26] i podacima iz 2017. godine Android je dominirao tržište s 87%, dok je iOS bio na drugom mjestu s 12% tržišta.



Slika 12. Distribucija iOS i Android operacijskih sustava u svijetu 2017. godine (Izvor: [26])

Slika dvanaest prikazuje rasprostranjenost pojedinog operacijskog sustava gdje se vidi dominacija Androida u zemljama Azije i Afrike koje su u razvitku. S druge strane iOS prednjači u razvijenim zemljama kao što su SAD, Australija i zemlje Europe, a vjerojatno je razlog toga različitosti kulturnih i sociooloških i ekonomskih faktora koji vladaju u navedenim zemljama.

7.1. iOS operacijski sustav

Svakih nekoliko mjeseci Apple izdaje dokument u kojem opisuje koja su poboljšanja napravljena kako bi se poboljšala sigurnost i zaštita podataka koje koriste njihovi uređaji. Najnoviji je izašao u kolovozu 2018. iteracije *iOS 11.4*.

U svojem dokumentu [27] Apple u jezgru razvijanja iOS platforme stavlja sigurnost. Uređaj kombinira softver, hardver i servise koji skupa surađuju pružajući maksimalnu sigurnost. iOS štiti uređaj i podatke kada je nekorišten, kada korisnik na njemu radi lokalno, na mrežama ili koristeći internetske servise. U dokumentu je detaljno opisano kako tehnologija radi te kako su ostala svojstva implementirana u iOS platformi. Dokument je podijeljen u osam poglavlja:

1. Sigurnost sustava
2. Enkripcija i zaštita podataka
3. Sigurnost aplikacija
4. Mrežna sigurnost
5. Apple plaćanje
6. Internet servisi
7. Kontrole uređaja
8. Kontrole privatnosti

7.1.1. Touch ID i Face ID

Apple je među pionirima korištenja biometrijskih karakteristika za identifikaciju korisnika pametnih mobilnih uređaja. U njihove uređaje implementiran je već godinama *Touch ID* sustav za prepoznavanje otiska prsta koji omogućava brži i sigurniji pristup uređajima. Tehnologija očitava podatke otiska prsta pomoću senzora te sa svakim novim korištenjem proširuje mapu već spremljenog otiska prsta.

U novijim uređajima kao što su to iPhone X, javlja se sustav za prepoznavanja lica *Face ID*. Taj sustav prepoznaje svojeg korisnika te otključava telefon jednostavnim pogledom u kameru. Sustav kamere koji sadrži taj mobitel, pomoću naprednih tehnologija točno mapira geometriju lica korisnika. Hvata se pogled i zatim se koriste neuronske mreže za uparivanje i *anti-spoofing*. Prema njihovim riječima, Face ID čuva privatnost korisnika i štiti biometrijske podatke koji su spremljeni u uređaju. [27]

7.1.1.1. Sigurnost

Vjerojatnost kod *Face ID* sustava da nasumična osoba otključa uređaj je 1 u 1.000.000 slučajeva dok s druge strane za *Touch ID* taj slučaj je moguć u 1 od 50.000 slučajeva. Za dodatnu sigurnost, dopušteno je samo pet neuspješnih pokušaja, a onda je potrebno upisati lozinku. Postoji mogućnost greške sustava *Face ID* ukoliko su u pitanju blizanci čiji je oblik lica vrlo sličan te ukoliko su u pitanju djeca mlađa od 13 godina jer njihove crte lica još nisu došle do izražaja. [27]

Touch ID

Senzor za otisak prsta je aktivan jedino dok osjeti otisak prsta koji skenira prst i šalje uzorak do sigurnosne enklave. To je koprocesor koji pruža kriptografske operacije za upravljanje ključem za zaštitu podataka te čuva integritet zaštite podataka iako je jezgra kompromitirana. Podaci koji su poslani u sigurnosnu enklavu ne mogu biti pročitani jer su kriptirani i autenticirani ključem sesije. Ključ sesije se odabire korištenjem dijeljenog ključa koji je dodijeljen svakom *Touch ID* senzoru i njegovoj korespondirajućoj sigurnosnoj enklavi prilikom proizvodnje u tvornici. Dijeljeni ključ je nasumičan, težak za probijanje i drugačiji za svaki *Touch ID* senzor. Skenirani uzorak se privremeno sprema u kriptiranu memoriju sigurnosne enklave uređaja gdje se vektorizira za analizu, a zatim se odbacuje. Zatim, skenirani uzorak se uspoređuje sa stvarnim uzorkom koji je bio spremljen na uređaju. Rezultat se sprema bez informacija identiteta u kriptiranome formatu te može biti pročitan samo od strane sigurnosne enklave uređaja. Također, skenirani podaci se ne šalju Apple organizaciji, niti se spremaju na ostale servise kao što su *iCloud* i *iTunes.* [27]

Face ID

Ideja sustava je bila da se identificira korisnik uređaja s niskom razinom pogrešnog uparivanja i zaobilaženja digitalnih i fizičkih podvala. Kamera uređaja projicira i čita preko 30.000 infracrvenih točaka kako bi se formirala dubinska mapa lica uz 2D infracrvenu sliku. Ti podaci se digitalno potpisuju i šalju u sigurnosnu enklavu uređaja. Kako bi se otkrile digitalne i fizičke podvale, kamera radi nasumične sekvence 2D slika i dubinskog mapiranja te se radi nasumičan uzorak koji je specifičan za svaki uređaj. Slike su spremljene kao matematička reprezentacija u sigurnosnoj enklavi. Uparivanje lica se vrši u sigurnosnoj enklavi koristeći neuronske mreže uspoređivanjem matematičkih reprezentacija spremljenih uzoraka biometrijske karakteristike lica. Podaci koji su spremljeni su kriptirani te su dostupni samo sigurnosnoj enklavi:

- Matematička reprezentacija lica koja je izračunata prilikom prvog postavljanja

- Matematička reprezentacija lica koja je izračunata prilikom otključavanja uređaja, a sustav misli da bi moglo biti korisno prilikom budućih uparivanja.

