Metode autentikacije korisnika

Nađ, Stjepan

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:937102

SVEUČILIŠTE U ZAGREBU
EKONOMSKI FAKULTET ZAGREB

MENADŽERSKA INFORMATIKA

METODE AUTENTIKACIJE KORISNIKA: PREDNOSTI I IZAZOVI BIOMETRIJSKE TEHNOLOGIJE

Diplomski rad

Stjepan Nađ

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
EKONOMSKI FAKULTET ZAGREB

MENADŽERSKA INFORMATIKA

METODE AUTENTIKACIJE KORISNIKA:

PREDNOSTI I IZAZOVI BIOMETRIJSKE TEHNOLOGIJE

USER AUTHENTICATION METHODS: ADVANTAGES AND CHALLENGES OF BIOMETRIC TECHNOLOGY

Diplomski rad

Student: Stjepan Nađ, 0067553068

Mentor: Dr.sc. Mario Spremić

Zagreb, rujan 2022.

STJEPAN NAD
Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je DIPLOMSKI RAD (vrsta rada) isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu, 15.9.2022.

Stjepan Nad
(potpis)

SAŽETAK

Kontrole pristupa. metode autentikacije i biometrijske tehnologije dio su šireg područja informacijske sigurnosti. Razvoj informacijskih tehnologija zahtijevao je i razvoj sigurnosnih tehnologija za informacijske sustave. Kontrole pristupa i metode autentikacije važne su sastavnice informacijske sigurnosti sa funkcijom ograničavanja pristupa na pojedince kojima je pristup dozvoljen. Kao najsuvremenija metoda autentikacije ističe se biometrijska tehnologija koja se bazira na fizičkim ili bihevioralnim karakteristikama pojedinca u svrhu utvrđivanja njegovog identiteta. Rad obrađuje razvoj i primjenu biometrijskih tehnologija u suvremeno doba te prikazuje rezultate istraživanja o poimanju biometrijskih tehnologija u društvu. Istraživanje provedeno među mladom populacijom pokazuje visoku razinu poznavanja barem nekih biometrijskih metoda, generalnu otvorenost mladeži prema biometrijskim tehnologijama , ali upućuje i na određenu mjeru opreza i skeptičnosti prema biometrijskim tehnologijama.

KLJUČNE RIJEČI:

Informacijske tehnologije, Informacijska sigurnost, Kontrole pristupa, Metode autentikacije Biometrijska tehnologija

ABSTRACT

Access controls, authentication methods and biometric technologies are part of the broader field of IT securtiy. Developement of information technologies has demanded the developement of security technologies for information systems. Access controls and authentication methods are important components of information security that serve for limiting of access to the individuals who have the permission to access. The most modern method of authentication is biometric technology, which is based on the physical or behavioral characteristics of an individual for the purpose of establishing his identity. The paper deals with the development and application of biometric technologies in modern times and presents the results of research on the perception of biometric technologies in society. The research conducted among the young population shows a high level of familiarity with at least some biometric methods, the general openness of young people towards biometric technologies, but also indicates a certain measure of caution and skepticism towards biometric technologies.

KEY WORDS: Information technologies, Information security, Access controls, Authentication methods, Biometric technology

Sadržaj

1. Uvod

1.1. Predmet i cilj rada

Diplomski rad bavi se metodama autentikacije korisnika s fokusom na biometrijsku tehnologiju. Metode autentikacije korisnika vrlo su važan aspekt informacijske sigurnosti, a biometrijska tehnologija predstavlja jedan od načina na koji se autentikacija izvršava. Rad pruža uvod u svijet informacijske sigurnosti, opisuje ulogu kontrola pristupa i metoda autentikacije te se na poslijetku fokusira na biometrijsku tehnologiju koju obrađuje u teoriji i kroz praktično istraživanje. Cilj rada jest upoznati čitatelja s nekim konceptima informacijske sigurnosti i biometrijske tehnologije te prokomentirati društvene stavove prema biometrijskoj tehnologiji. Sukladno tome, radom se želi skrenuti pozornost na važnost informacijske sigurnosti i osvjestiti stručnu javnost o suvremenim trendovima u ovome području.

1.2. Izvori podataka i metode prikupljanja

Izvori podataka korištenih u radu su knjige, znanstveni članci, internetske stranice te druge publikacije. Izvori su prikupljani selekcijom radova čiji se naslovi čine relevantnim za obradu ove teme, a jedan dio izvora sugestija je mentora rada. Podaci korišteni u poglavlju koje se bavi istraživanjem percepcije biometrijske tehnologije u društvu jesu primarni podaci koje je sakupio autor putem internet anketa. Pitanja iz ankete jednim su dijelom preuzeta iz prošlih radova, a jednim dijelom su osmišljena od strane autora rada.

1.3. Sadržaj i struktura rada

Rad je podijeljen u 6 poglavlja od kojih je prvi uvodni dio. Prva tema koja se obrađuje odnosi se na informacijsku sigurnost kako bi se čitatelja uvelo u širi kontekst rada. Sljedeće poglavlje bavi se kontrolama pristupa i metodama autentikacije kao užeg pojma informacijske sigurnosti. Ono daje kontekstualni uvod u četvrto poglavlje koje se bavi razvojem, principom rada i primjerima korištenja biometrijske tehnologije. U petom poglavlju obrađuju se rezultati istraživanja o percepciji biometrijske tehnologije u društvu nakon čega slijedi zaključak rada.

2. Informacijska sigurnost

2.1. O informacijskoj sigurnosti

Svaki se čovjek s vremena na vrijeme prisjeti nekih događaja ili perioda u svojoj prošlosti i imajući njih na umu razmišlja o svojoj mladosti. Većina ljudi, neki prije, a neki kasnije, u tom nekom mladenačkom vremenu iskusila je i prve simpatije kojih se možda sa osmjehom prisjeća. Neki su njihova imena čuvali samo za sebe. S druge strane, Marko je ipak priznao svom prijatelju Mihaelu da mu se sviđa Lucija, uz obavezan uvjet da o tome nikome ne govori. No, kako je to isto priznanje u obliku informacije stiglo do Mihaela, Marko može početi razmišljati o sljedećim pitanjima: Je li moja privatna informacija sada kompromitirana? Može li curenje informacije u javnost naštetiti mom ugledu? Je li bilo neophodno da Mihael zna za taj dio moje privatnosti? Mogu li zapravo biti siguran da Mihael nikako neće odati tajnu? Drugim riječima, Marko se suočava sa izazovima informacijske sigurnosti.

Whitman i Mattord (2017.) u svojoj knjizi definiraju informacijsku sigurnost kao „zaštitu povjerljivosti, cjelovitosti i dostupnosti informacijske imovine, bilo da su pohranjene, u fazi procesiranja ili prijenosa, a putem politika, edukacije, uvježbavanja, podizanja svjesnosti i tehnologije."

Whitman & Mattord (2017.) navode kako Američki Odbor za nacionalne sigurnosne sustave (CNSS) u svojoj definiciji naglašava i važnost zaštite tehnologije (hardware-a) kao komponentu informacijske sigurnosti kao i svakog sustava koji sudjeluje u „korištenju, pohrani i prijenosu informacija". Imajući na umu hardware kao materijalnu komponentu, valja promotriti sam povijesni razvoj informacijske sigurnosti koji, prema Whitmanu i Mattordu (2017.), započinje upravo kao zaštita materijalne imovine, o čemu slijedi u nastavku.