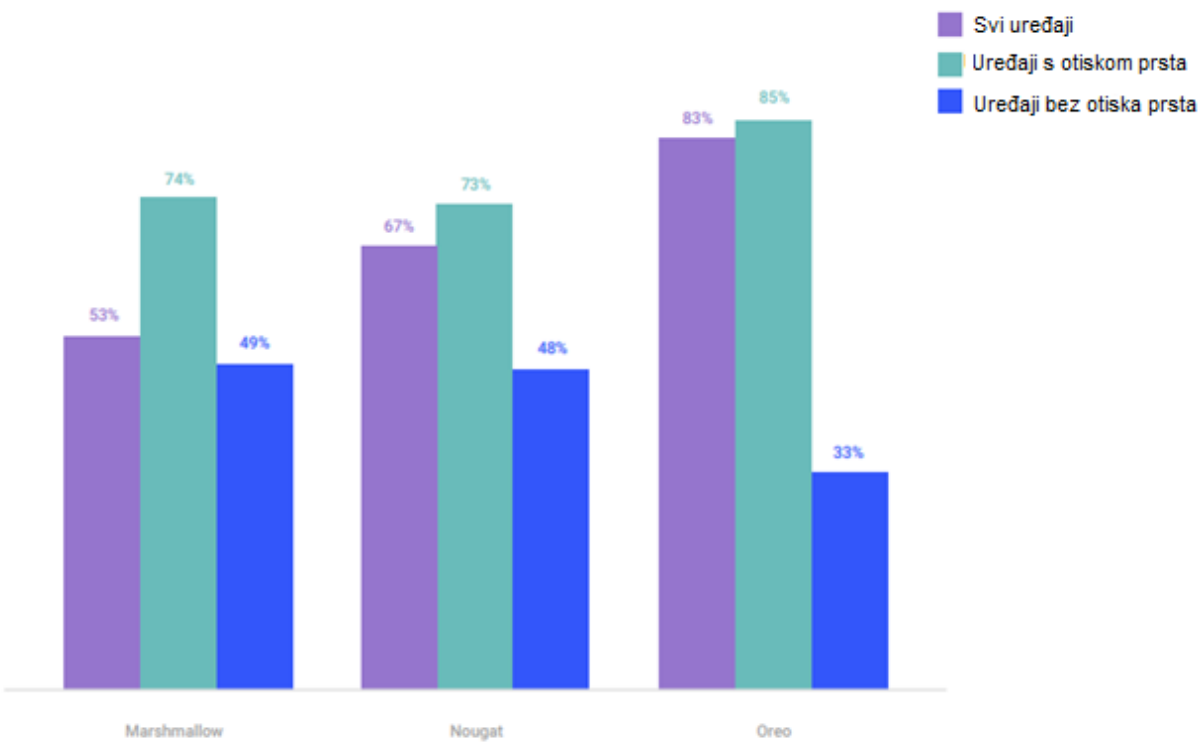
Također kao i kod *Touch ID* tako i ovdje, podaci ne odlaze sa mobilnog uređaja te se ne šalju nikakvim dodatnim servisima. Uhvaćene slike se brišu kada se izvrši njihova matematička reprezentacija. [27]

7.2. Android operacijski sustav

S druge strane tu se nalazi Android operacijski sustav. Na svojim službenim stranicama objavljuju godišnji pregled Android sigurnosti na njihovoj platformi. U dokumentu [28] u šest poglavlja navode se najvažnije promjene i statistički podaci te novosti koji su se dogodili u prethodnoj godini:

1. Pregled
2. Google Play Protect
3. Sigurnost Android platforme
4. Podaci ekosistema
5. Naglasci PHA obitelji
6. Priznanja

Što se tiče biometrijskih karakteristika, u dokumentu [28] se spominje da se od verzije operacijskog sustava Android 6.0 dodala podrška za uređaje koji imaju senzore otiska prstiju. To je potaklo više korisnika da postave sigurniji zaključani ekran (PIN, lozinka, uzorak). Prije te instance više od pola Android uređaja nije uopće imalo postavljen siguran ekran. Može se zaključiti da su ljudi prihvatili sigurnost preko biometrijskih karakteristika pa kako je vrijeme prolazilo sve više uređaja koji podržavaju Android operacijski sustav je počelo implementirati senzore za otisak prsta. Od 2017. 85% Android 8.0 (Oreo) uređaja koristi siguran zaključani ekran pomoću senzora za otisak prsta što možemo vidjeti prikazano na slici 13.



Slika 13. Uređaji koji imaju siguran zaključani ekran prema izdanjima Android operacijskih sustava (Izvor: [28])

Budući da je Android *open source* projekt, na njihovim „Source“ stranicama možemo vidjeti cijeli kod, biblioteke i svojstva koja se mogu koristiti prilikom izrade novih aplikacija. Tako postoji i dio autentikacije koji opisuje na koji način se vrši autentikacija korisnika prilikom otključavanja uređaja.

7.2.1.1. Autentikacija

Za autentikaciju, Android koristi koncept korisničkog autenticiranja preko čuvanih kriptografskih ključeva. Za to potrebne su komponente: [29]