2.2. Razvoj informacijske sigurnosti

Kako navode Whitman i Mattord (2017.), prvi koraci razvoja računalne sigurnosti započinju tijekom Drugoga svjetskog rata kada se pojavljuju prva središnja računala (eng. *mainframe computers)* s ciljem razbijanja neprijateljskih poruka. Čuveni kriptografski uređaj iz tog doba jest „Enigma". U tome periodu, sve do 1960.-ih, fokus informacijske sigurnosti zapravo je bila fizička zaštita, odnosno zaštita lokacija na kojima se nalazila svojevremena informatička oprema. U periodu hladnoga rata razvijaju se sve sofisticiranija računala sposobnija za rješavanje složenijih zadataka. U duhu toga vremena razvija se i umreženi komunikacijski

sustav „ARPANET“ koji se koristio za vojne potrebe, a koji je preteča današnjeg interneta. Ipak, sustav je pokazao svoje manjkavosti po pitanju informacijske sigurnosti, što je i razumljivo s obzirom na činjenicu da su to bila vremena kada je sama informatička znanost još bila u povojima. 1970.-te godine, korporacija RAND objavila je dokument s ciljem podizanja informacijske sigurnosti, a danas se smatra dokumentom kojime je započela era izučavanja računalne sigurnosti. Vrijedi spomenuti i sustav zvan MULTICS (Multiplexed Information and Computing Service) koji je bio popularan tijekom ranih istraživanja računalne sigurnosti, a spomenuti ga treba iz razloga što je to prvi operacijski sustav koji je integrirao sigurnost u svoje temeljne funkcije. Sljedeću etapu razvoja označio je izum mikroprocesora odnosno osobnog računala (engl. *PC)* koji tada postaje glavna snaga razvoja računalne znanosti. To je sa sobom zasigurno donijelo i nove izazove po pitanju informacijske sigurnosti, na što sugeriraju i dokumenti vlade sjedinjenih država doneseni sredinom osamdesetih, kojima se računalna sigurnost prepoznaje kao „kritična stavka za federalne informacijske sustave“.

Ovdje valja spomenuti da je SAD kibernetički prostor proglasio „petom vojnom domenom, pored kopna, mora, zraka i svemira“, navodi Spremić (2017.a).

Devedesete godine donose veliku prekretnicu: pojavio se internet. Internet je omogućio povezivanje mnogih računala koji su zadovoljavali infrastrukturne uvjete. Internet postaje poveznica milijuna drugih mreža, ali u svojim počecima informacijska sigurnost nije smatrana prioritetom. U kasnim devedesetima sve više velikih poduzeća počinje ozbiljnije u obzir uzimati faktor sigurnosti, a dolazi i do široke uporabe antivirusnih programa. U tom vremenu možemo prepoznati rađanje informacijske sigurnosti kao „neovisne discipline“. Ulaskom u 21. stoljeće počinje suvremena era informacijske sigurnosti u kojima raste svjesnost o potrebi informacijske sigurnosti, kao i njene važne uloge u zaštiti kritične nacionalne infrastrukture i nacionalne obrane (Whitman & Mattord, 2017.).

U suvremeno doba, jednostavno je primijetiti kako gotovo sve poslovne organizacije funkcioniraju uz pomoć informacijskih tehnologija bez kojih bi mnogima čak i jedan radni dan bio nezamisliv. Velik je naglasak na dostupnost informacija stoga se poslovne organizacije najčešće odlučuju za informacijske sustave koji će biti aktivni u svako doba, svakoga dana, tijekom cijele godine, navode Spremić et al. (2018.).

2.3. Sigurnosne tehnologije

Razvoj informacijskih tehnologija paralelno je slijedio i razvoj informacijske sigurnosti. Tema ovog rada i sama obuhvaća koncepte koji sami po sebi pripadaju u domenu informacijske sigurnosti. Ovaj odjeljak osvrnut će se na neke od postojećih tehnologija u svijetu informacijske sigurnosti. Impresije radi, pogodno je spomenuti razinu ozbiljnosti i nesagledivi obujam incidenata u svijetu kibernetičke sigurnosti koje dočarava pogled na najveće incidente u posljednjih 10-ak godina: Brook (2019.) u svojem izvještaju navodi da je

čak 110 milijuna korisničkih podataka kupaca Target trgovine „procurilo“ iz sustava 2013. godine. Godinu dana poslije, 500 milijuna Yahoo korisničkih računa biva kompromitirano, da bi se otkrilo kako je godinu prije toga Yahoo isto bio žrtva napada pa se broj kompromitiranih podataka popeo na gotovo 3 milijarde. U nekim je slučajevima došlo čak i do curenja biometrijskih podataka (otisaka prsta) korisnika. Ovakve brojke zasigurno utjeruju strahopoštovanje prema svijetu informacijskih tehnologija i upozoravaju na važnost adekvatnih informatičkih zaštita kako bi na vrijeme prevenirali incidente koji, ne samo da ugrožavaju korisnike čiji podaci bivaju kompromitirani, već stvaraju golemu mrlju ugledu poduzeća.

Pedamkar (2021.) donosi pregled sigurnosnih tehnologija koje će biti kratko objašnjene u nastavku:

Data loss prevention (DLP) jest tehnologija sa svrhom kontrole protoka podataka kako bi se praćenjem tijeka podataka spriječilo „curenje“ povjerljivih podataka iz organizacije.

Intrusion detection system (IDS) tehnologija je kontrole podatkovnog prometa s ciljem detektiranja malicioznog prometa unutar organizacije.

Intrusion prevention sytem (IPS) tehnologija je koja reagira na sumnjivi promet kojeg je prethodno detektirao IDS sa ciljem sprječavanja njegovog ulaska u organizacijsku mrežu.

Security incident and event management (SIEM) predstavlja svojevrsni „alarm“ koji se aktivira prilikom primjećivanja sumnjivih elemenata u mreži.

Antivirusni programi tehnologija je sa ciljem zaštite od informatičkih virusa (zloćudnih kodova sa ciljem nanošenja štete domaćinu ili mreži).

Vatrozid (engl. *firewall*) tehnologija je poznatija kao prva linija obrane. Postoje različite vrste vatrozida, a cilj im je zaštititi unutarnju mrežu od sumnjivog prometa. Whitman i Mattord

(2017.) definiraju vatrozid kao „kombinaciju hardwarea i softwarea koja filtrira i štiti specifične informacije od protoka između unutarnje i vanjske mreže“.

U ovaj popis valja dodati i **kontrole pristupa** (engl. *access controls*) budući da su upravo one dio sigurnosne tehnologije koji će se detaljnije obrađivati u ovom radu. Whitman i Mattord (2017.) definiraju kontrole pristupa kao „selektivne metode uz pomoć kojih sustav specificira tko i na koji način može koristiti resurse sustava“.

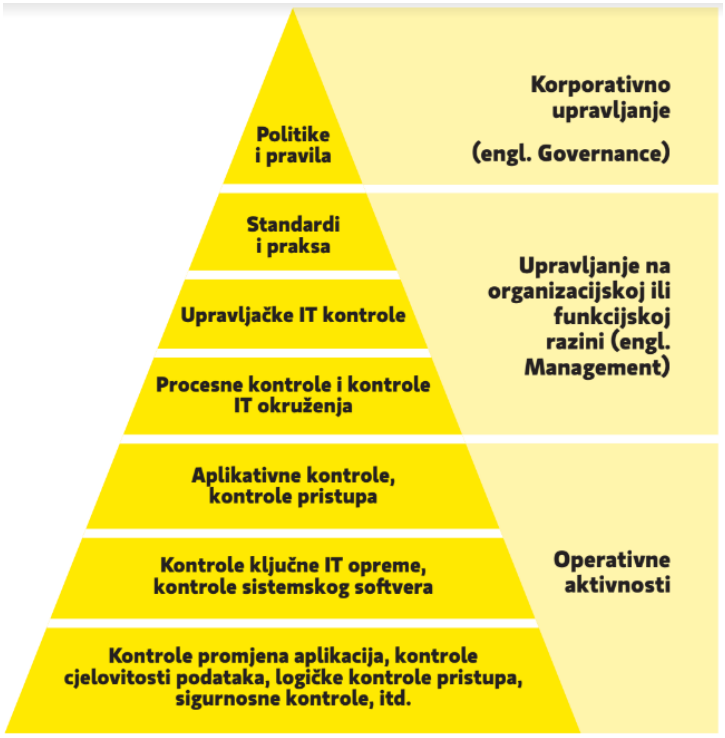
Ipak, valja istaknuti kako koncept sigurnosti ne počiva samo na kvalitetnim software i hardware rješenjima, već i na zaposlenicima poduzeća. U svojemu istraživanju Spremić i Šimunic (2018.) ističu važnost tretiranja svakog zaposlenika kao karike u lancu kibernetičke sigurnosti cijelog poduzeća. Naime, iz provedenog istraživanja o izazovima kibernetičke sigurnosti koje se provodilo kroz 9 velikih i značajnih hrvatskih poduzeća, Spremić i Šimunic zaključuju kako postoji solidna zaštita na osnovnim razinama, dok ispitanici (zaposlenici na odgovarajućim pozicijama u IT sektorima svojih poduzeća) imaju veliko pouzdanje u sustav zaštite od velikih kibernetičkih prijetnji. Ipak, Spremić i Šimunic zamjeraju činjenicu što se na kibernetičku sigurnost uglavnom gleda kao na odgovornost IT sektora u poduzeću, a ne kao na odgovornost svakog zaposlenika čime bi kolektivna svijest o kibernetičkoj sigurnosti postala integralnim dijelom organizacije i kulture poduzeća. Važnost uključivanja „lifewarea“ tj. socijalnog aspekta u razvoj kulture informacijske sigurnosti unutar poduzeća, uz aspekte tehnologije, organizacije i menadžmenta proučavali su i Arbanas et al. (2021.). Da pojedinac kao faktor sigurnosti i dalje nije prepoznat kao krucijalna stavka smatra i Georgiadou et al. (2021.). Bitna uloga pojedinca u informacijskoj sigurnosti poduzeća može se promatrati u svjetlu BYOD (engl. *bring your own device*) politike. BYOD politika odnosi se na trend u kojem zaposlenici koriste svoje osobne mobilne uređaje u svrhu obavljanja posla ili pristupa poslovnim mrežama ili sustavima (Forcepoint, b.d.). Prema nekim izvorima, u 2018. 45% britanskih poduzeća imalo je iskustva s BYOD politikama (Statista, b.d.). Ti su brojevi možda i veći kada se u obzir uzme vrijeme pandemije virusa Covid-19 i lockdowna tijekom kojega su mnogi zaposlenici radili „od doma“. Prednosti ovakve politike jesu povećano zadovoljstvo i efikasnost zaposlenika, no s druge strane BYOD politika nosi i sigurnosne rizike za poduzeće koje se odnose na curenje podataka i sigurnosnu infrastrukturu (Forcepoint, b.d.). Pitanjem informacijske sigurnosti u BYOD okruženju bavili su se i Hajdarevic et al. (2016.) nastojeći kroz primjere doprinijeti pitanju sigurnosti u BYOD okruženju. U drugom istraživanju Suša Vugec et al. (2017.) zaključuju kako ne postoji jedinstvena formula za savršeno upravljanje IT sektorom unutar poduzeća, već svako poduzeće zahtijeva određenu vrstu prilagodbe svojim

potrebama. Ipak, u zaključku daju i određene ideje za kvalitetniji razvoj i primjenu informacijske tehnologije u poslovanju.

3. Kontrole pristupa i metode autentikacije

3.1. Kontrole pristupa

„Kontrole pristupa su dozvoljene interakcije između subjekta i objekta. Baziraju se na dodjeljivanju prava ili privilegija subjektu, a koje se odnose na objekt“ (Chapple, 2020.). Spremić (2017.a) navodi obvezne kontrole pristupa, proizvoljne kontrole pristupa te kontrole pristupa temeljene na ulogama. Pored samih kontrola pristupa, u komapnijama postoji čitav niz informatičkih kontrola koje su organizirane hijerarhijski, kao što je prikazano na slici 1 (Spremić, 2017.b).



Slika 1: Vrste informatičkih kontrola obzirom na hijerarhijsku razinu njihova djelovanja

Izvor: Spremic (2017.b)

Obvezna kontrola pristupa (MAC – engl. *Mandatory Access Control*) odnosi se na kontrolu pristupa koja djeluje statički, utemeljena je na unaprijed određenim pravilima i politikama koje u konačnici determiniraju legitimnost pristupa korisnika određenim zaštićenim podacima. MAC model koristi oznake (engl. *Labels)* pomoću kojih sustav dopušta ili uskraćuje korisniku pristup objektu, ovisno o tome kakvu oznaku posjeduje pristupnik (Spremić, 2017.a). Laičkim rječnikom, svaki podatak ili skup podataka koji su zaštićeni odn. povjerljivi, imaju svoju

kategoriju povjerljivosti (npr. srednja, visoka, vrlo visoka). Isto tako, svaki korisnik koji želi pristupiti tim informacijama morat će dokazati sustavu da on uistinu ima legitimno pravo pristupa podacima, a to dokazuje putem vjerodajnica. Ovu metodu kontrole pristupa najčešće zastupaju vladine i vojne organizacije, objašnjava Shea (2013.).

„Proizvoljna kontrola pristupa (DAC – engl. *Discretionary Access Control*) počiva na načelu da se odredi vlasnik resursa (podatka, funkcije, uređaja) za kojega se traži pristup“ (Spremić, 2017.a). Ova metoda nema obvezne razine pristupa poput MAC modela, međutim mogu se implementirati po potrebi. Funkcioniranje modela svodi se na to da vlasnik resursa ima listu korisnika koji imaju dozvolu za pristup (ACL – Access Control List) te vlasnik resursa može korisnicima dodijeljivati ili uskraćivati dozvolu za pristup, navodi Spremić (2017.a).