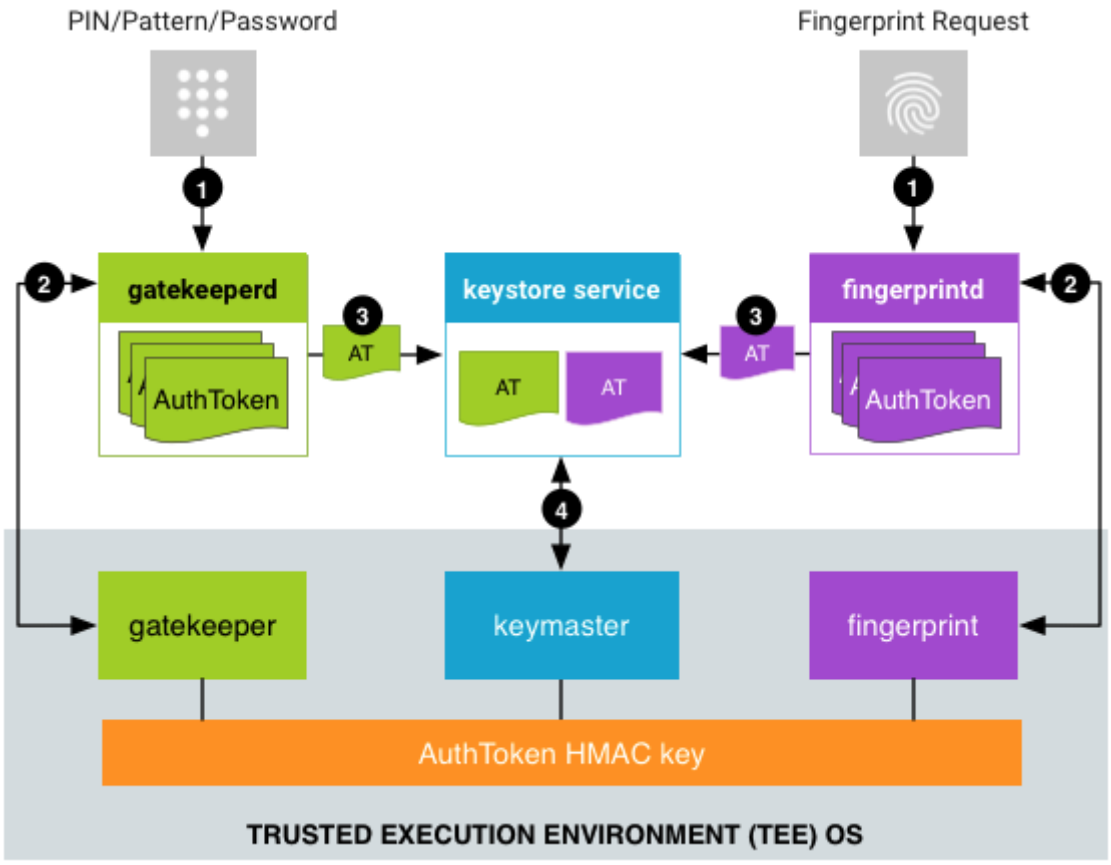
- **Skladištenje kriptografskih ključeva i usluga servisa**
  Na razini hardvera, Android omogućuje spremanje ključeva za kriptografske servise. *Trusted Execution Environment (TEE)* ili *Secure Element (SE)* mogu biti uključeni
- **Korisnički autentikatori**
  Android koristi *Gatekeepere* za PIN/uzorak/lozinku i otisak prsta za autentikaciju korisnika. Uređaji koji koriste sustav Android 9 mogu koristiti *BiometricPrompt* za integraciju otiska prsta ili neke druge biometrijske

karakteristike za koje postoji senzor. Te komponente međusobno komuniciraju o stanju preko autenticiranog kanala *Android Keystore system.*

Gatekeeper, otisak prsta i ostale biometrijske komponente rade sa *Keystore* i ostalim komponentama kako bi se podržali hardverski autenticirani tokeni (*AuthTokens).*

Tijek autentikacije

Korisnik na Android uređaju koji koristi biometrijsku karakteristiku otiska prsta opisan je u četiri koraka. Prema [29] 1. korisnik pruža autentikacijsku metodu i asocirani servis te radi zahtjev prema asociranom demonu. Tako *FingerprintService* ili *BiometricPrompt* radi zahtjev prikladnom biometrijskom demonu koristeći *BiometricManager* klasu. Autentikacija se vrši asinkrono nakon što je zahtjev poslan. Nakon toga 2. demon šalje odgovarajuće podatke slijedniku gdje se generira AuthToken. Demon 3. natrag prihvati potpisani AuthToken te ga šalje servisu koji čuva ključeve. Na kraju, 4. baza sa ključevima šalje potpisane AuthTokene prema Keymateru kako bi se verificirali koristeći dijeljeni ključ sa *Gatekeeperom* i podržanom TEE komponentom. *Keymaster* vjeruje zadnjoj vremenskoj oznaci kao zadnjem vremenu autentikacije te na temelju toga bazira odluku otpuštanja ključa.



Slika 14. Tijek autentikacije u Android operacijskom sustavu (Izvor: [30])

Fingerprint HAL

Android [30] koristi Fingerprint Hardware Abstraction Layer (HAL) kako bi se spojio sa bibliotekom uređaja i hardverom za otisak prsta kao što je to senzor za otisak prsta. Senzor je većinu vremena besposlen, ali kada se pozove autentikacija ili inicijalni upis korisnika, senzor čeka dodir. Budući da je ta biblioteka slobodna za korištenje programerima su napisane upute kako ne bi došlo do sigurnosnih propusta prilikom brisanja korisnika s uređaja:

1. Podaci otiska prsta ili izvedenice (uzorci) nikada ne smiju biti dostupni izvan senzora ili TEE.
2. Preuzimanje otiska prsta, upis, ili prepoznavanje uzorka mora se vršiti unutar TEE.
3. Samo kriptirani izvučeni podaci iz otiska prsta mogu biti spremljeni u sustav.
4. Uzorci otiska prsta moraju biti potpisani privatnim ključem koji je specifičan za svaki uređaj.
5. Implementacije moraju koristiti putanju koja pruža *set_active_group()* funkcija ili moraju implementirati način kojim će se obrisati podaci uzoraka svih korisnika.