„Kontrola pristupa temeljena na ulogama (RBAC – engl. *Role Based Access Control*) unaprijed određuje prava pristupa temeljem radnog mjesta odnosno uloge koju korisnik ima u organizaciji. Sistematizacija radnih pozicija odražava uloge koje zaposlenici imaju, propisuje njihove radne zadatke, obveze, prava i odgovornosti“ (Spremić, 2017.a). Spremić (2017.a) nadalje objašnjava kako će korisnik s ulogom prodavač moći će pristupiti samo onim podacima u sustavu koje se odnose na njegovo područje odgovornosti tj. koristit će one mogućnosti sustava koje su potrebne za odrađivanje njegovog posla. Jednako tako, njegov će nadređeni tj. voditelj prodaje imati drugačiji odn. širi set dozvola pomoću kojih će upravljati u svom području odgovornosti. Na taj način možemo razlikovati uloge prodavača, programera, računovođe, službenike u odjelu ljudskih resursa itd.

Od ostalih metoda kontrola pristupa Mike Chapple (2020.) spominje i kontrolu pristupa baziranu na atributima (ABAC – engl. *Attribute based access control*), kontrolu pristupa baziranu na pravilima (RuBAC – engl. *Rule based access control*) te kontrolu pristupa baziranu na rizicima (RAdAC – engl. *Risk adaptive access control*).

ABAC metoda odnosi se na „autentikaciju temeljenu na nekom od dodatnih atributa korisnika. Npr. kada je sustav ograničen samo na stanovnike određenog grada, prilikom prijave u sustav korisnik će morati ponuditi sustavu točnu adresu unutar tog grada“ (Chapple, 2020.).

RuBAC metoda funkcionira na princip sličan MAC metodi zbog korištenja unaprijed određenog seta pravila. Kao primjer ove metode može se uzeti mrežni vatrozid (engl. *Network firewall*) u kojem postoje određena pravila prometa kroz vatrozid (Chapple, 2020.).

RAdAC metoda karakteristična je zbog složenijega procesa određivanja rizika. Naime, metoda u obzir uzima „sigurnosni rizik pristupa“, ali i „operativnu potrebu za tom akcijom“ (Chapple, 2020.).

3.2. Proces pristupa korisnika

Proces pristupa kao skup određenih pravila i protokola može se zamisliti i izvan digitalnih okvira, na čisto fizičkom nivou. U vremenu koje je prethodilo širokoj upotrebi računala, informacije je također trebalo čuvati, što bi samo po sebi značilo i kontrolirati pristup istima. Whitman & Mattord (2017.) kao primjer navode „vojne lokacije“ u kojima se pristup kontrolirao kroz „sustav bedževa, ključeva i prepoznavanja lica autorizirane osobe od strane zaštitara“.

Na gotovo istu logiku kontrola pristupa funkcionira i danas u digitalno doba, izuzev toga da na pristupamo zaštitarima već inteligentnim računalnim sustavima koji, sukladno naredbama koje su u njih programirane, dozvoljavaju ili odbijaju pristup u sustav. Prema Whitmanu i Mattordu (2017.), „kontrole pristupa počivaju na četiri mehanizma koji ujedno predstavljaju i najvažnije funkcionalnosti sustava“. Oni navode identifikaciju, autentikaciju, autorizaciju i odgovornost (engl. *Accountability*) kao ta četiri mehanizma. Ovdje vrijedi istaknuti kako se pojam „autentikacija“ i pojam „autentifikacija“ koriste naizmjenično u literaturi na hrvatskom jeziku. Naime, službeni rječnik hrvatskog jezika ne poznaje niti jedan od navedenih pojmova. „Autentifikacija“ je vjerojatno derivirana iz njemačkog govornog područja (njem. *die Autentifizierung*), dok je „autentikacija“ ono što bi više sličilo engleskom izrazu (engl. *authentication*). Važno je zapamtiti da se one odnose na jednu te istu stvar, barem u kontekstu ovog rada. Na sličan način kontrole pristupa objašnjava i Spremić (2017.a) navodeći još i metode zaštite u prijenosu te kriptografske metode zaštite. U nastavku poglavlja obradit će se koraci u procesu pristupa korisnika, od kojih se prvi korak odnosi na identifikaciju. Prikaz cjelokupnog procesa prikazan je na slici 2.

Identifikacija je, općenito rečeno, mogućnost prepoznavanja osobe odnosno mogućnost prepoznavanja njenog identiteta (Hrvatski jezični portal, b.d.). U kontekstu procesa kontrole pristupa, identifikacija se, prema Spremiću (2017.a) definira kao „postupak prijave korisnika na informacijski sustav korištenjem fizičkih, logičkih ili biometrijskih identifikacijskih oznaka i provjere njihove vjerodostojnosti“.

U ne-digitalnom svijetu, identifikacija se odnosi na davanje tj. obznanjivanje svojeg imena. Kada se predstavljamo nekome, govorimo „Ja sam Ivan“ ili „Ja sam Jelena“ te se na taj način identificiramo. U digitalnom svijetu ta se identifikacija odnosi na pružanje svojeg korisničkog imena, e-mail adrese ili neke druge značajke informacijskom sustavu kojem želimo pristupiti, npr. pomoću biometrijskih značajki (otisak prsta, skeniranje rožnice itd.). Identifikacija predstavlja prvi korak u procesu pristupa korisnika informacijskom sustavu (Vitale, 2021.).

Autentikacija jest drugi korak procesa pristupa informacijskom sustavu. Spremić (2017.a) ovaj proces naziva procesom verifikacije (provjere) no u praktičnom smislu može se zaključiti kako su verifikacija i autentikacija u ovom slučaju istoznačnice. Spremić (2017.a) definira ovaj korak kao „postupak kojim se uneseni identifikacijski podaci uspoređuju s ranije pohranjenima i potvrđuje identitet korisnika“. Chapple (2020.) navodi kako se autentikacija nadovezuje na prethodni korak identifikacije na način da od pristupnika traži potvrdu identiteta.

Vratimo se u nedavni primjer identifikacije u ne-digitalnom svijetu gdje se korisnik predstavio kao Ivan prilikom predstavljanja. Zamislimo da se Ivan predstavljao recepcijskom službeniku u hotelu jer želi preuzeti ključeve od sobe koju je rezervirao. Recepcioner može vjerovati Ivanu da je on uistinu Ivan, međutim, s obzirom da nema nikakav dokaz, takvo bi ponašanje bilo krajnje rizično jer bi mogao sobu predati krivoj osobi. Recepcioner će stoga zatražiti Ivana njegovu osobnu iskaznicu kako bi se uvjerio da je on uistinu osoba koja se predstavlja i koja ima rezerviranu sobu. Dakle, recepcioner će započeti proces autentikacije (Vitale, 2021.).

Ova alegorija dana je radi pojednostavljenja procesa kako bi se on lakše i bolje razumio. Primjeni li se alegorija na konkretan primjer koristeći informacijski sustav, to bi značilo da će sigurnosna kontrola tražiti od nas, nakon što smo pružili svoj identitet (korisnički ID, korisničko ime, e-mail ili dr.) da isti i potvrdimo (Vitale, 2021.). Jedan od načina potvrđivanja jest kroz lozinku ili zaporku koja je vezana uz naše korisničko ime te na taj način sustav dobiva potvrdu (Spremić, 2017.a). Naravno, ovaj princip funkcioniranja ima svoje manjkavosti, o čemu će se govoriti u potpoglavlju „opasnosti i rizici“. Uz metodu korisničkog imena i lozinke, postoje i druge metode provjere identiteta odn. autentikacije, o čemu više riječi u nastavku rada.