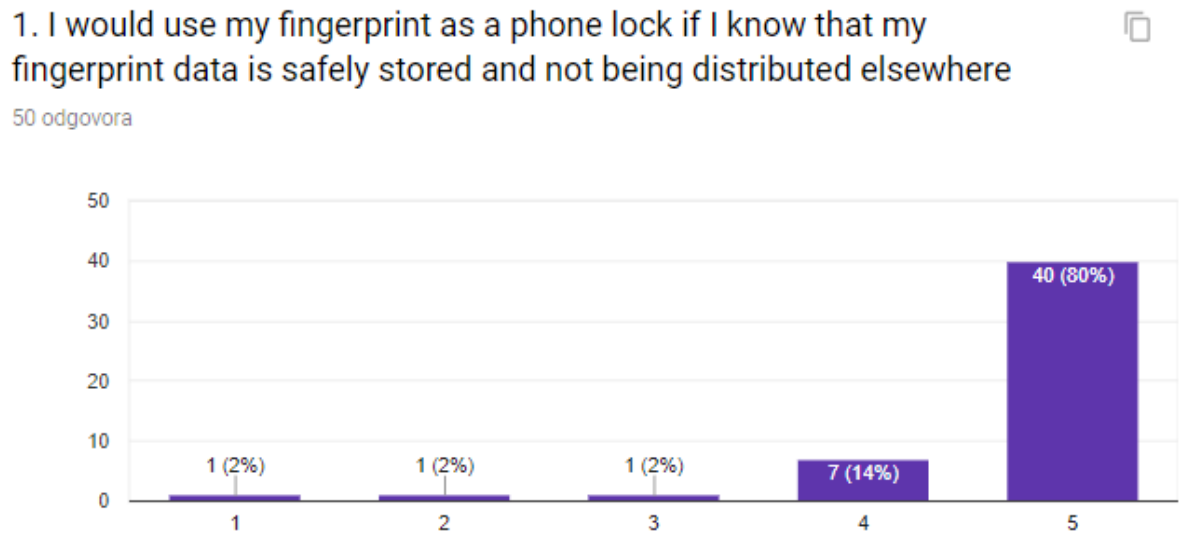
8. Anketa

Provela se online anketa od 8 pitanja na uzorku od 50 ispitanika kako bi se vidjelo razmišljanje prema upotrebi biometrijskih karakteristika umjesto lozinke, zaštite biometrijskih podataka na uređajima, distribucija biometrijskih podataka od strane velikih organizacija te dopuštenje korištenja biometrijskih podataka u drugim aplikacijama.

Rangiranje odgovora se provodi u brojevi od 1 do 5 koji svaki od njih znači:

1. Uopće se ne slažem
2. Djelomično se ne slaže
3. Niti se slažem niti se ne slažem
4. Djelomično se slažem
5. U potpunosti se slažem

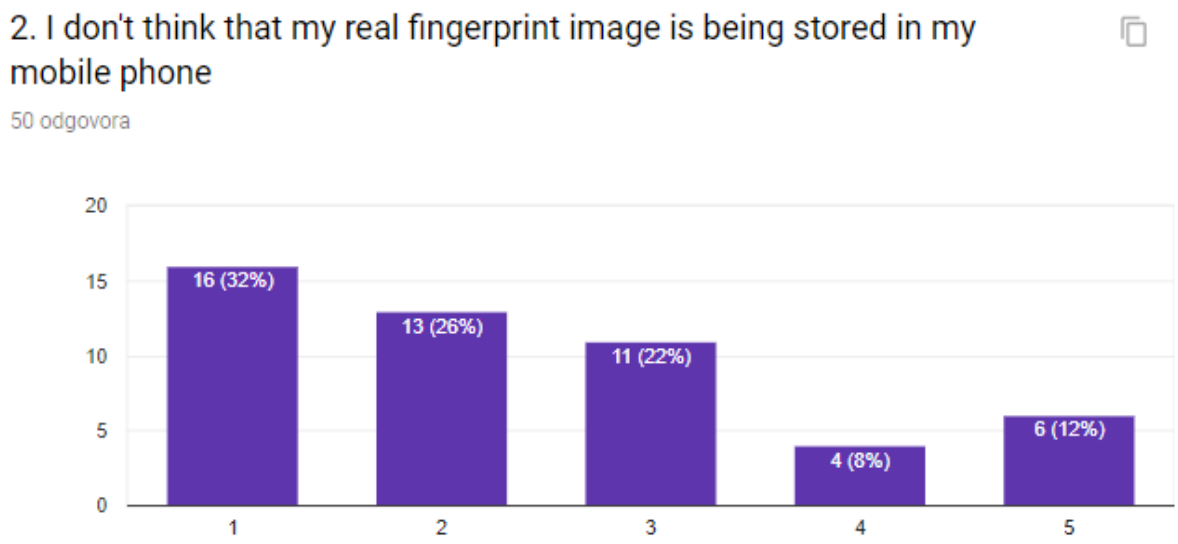
Pitanja su sastavljena na engleskom jeziku jer se anketa distribuirala u organizaciji *Searchmetrics Gmbh*, čije je sjedište u Berlinu, a službeni jezik poduzeća je engleski. Također, anketa se distribuirala studentima Fakulteta organizacije i informatike i Medicinskog fakulteta u Zagrebu.



Slika 15. Prikaz rezultata ankete na izjavu: "Koristio bih otisak prsta za zaključavanje mobitela ukoliko znam da biometrijski podaci otiska prsta zaštićeni na uređaju te se ne šalju nigdje drugdje.“

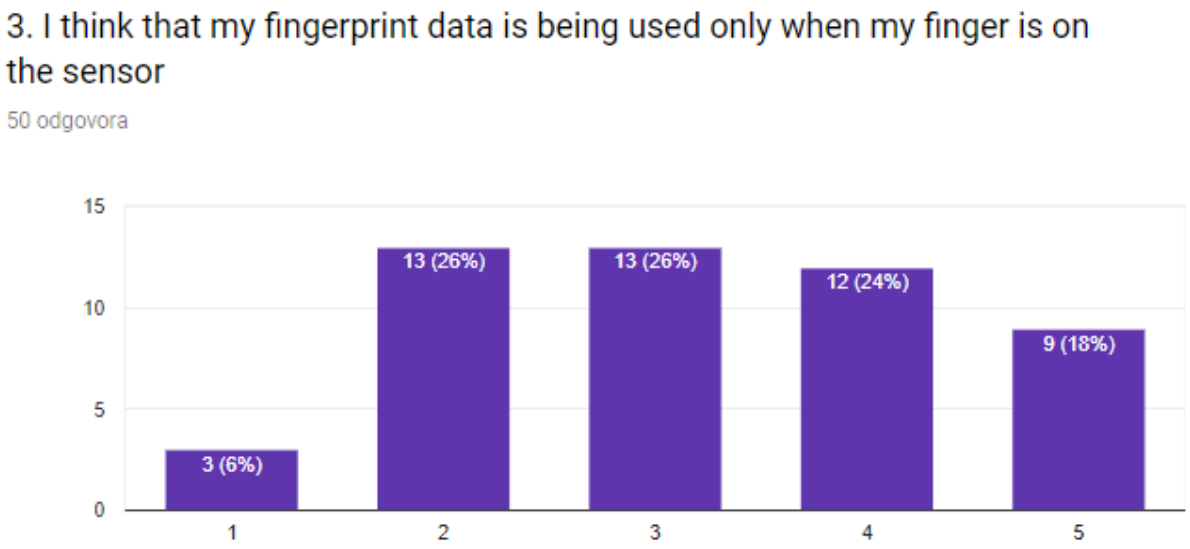
Prijevod prvog pitanja jest: „Koristio bih otisak prsta za zaključavanje mobitela ukoliko znam da biometrijski podaci otiska prsta zaštićeni na uređaju te se ne šalju nigdje drugdje.“ To pitanje je postavljeno u smislu da li bi korisnik odabrao zaključavanje uređaja otiskom prsta ukoliko biometrijski podaci koji se koriste za izvršavanje procesa ne bi bili distribuirani bilo gdje drugdje

osim na uređaju korisnika. To pitanje je i jedino pitanje na koje je od 50 ispitanika čak 80% odgovorilo da se u potpunosti slažu s tom izjavom što znači da je korištenje biometrijskih karakteristika za verifikaciju korisnika vrlo popularna.



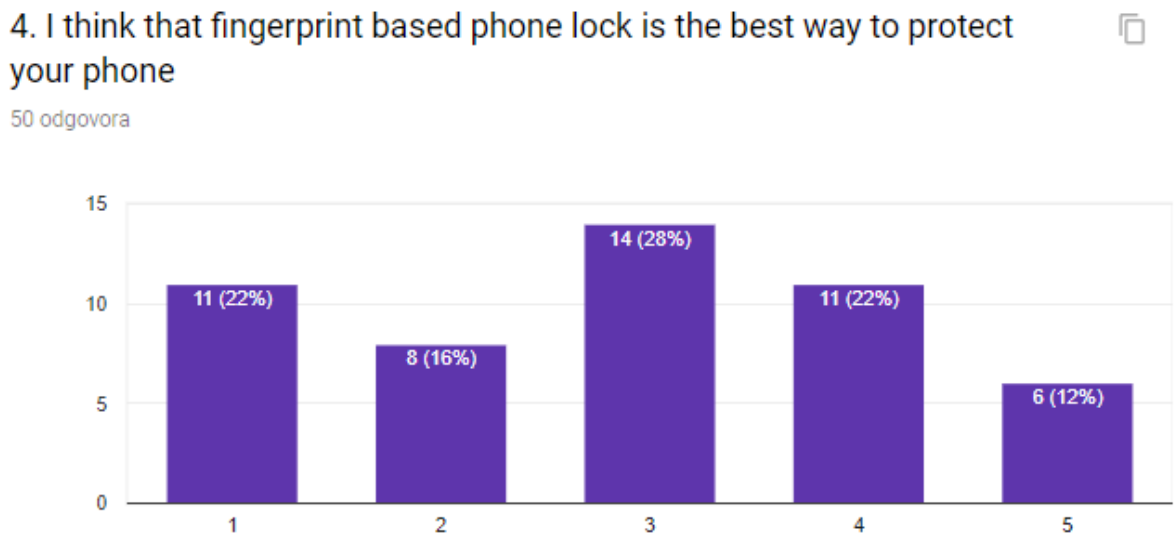
Slika 16. Prikaz rezultata ankete na izjavu: „Ne mislim da se stvarna slika mojeg otiska prsta sprema na mobitel.“

Sljedeća izjava „Ne mislim da se stvarna slika mojeg otiska prsta sprema na mobitel.“ je bila postavljena ispitanicima da se vidi koliko su upoznati sa načinom na koji se vrši verifikacija otiska prsta korisnika. Prema rezultatima 32% ispitanika se uopće ne slaže s tom izjavom, 26% se djelomično ne slaže s tom izjavom, a 22% se niti slaže niti ne slaže s tom izjavom. Prema tim rezultatima možemo zaključiti da većina ispitanika ne zna na koji način se vrši verifikacija, odnosno da ne znaju da se biometrijska karakteristika otiska prsta transformira u matematičku reprezentaciju koja je kriptirana.



Slika 17. Prikaz rezultata ankete na izjavu: „Mislim da se biometrijski podaci otiska prsta koriste samo kada je moj prst na senzoru.“

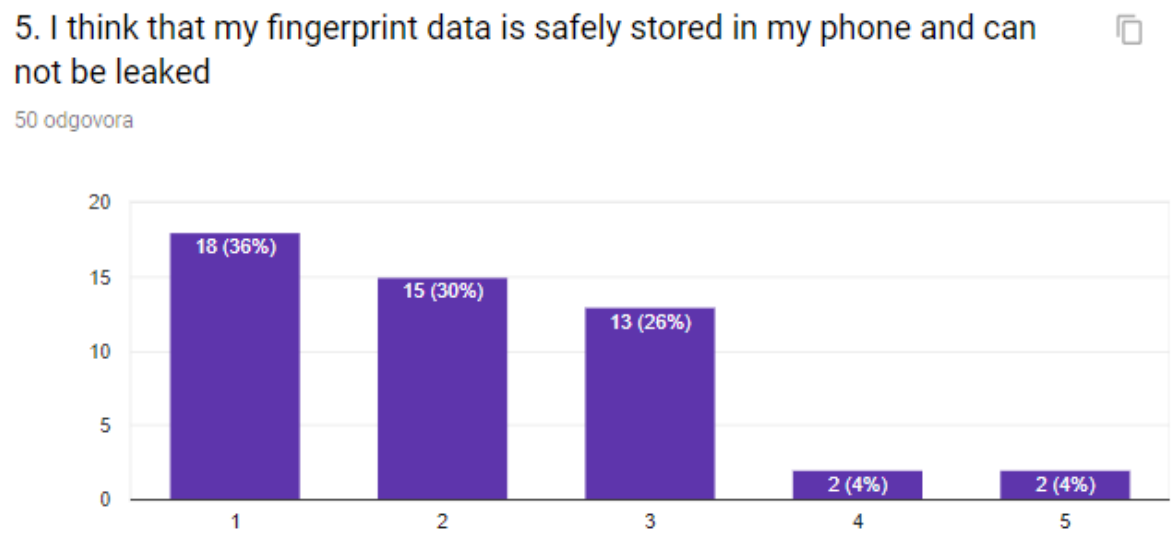
Izjava „Mislim da se biometrijski podaci otiska prsta koriste samo kada je moj prst na senzoru.“ je također bila postavljena da se još detaljnije vidi koliko su korisnici upoznati na koji način funkcionira verifikacija. Prema rezultatima na slici sedamnaest možemo vidjeti da 42% ispitanika naginje odgovorima broj četiri ili pet što znači da se većina slaže sa navedenom izjavom. Međutim, važno je spomenuti da čak 26% ispitanika uopće nije upoznato s navedenom izjavom te se s njom niti slaže niti ne slaže.