Autorizacija predstavlja treći korak u procesu i odnosi se na dodjeljivanju prava korisniku za rad u informacijskom sustavu, a sve u granicama koje su mu unaprijed definirane unutar sustava. Time se svakom pojedinom korisniku omogućava rad unutar informacijskog sustava, sukladno ovlastima koje ima. Ovlasti rada unaprijed su organizirane i definirane. Primjer toga

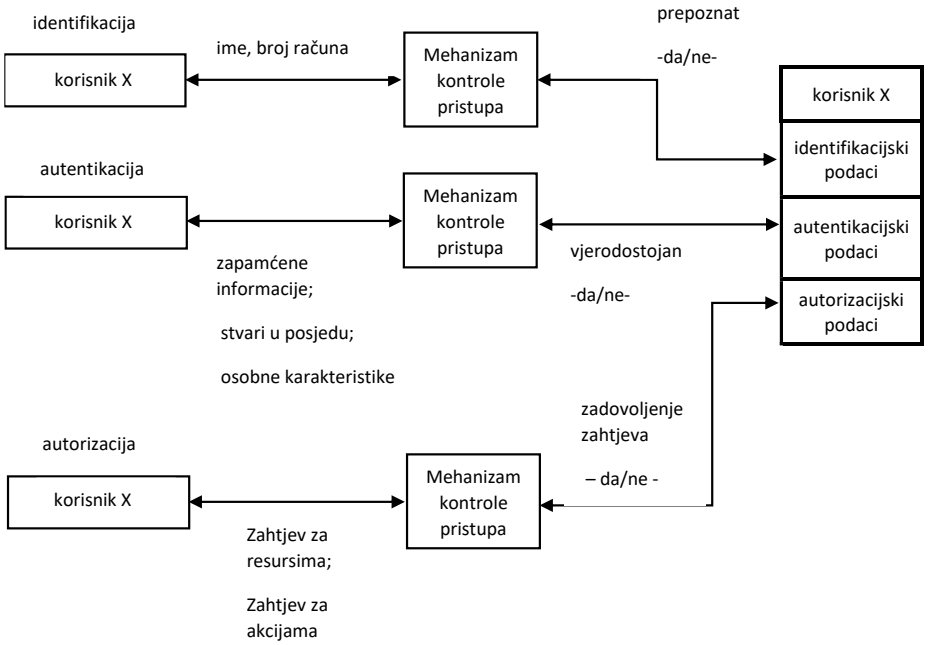
jest pristup studenta u ISVU sustav. Autorizacijom student dobiva ovlast da pregledava datume ispitnih rokova u sustavu i prijavljuje ispite, ovlast da pregledava svoje ocjene, osobne podatke i dr. Međutim, student nema ovlaštenja brisati ili ispravljati ocjene, mijenjati datume ispitnih rokova, uređivati obavijesti administratora i sl. Takve ovlasti dane su drugim korisnicima koji su za to predviđeni. Primjerice, profesori mogu unositi ocjene, administratori sustava mogu objavljivati obavijesti i sl. Pogrešno dodijeljenim pravima odnosno pogrešnom autorizacijom organizacija bi mogla upasti u velike probleme (Spremić, 2017.a).

U navedenom primjeru sa Ivanom koji dolazi u hotel, nakon uspješne autentikacije koju je obavio recepcioner i time dobio potvrdu da se uistinu radi o Ivanu koji je rezervirao sobu, korak autorizacije predstavljalo bi konačno uručivanje ključeva od sobe gostu Ivanu koji je sada slobodan smjestiti se u svoju sobu, ali ne i u one za koje nije dobio dozvolu. (Vitale, 2021.)

Odgovornost (engl. *accountability*; još i: *auditability*) predstavlja posljednji korak u procesu pristupa korisnika i odnosi se na osiguravanje praćenja svih poslova koje korisnik odrađuje u sustavu i mogućnost povezivanja određenog obavljenog posla tj. akcije sa točno određenim korisnikom koji je tu akciju izvršio (Whitman & Mattord, 2017.).

Spremić (2017.a) navodi i metode zaštite prijenosa podataka ističući prijenos podataka kao područje velike ranjivosti u informacijskom sustavu. Mehanizmi zaštite u protokolima komuniciranja doprinose efikasnosti zaštite. U istom radu Spremić navodi i kriptografske metode zaštite koje se koriste za zaštitu povjerljivih podataka poduzeća. Kriptiranje i dekriptiranje postupci su koje sačinjavaju kriptografske metode.

Slika 2 prikazuje shemu procesa kontrole pristupa koji se sastoji od identifikacije, autentifikacije i autorizacije. U koraku identifikacije korisnik pruža sustavu neki od svojih identifikacijskih podataka (ime, broj računa). Sustav tada kontrolira podatke i identificira osobu. Sljedeći korak zahtijeva od identificiranog korisnika da dokaže sustavu kako je on uistinu ta osoba kojeg je sustav prepoznao u prethodnom koraku. Korisnik to dokazuje pomoću nečega što zna, što ima ili što jest, o čemu će više riječi biti u sljedećem poglavlju. Nakon što je uspješno potvrdio svoj identitet, sustav u koraku autorizacije omogućava korisniku rad u skladu sa njegovim pravima u sustavu.



Slika 2: Identifikacija, autentifikacija, autorizacija

Izvor: Panian (2001)

3.3. Metode autentikacije korisnika

Prisjećanja radi, autentikacija predstavlja drugi korak u procesu pristupa korisnika, odmah iza identifikacije, a za cilj ima potvrditi da je osoba koja pristupa sustavu uistinu osoba kojom se predstavlja. U ovoj rečenici ogleda se i kritična važnost samog koraka autentikacije: ukoliko pristupnik bude pogrešno autenticiran, to može značiti da sada pristup u sustav ima osoba koja ga uopće ne bi smjela imati, što organizaciju ili poduzeće stavlja u vrlo veliki rizik informacijske sigurnosti, na što upućuje Spremić (2017.a). Vjerojatan je to razlog zašto se kroz razvoj tehnologije nastojalo razviti i sofisticiranije načine autentikacije, a sve kako bi njeni rezultati bili što točniji, a samim time i sigurnost podataka na što višoj razini.