Slika 18. Rezultati ankete na izjavu: „Mislim da je zaključavanje mobitela bazirano na otisku prsta najsigurniji način zaštite mobitela.“

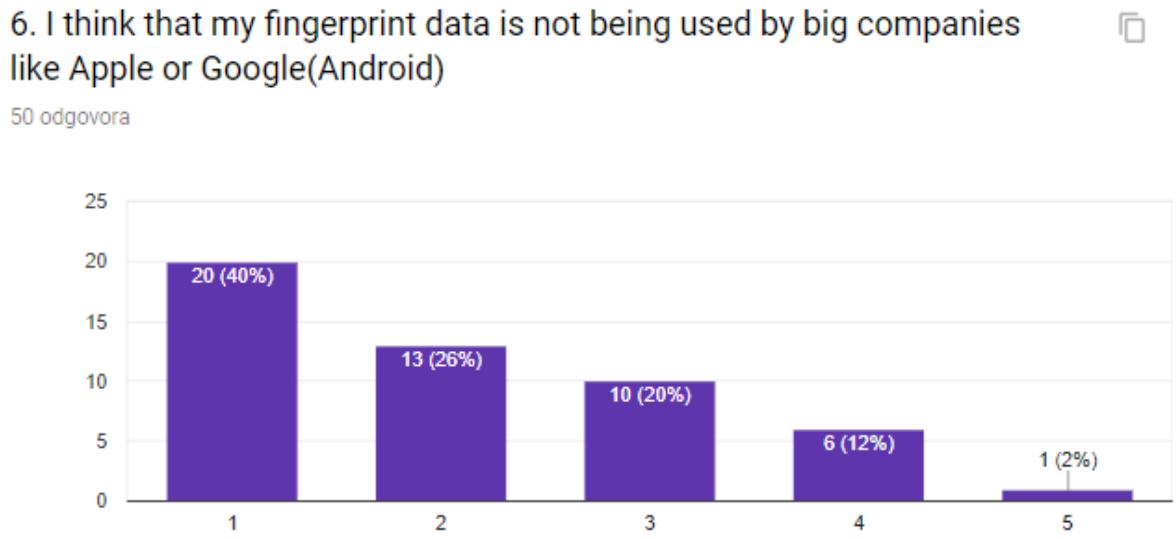
Izjava broj četiri „Mislim da je zaključavanje mobitela bazirano na otisku prsta najsigurniji način zaštite mobitela.“ ispitanike je htjelo navesti na zaključak koliko vjeruju načinu zaključavanja mobitela biometrijskom karakteristikom da im nitko ne može provaliti u njihov uređaj. Na ovu izjavu rezultati su podjednaki što znači da se 38% ne slaže s tom izjavom, a

34% se slaže. Detaljnijom analizom vidi se da se 22% uopće ne slaže s tom izjavom, a 22% se djelomično slaže sa izjavom pa iz toga možemo tanko zaključiti da je ipak mišljenje da ispitanici nisu baš sigurni da je to najbolji način kako bi se zaštitio mobilni uređaj.



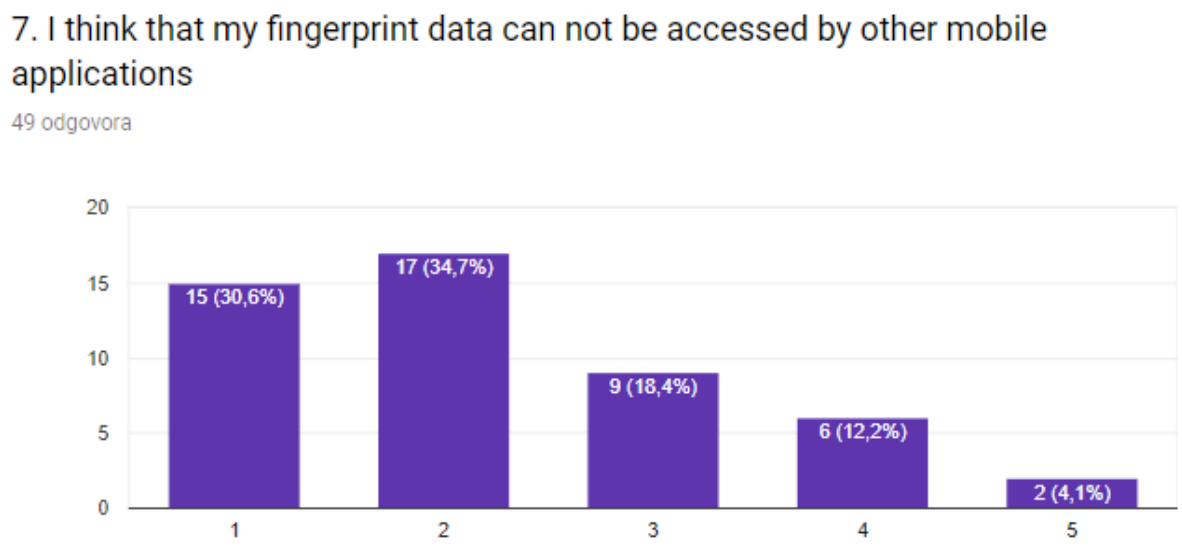
Slika 19. Rezultati ankete izjave: „Mislim da su biometrijski podaci otiska prsta sigurni na mobitelu i ne može se dogoditi curenje informacija.“

Izjavom pet „Mislim da su biometrijski podaci otiska prsta sigurni na mobitelu i ne može se dogoditi curenje informacija.“ željelo se vidjeti koliko ispitanika vjeruje misli da biometrijski podaci koji se koriste za verifikaciju ne mogu biti izloženi napadu kako bi procurili. Zanimljivo je da se čak 66% ispitanika ne slaže s tom izjavom i misle da postoji mogućnost da njihovi podaci, ukoliko dođe do napada, mogu biti izloženi javnosti. Također, zanimljivo je da 26% ispitanika nema mišljenje, a samo četiri ispitanika vjeruje da su podaci veoma sigurni na njihovim uređajima.