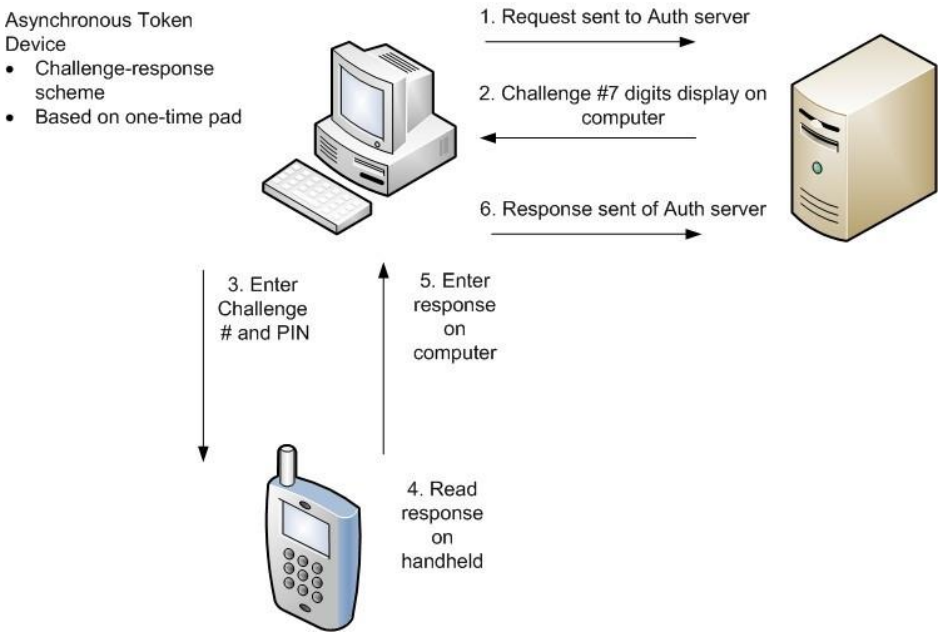
Autentikacija se, prema Whitmanu i Mattordu (2017.), zasniva na 3 metode („mehanizma“) koji se još nazivaju i faktori autentikacije. Autentikacija se može bazirati na nečemu što korisnik zna, na nečemu što korisnik posjeduje ili na nečemu što korisnik jest (Whitman & Mattord, 2017.). Spremić (2017.a) u svojoj knjizi podrazumijeva ova 3 mehanizma

objašnjavajući ih u kontekstu metoda identifikacije koje je podijelio na logičke i fizičke metode identifikacije.

Prva metoda autentikacije predstavlja ono što korisnik zna. Spremić (2017.a) ovaj mehanizam kategorizira kao logičku identifikaciju koja se „temelji na provjeri zna li korisnik nešto što bi trebao znati odnosno može saznati bez činjenja prekršaja“. Uglavnom, podatak kojega bi korisnik trebao znati jest zaporka ili lozinka, iako se rabe i nazivi poput „ključa“, „osobnog identifikacijskog broja“ itd. Sustav baziran na lozinkama još je uvijek najzastupljeniji način autentikacije korisnika. Lozinka dana sustavu se uspoređuje sa ranije pohranjenim podacima na temelju čega sustav raspoznaje korisnika (Spremić, 2017.a).

Druga metoda autentikacije odnosi se na ono što korisnik posjeduje. Spremić (2017.a) ovaj mehanizam kategorizira kao fizičku identifikaciju koja pretpostavlja da „korisnik posjeduje neki predmet“. Predmeti koji se mogu koristiti u svrhu identifikacije mogu biti kartice, tokeni i dr. U suštini, bilo koja stvar koja bi mogla potvrditi naš identitet samo zato što mi posjedujemo tu stvar – može poslužiti kao mehanizam autentikacije (Chapple, 2020.).

Tokeni, kao jedan od načina pomoću kojih se provodi autentikacija, postoje u dva tipa: sinkroni i asinkroni tokeni. Primjer sinkronog tokena jest vremenski-varijabilni token token koji se bazira se na pružanju jednokratnih lozinki, a ograničen je vremenom. Uređaj „izazova i odgovora“ (engl. *Challenge and response device*) primjer je asinkronog tokena koji koristi metodu „izazova i odgovora“ za ostvarivanje autentikacije (Chapple, 2020.). Princip rada asinkronog tokena vidljiv je na slici 3.



Slika 3: Sustav asinkronog tokena

Izvor: Assignmenthelp.net, preuzeto 13. rujna 2022. s https://www.assignmenthelp.net/identity-and-access-management-part-2

Uz tokene, valja navesti i pametne kartice. Pametne kartice u sebi sadrže čip. Dijele se na kontaktne i beskontaktne. Kontaktne se kartice prilikom autentikacije moraju očitati pomoću čitača pametnih kartica, dok se beskontaktne najčešće koriste za pristup određenim prostorima i poznate su pod nazivom „prox“ kartice (Chapple, 2020.).

Treća metoda autentikacije jest korištenje onoga što korisnik jest tj. neku njegovu karakteristiku kojom se može potvrditi njegov identitet, što se službeno naziva biometrijskim prepoznavanjem (Jain et al., 2011.). Spremić (2017.a) ovaj princip također svrstava pod fizičku identifikaciju. Prema Jain et al. (2011.), biometrijsko prepoznavanje može biti bazirano na fizičkim značajkama ili bazirano na ponašanju. U tablici na slici 4 može se vidjeti raznolikost biometrijskih identifikatora odnosno značajki ljudskog tijela pomoću kojih se može izvršavati identifikacija. Među njima su otisak prsta, izgled lica, geometrija dlana, šarenica oka, glas i dr. Nisu svi biometrijski identifikatori jednako kvalitetni. Razlikuju se po određenim parametrima koji su navedeni u zaglavlju stupaca. O njima će više riječi biti u sljedećem poglavlju. Podrobniji prikaz biometrijske tehnologije bit će dan u za to predviđenim poglavljima u nastavku.

Table 1
Comparison of Different Biometric Technologies (Jain et al., 2004) (*H* = High, *M* = Medium, *L* = Low).

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
keystroke	l	l	l	m	l	m	m
odour	h	h	h	l	l	m	l
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Slika 4: Tablica usporedbe biometrijskih tehnologija

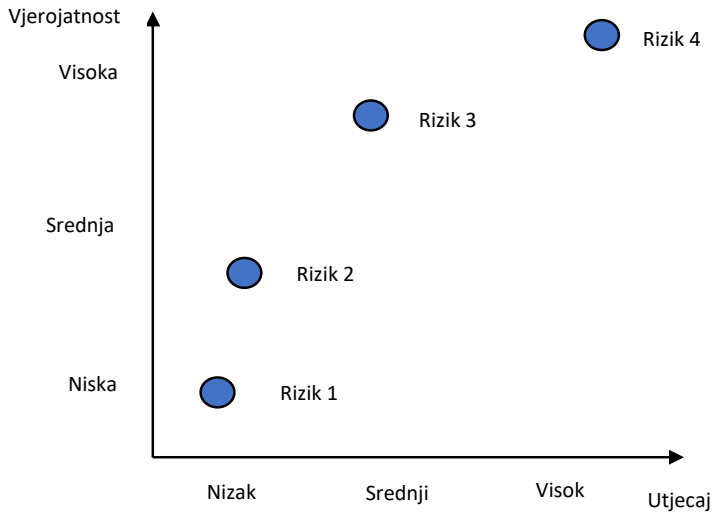
Jain et al. (2004.) , navedeno u (Khan & Efthymiou, 2021.)

Metoda multifaktorske tj. višefaktorske autentikacije metoda je prilikom kojeg se koristi kombinacija dva ili više mehanizma prilikom autentikacije, a u svrhu ostvarivanja što višeg stupnja pouzdanosti (Spremić, 2017.a). Prema Chappleu (2020.), dvofaktorska autentikacija obično je kombinacija nečega što korisnik posjeduje i nečega što korisnik zna, odnosno nečega što korisnik posjeduje i nečega što korisnik jest. Jednostavan primjer dvofaktorske autentikacije jest plaćanje karticama u trgovini (s pretpostavkom da je unos PIN-a obvezan neovisno o iznosu koji se plaća). Da bi se uspješno izvršila kupovina, potrebno je imati karticu (ono što korisnik ima) te transakciju potvrditi unosom ispravnog PIN-a (ono što korisnik zna).

Korištenje multifaktorske autentikacije kao dodatne zaštite preporučuje i Brook (2019.). OTP (engl. *one time password*) tj. jednokratna lozinka metoda je koja se može susresti prilikom korištenja internet bankarstva tj. obavljanja novčanih transakcija na internet bankarstvu. Prema Kwon et al. (2019.), OTP se smatra najjačom metodom autentikacije, iako i dalje podložna ranjivostima o kojima su istraživali Kim et al. (2020.).

3.4. Opasnosti i rizici

Već je spomenuto kako je razvoj informacijske tehnologije za sobom vukao i sve sofisticiranije načine neovlaštenog pristupa podacima koji se nalaze u nekom sustavu. Aktivnosti vezane uz informacijske tehnologije i sigurnost podataka suočavaju se sa određenim opasnostima i rizicima. Uostalom, kada to ne bi bilo pretpostavljeno, vjerojatno ne bi niti postojao termin „informacijske sigurnosti“ ili „sigurnosti podataka“. Mike Chapple (2020.) definira rizik kao pojavu koja nastaje kada „postoji potencijal da određena prijetnja iskoristi ranjivost našeg sustava ili organizacije nanoseći time štetu organizaciji, a mjeri se kroz odnos vjerojatnosti i utjecaja“. Govoreći o kontrolama pristupa unutar poduzeća, Chapple (2020.) navodi analizu troškova i koristi kao pomoćni alat koji se koristi u svrhu donošenja dobrih poslovnih odluka za poduzeće. U kontekstu zaštite informacija postavlja pitanje potrebe za zaštitom određene informacije ili informacija. Poduzeće mora odlučiti je li zaštita informacija vrijedna svih ulaganja koje zahtjeva implementacija kontrola pristupa. Kako bi se poduzeće imalo što bolju predodžbu o navedenome, Chapple savjetuje sagledavanje prednosti koje poduzeće ostvaruje ako informacija ostane u tajnosti i rizike koji se mogu izbjeći implementacijom kontrola pristupa. Naglašava kako nisu sve informacije jednake važnosti, stoga ni potreba za zaštitom nije jednaka za svaku informaciju. „Procjena rizika je krucijalni prvi korak u dizajniranju bilo kojeg sustava kontrola pristupa. U procjeni rizika, određuje se koji rizici postoje u našem okruženju ili koji se mogu pojaviti u budućnosti“ (Chapple, 2020.). Potencijal za nanošenje štete bi se zapravo mogao promatrati kroz gore navedeni odnos vjerojatnosti i utjecaja.



*Slika 5: Rizik=vjerojatnost*utjecaj*

Izvor: Chapple (2020.)

Kako objašnjava Chapple (2020.), svatko bi htio ublažiti svaku ranjivost sustava koja postoji, međutim, s obzirom da ništa nije besplatno, potrebno je napraviti analizu kojom će se procijeniti koji su rizici prioritetni kada se govori o informacijskoj sigurnosti. Na slici 5 prikazan je graf pomoću kojeg menadžment može promatrati rizike.

Prema Spremiću (2017.b), postoji prihvatljiva razina rizika, a to je ona koja ne ugrožava odvijanje važnih poslovnih procesa. Nadalje, Spremić napominje da se u današnjem informatički povezanom svijetu rizici jednog poduzeća prelijevaju i na drugo poduzeće koje mu je partner, što upućuje na potrebu za kolektivnim podizanjem svjesnosti o informacijskoj sigurnosti.

Nakon generalnog pogleda na rizike iz perspektive poduzeća i kontrola pristupa, valja se osvrnuti i na opasnosti koje vrebaju pojedine metode autentikacije.

Govoreći o metodi temeljenoj na onome što korisnik zna, ranjivost se očituje u problematici korištenja lozinki. Chapple (2020.) navodi neke od najučestalijih vrsta napada na lozinke:

Dictionary attacks (hrv. *Napad rječnikom*) podrazumijevaju napade u kojima napadač koristi poznate riječi koje se nalaze u rječniku ne bi li pogodio lozinku koju nastoji probiti

Brute-force attacks (hrv. *Napad grubom silom*) odnose se na napade pomoću softwarea koji nastoji pogoditi slova, znamenke ili simbole u lozinci

Eavesdropping (hrv. *Prisluškivanje*) jest napad prisluškivanjem na mreži

Social engineering (hrv. *Društveni inženjering*) manipulativna je vrsta napada u kojem se lažnim predstavljanjem od korisnika iziskuju njihovi povjerljivi podaci.

Duži popis napada dokumentira Spremić (2017.a) pa, između ostaloga, još navodi i:

Phishing kao „vrstu računalne prijevare sa ciljem krađe identiteta“

Man-in-the-middle kao napad u kojem napadač neovlašteno presreće komunikaciju između klijenta i poslužitelja, zaobilazeći protokole komunikacije ugrožava njenu sigurnost

Napadi uskraćivanjem usluge (engl. Denial of service – DoS) odnose se na „nedopuštene aktivnosti sprječavanja ili onemogućavanja ovlaštene uporabe računalne mreže, sustava ili programa iskorištavanjem njihovih resursa“

Backdoor napadi u kojima napadač nastoji neovlašteno ristupiti mreži te daljnjim koracima kreirati daljnje napade.

Najveći problem s kojim se susreću korisnici lozinki jest taj da odaberu lozinku koju će moći zapamtiti, ali koja neće biti prejednostavna da je haker može otkriti (Chapple, 2020.). Danas postoje različite praktične metode za kreiranje kvalitetnih lozinki, kao što postoje i password manageri. Password manageri su softwarei pomoću kojih je moguće pohraniti sve lozinke na jednom mjestu, pamteći samo jednu, „master“ lozinku (Huth et al., 2012.). Password manageri nisu zaživjeli u široj uporabi, a zašto je tomu tako istraživali su Ayyagari et al. (2019.). Slika 6 prikazuje potrebno vrijeme da software pogodi lozinku, u ovisnosti o njenoj kompleksnosti.

Case-Insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)		
Password Length	**Odds of Cracking: 1 in (Based on Number of Characters ^ Password Length):**	**Estimated Time to Crack***
8	208,827,064,576	1.01 seconds
9	5,429,503,678,976	26.2 seconds
10	141,167,095,653,376	11.4 minutes
11	3,670,344,486,987,780	4.9 hours
12	95,428,956,661,682,200	5.3 days
13	2,481,152,873,203,740,000	138.6 days
14	64,509,974,703,297,200,000	9.9 years
15	1,677,259,342,285,730,000,000	256.6 years
16	43,608,742,899,428,900,000,000	6,672.9 years
Case-Sensitive Passwords Using a Standard Alphabet Set (with Numbers and 20 Special Characters)		
Password Length	**Odds of Cracking: 1 in (Based on Number of Characters ^ Password Length):**	**Estimated Time to Crack***
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

Table 2-6 Password Power

*Estimated Time to Crack is based on a 2015-era PC with an Intel i7-6700K Quad Core CPU performing 207.23 Dhrystone GIPS (giga/billion instructions per second) at 4.0 GHz.