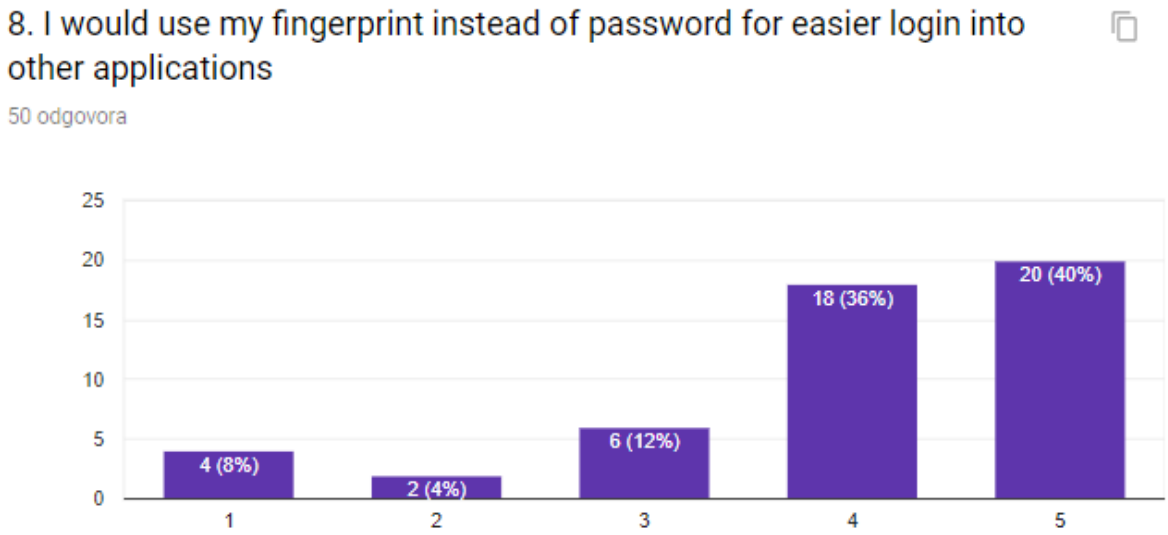
Slika 20. Rezultati ankete izjave: „Mislim da moje biometrijske podatke ne koriste velike organizacije kao što su Apple i Google (Android).“

„Mislim da moje biometrijske podatke ne koriste velike organizacije kao što su Apple i Google (Android).“ je izjava broj šest u kojoj se ispitanike htjelo navesti na odgovor iz kojeg možemo zaključiti koliko vjeruju proizvođačima mobilnih uređaja koji barataju njihovom privatnošću i osobnim podacima. Ovdje također 66% ispitanika naginje na stranu da se ne slaže sa navedenom izjavom, ali je važno napomenuti da od tih 66%, 40% ispitanika se uopće ne slaže s navedenom izjavom. Ti rezultati se mogu povezati nedavnom aferom Facebooka gdje je bilo otkriveno da Facebook koristi osobne podatke korisnika kako bi mogli bolje personalizirati oglase.



Slika 21.Rezultati ankete izjave: „Mislim da ostale aplikacije nemaju pristup biometrijskim podacima otiska prsta.“

„Mislim da ostale aplikacije nemaju pristup biometrijskim podacima otiska prsta.“ Ovom izjavom također se htjelo vidjeti što misle ispitanici, imaju li ostale aplikacije pristup njihovim biometrijskim podacima. Opet u većini od 66% ispitanici odgovaraju da se ne slažu s tom izjavom i misle da aplikacije imaju pristup osobnim biometrijskim podacima što nije točno.



Slika 22. Rezultati ankete izjave: „Koristio bih otisak prsta umjesto lozinke za lakši pristup aplikacijama.“

„Koristio bih otisak prsta umjesto lozinke za lakši pristup aplikacijama.“ je izjava osam na koju su ispitanici dali vrlo zanimljivi odgovor. Uz sve sumnje u velike organizacije i vjerovanja da njihovi biometrijski podaci nisu sigurno i skloni curenju u javnost te da ostale aplikacije mogu imati pristup njihovim biometrijskim podacima, čak 76% ispitanika se slaže sa navedenom izjavom. Većina bi ispitanika uz mane za koje misle da su realne i dalje radije

koristilo biometrijsku karakteristiku otiska prsta za verifikaciju. Te rezultate možemo povezati sa sve većim rastućim trendom uređaja koji imaju senzore za biometrijsku verifikaciju.

9. Zaključak

Razvojem novih i usavršavanjem sadašnjih tehnologija sve više će se primjenjivati biometrijske karakteristike u novim uređajima i šire. Učinkovite, brze i sigurne verifikacije, senzori, obavljanje brzih transakcija bez upotrebe PIN broja ili lozinke samo su neki procesi koji mogu biti pojednostavljeni. U nadležnoj budućnosti biti će osnova da uređaj ima neku od biometrijskih karakteristika za verifikaciju korisnika Uređaja. Prema anketi koja je provedena može se vidjeti da korisnici žele jednostavnije verificiranje na svojim uređajima, a čak se može vidjeti i trend rasta želje zamjene lozinke sa biometrijskim karakteristikama.

Međutim, budući da su biometrijske karakteristike jedinstvene i ukoliko je ona kompromitirana, ne može se lako zamijeniti kao lozinka. Javlja se problem sigurnosti što prema anketi koja je provedena sami korisnici uređaja s biometrijskim karakteristikama znaju vrlo malo ili uopće nisu upoznati s time. Zbog toga, tu je Europska unija i države članice koji postavljaju zakonske regulative kako bi zaštitili svoje građane. Također, postoji velika odgovornost organizacija koje izrađuju operacijske sustave da vode brigu o privatnosti i sigurnosti njihovih korisnika. Izdavanjem izvještaja o sigurnosti Apple i Google (Android) organizacija koji prikazuju pregled poboljšanja i usavršavanja samih sustava a time i njihovih sigurnosti rezultat je zakonskih regulative, ali ponekad i propusta.

S pozitivne strane, ukoliko se vodi ozbiljna zaštita biometrijskih karakteristika i ukoliko su postavljene kvalitetne zakonske regulative prema kojima će velike organizacije i proizvođači aplikacija morati voditi računa, sam korisnik će biti zaštićen. Kao rezultat toga korištenje biometrijskih karakteristika će imati vrlo blistavu budućnost.

Popis literature

[1.] Techcrunch (2017.) *Alibaba debuts 'smile to pay' facial recognition payments at KFC in China*, https://techcrunch.com/2017/09/03/alibaba-debuts-smile-to-pay. Pristupljeno 11. Travnja 2018.

[2.] Jain A.,K., Flynn P., Ross A., A. (2008.) *Handbook of Biometrics,* New York, NY 10013, USA: Springer Science + Business Media*, 978-0*-387-71041-9.

[3.] Liu, S., Silverman, M. (2001.), A Practical Guide to Biometric Security Technology, *Security IT Pro,* Siječanj | Veljača 27- 32*.*

[4.] Sareen, P. (2014.), Biometrics – Introduction, Characteristics, Basic technique,its Types and Various Performance Measures, *Department of Computer Applications,Baddi University of Emerging Sciences & Technology, India, International Journal of Emerging research in Management & Technology* 3 | 4, 109-119.

[5.] Jain, A., K., Bolle, R., Pankanti, S. (2006.), *BIOMETRICS Personal Identification in Networked Society,* New York, NY 10013, USA: Springer Science + Business Media,, 978-0387-28539-9.

[6.] Prabhakar, S., Pankanti, S., Jain, A.,K. (2003.) Biometric Recognition: Security and Privacy Concerns, *Securtity and Privacy Magazine,* 33-42.

[7.] Sharifah, M., S., A., Borhanuddin M., A., Wan Azizun, W., A., (2012.), Technical Issues and Challenges of Biometric Applications as Access Control Tool of Information Security, *International Journal of Innovative Computing, Information and Control,* Izdanje 8, Broj 11, 7983-7999.

[8.] Jain, A., K., Hong, L., Kulkarni, Y. (1999.), A Multimodal Biometric System Using Fingerprint, Face and Speech, *Department of Computer Science and Engineering Michigan State University*

[9.] Panachal, T., Singh A. (2013.), Multimodal Biometric System, *International Journal of Advanced Research in Computer Science and Software Engineering, Izdanje 3, Broj 5, 1360-1363*

[10.] Das, R. Multimodal biometric systems, http://keesingjournalofdocuments.com/content/General_interest/KJDI_2012_37_Das.pdf, pristupljeno 20. svibnja 2018.

[11.] W., A. Parent (1983.), Privacy, Morality and the Law, *Philosophy & Public Affairs,* Izdanje 12, Broj 4, 269-288

[12.] Thakkar, D. (2017.), How Different Techniques Are Leveraged To Secure Biometric Data, https://www.bayometric.com/techniques-secure-biometric-data/ ,pristupljeno 15. lipnja 2018.

[13.] Grawrock, W. D. (2004.), Portable Token Controlling Trusted Environment Launch, *United States Patent Application Publication,* broj izdanja: US 2004/0117318 A1, datum izdavanja: 17. lipnja 2004.

[14.] Singh S., K., (2011.), *Database Systems: Concepts, Design and Applications,* Pearson Education india, 8131760928, 9788131760925

[15.] Jain, K., A., Nandakumar K., Nagar A., (2007.), Biometric Template Security, *Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Procesing,* Izdanje 2008, Članak ID 579416, 17 str., doi: 10.1155/2008/579416

[16.] N. K. Ratha, J. H. Connell, and R. M. Bolle, *An analysis of minutiae matching strength*, in Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01), pp. 223–228, Halmstad, Sweden, June 2001.

[17.] K. Ishikawa (1976.), Guide to Quality Control, Nordica International, Tokyo, Japan.

[18.] Li, S. Z., & Jain, A. (2015). Encyclopedia of biometrics. Springer Publishing Company, Incorporated.

[19.] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media.

[20.] Schneier, B. (1999). The uses and abuses of biometrics. Communications of the ACM, 42(8), 136-136.

[21.] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

[22.] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith (2006.), "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," Tech. Rep. 235, Cryptology ePrint Archive.

[23.] Y. Dodis, L. Reyzin, and A. Smith (2004), "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '04), vol. 3027 of Lecture Notes in Computer Science, pp. 523–540, Interlaken, Switzerland

[24.] Europska komisija (2018), Zaštita podataka u EU, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_hr, pristupljeno 25. kolovoza 2018.

[25.] Europski parlament i vijeće (2016), Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN, pristupljeno 26. kolovoza 2018.

[26.] Katariya J. (2017), Apple Vs Android – A comparative study 2017, https://android.jlelse.eu/apple-vs-android-a-comparative-study-2017-c5799a0a1683 , pristupljeno 26. kolovoza 2018.

[27.] Apple (2018), iOS Security, iOS 11.4, https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf, pristupljeno 26. kolovoza 2018.

[28.] Android (2017), Android Security 2017 Year In Review, https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf, pristupljeno 26. kolovoza 2018.

[29.] Source (2018), Authentication, https://source.android.com/security/authentication/, pristupljeno 26. kolovoza 2018.

[30.] Source (2018), Fingerprint HAL, https://source.android.com/security/authentication/fingerprint-hal, pristupljeno 26. kolovoza 2018.

Popis slika

Popis tablica