Slika 6: Snaga lozinki

Izvor: Whitman i mattord (2017.)

Najznačajnija slabost metode temeljene na onome što korisnik posjeduje, prema Chappleu (2020.) jest „mogućnost da uređaj koji koristimo u svrhu identifikacije može biti izgubljen ili ukraden“. Opasnosti koje prijete trećoj metodi autentikacije, tj. biometrijskoj tehnologiji, obrađivat će se u sljedećem poglavlju koje se detaljnije fokusira na biometrijsku tehnologiju.

3.5. Navike korisnika vezane uz kibernetičku sigurnost

Ovaj dio referirat će se na istraživanje novinarske kuće Guardian (Lord, 2020.) u kojem su ispitivali 1000 korisnika o njihovim sigurnosnim navikama prilikom korištenja interneta. Istraživanje je svojevrsno ispitivanje društvene „kibernetičke higijene“ (engl. *Cyber hygiene*), zanimljivog pojma kojeg guardian definira kao praktične korake kojeg korisnici čine s ciljem očuvanja sigurnosti na internetu (Brook, 2020).

Prema procjenama navedenim u istraživanju (Vance, 2010., navedeno u Ayyagari et al., 2019.), od 32 milijuna lozinki njih 5000 moglo se povezati sa čak 20% korisničkih računa.

Istraživanje (Lord, 2020.) je fokusirano na navike korisnika koje se tiču primjene lozinki na internetu. Istraživanje pokazuje da čak 70% ispitanika ima više od 10 korisničkih računa koji su zaštićeni lozinkama, od kojih čak 30% nije sigurno u točan broj svojih računa jer ih ima „previše“. Sekundarno istraživanje navedeno u ovom članku ističe da je prosječna e-mail adresa u SAD-u povezana sa 130 korisničkih računa (to mogu biti društvene mreže, internetske trgovine itd.). 11% ispitanika koristi jednu te istu lozinku za sve korisničke račune, a 49% korisnika koristi iste lozinke za račune koji ne sadrže osjetljive podatke. 40% ispitanika nikada ne koristi istu lozinku za više računa. 39% ispitanih pamti lozinku tako da je zapišu na papir, dok ih 28% koristi „password managere“. Na pitanje o učestalosti mijenjanja lozinke, 70% korisnika mijenja svoje lozinke najmanje jednom godišnje, a 40% barem 3 puta godišnje. 56% korisnika kreira fraze ili kompleksne lozinke koje sadrže velika i mala slova, brojeve i posebne znakove. Generacijski gledano, najkompleksnije lozinke imaju oni u dobi od 18 do 34 godine (63.5% koristi vrlo kompleksne lozinke), dok starije generacije imaju manji udio vrlo kompleksnih lozinki (manje od 50%). Prilikom kreiranja lozinke, za gotovo dvije trećine ispitanika važnija je razina sigurnosti nego jednostavnost pamćenja lozinke. Za kraj valja još spomenuti kako minimalno 48% korisnika koristi metodu dvofaktorske autentikacije tamo gdje je ona moguća.

4. Biometrijska tehnologija

4.1. Koncept i razvoj biometrijske tehnologije

Suština pisanja ovog rada, kao što to i sam naslov sugerira, krije se u pojmu biometrijske tehnologije. No, kako bi čitatelj bio što bolje upućen u kontekst u kojemu se, kroz teoriju i praksu, susrećemo sa biometrijskom tehnologijom, do sada su obrađena šira područja iz domene informacijske sigurnosti i kontrola pristupa kao neizostavnih sastavnica nužnih za razumijevanje biometrijske tehnologije. Preostaje proučiti onaj treći princip autentikacije kojeg se još pamti po spomenutoj krilatici „ono što korisnik jest".

Biometrijska tehnologija (engl. *Biometrics*) bazira se na korištenju jedinstvenih ljudskih fizičkih ili bihevioralnih karakteristika u svrhu identifikacije ili autentikacije te ubrzano zamjenjuje tradicionalne metode u svijetu (Jain et al., 2007. navedeno u Yang et al., 2019.).

Važno je primijetiti kako se metode autentikacije temeljene na onome što korisnik zna ili posjeduje očigledno oslanjaju na pretpostavku da će korisnik „surađivati" sa sustavom te ispoštovati zahtjeve koje sustav podrazumijeva, a taj je zahtjev zapravo pretpostavka da jedino taj ovlašteni korisnik posjeduje tu određenu stvar ili da jedino on zna određenu lozinku za pristup. S druge strane, biometrijske značajke neprenosive su i usko vezane uz točno određenog pojedinca te se na taj način sustav mnogo teže može prevariti (National Research Council et al., 2010.).

Prema Caballero (2022.), biometrijski se podaci moraju promatrati kroz nekoliko kriterija kako bi se smatrali jedinstvenima:

1. Univerzalnost - podatak mora biti neka značajka koju ima svaki pojedinac u populaciji, osim u vrlo rijetkim iznimkama

2. Unikatnost – uzorak mora biti jednoznačan za svakog pojedinca

3. Stabilnost – fizička materija iz koje se derivira podatak mora biti stabilna tijekom dugog perioda, ne sklona promjenama koje mogu utjecati na izgled uzorka

4. Dostupnost – odnosi se na jednostavnost preuzimanja biometrijskog uzorka

5. Korisnost – uzorak mora biti takav da programi i oprema na njemu lako mogu pronaći diferencijacijske elemente

6. Prihvatljivost – populacija mora biti voljna prihvatiti biometrijski sustav

7. Falsificiranost – odnosi se na mogućnost da biometrijski podatak bude falsificiran

Etimologija riječi „biometrija“ pokazuje nam da je riječ nastala spajanjem dva pojma iz grčkog jezika: „bio“ što znači „život“ i „metrija“ što bi značilo „mjeriti“. Prvi tragovi korištenja biometrije datiraju još iz doba drevnih civilizacija poput babilonske, kineske i egipatske. Naravno, u tim se vremenima nije koristila suvremena tehnologija kakvu mi danas imamo, ali se korištenje biometrije očitovalo kroz praksu uzimanja otisaka prsta i dlanova u poslovanju i trgovini. Navedimo za primjer da su popisi babilonskih poslovnih transakcija na glinenim pločicama sadržavale i otiske prsta (Mayhew, 2018.).

No pravi razvoj biometrije započinje u devetnaestom stoljeću kada Parižanin Alphonse Bertillon započinje koristiti biometrijske karakteristike kako bi obrađivao i klasificirao kriminalce. Već potkraj devetnaestog stoljeća otisci se prsta koriste u kriminalističke, ali i poslovne svrhe. Edward Henry razvio standard za otiske prstiju nazvan „Henrijev klasifikacijski sustav“. Zakon je postupno ukinuo dotadašnji Bertillonov sustav prihvativši Henrijev koji postaje standardom za identificiranje kriminalaca (Recfaces, b.d.).

Dvadeseto stoljeće vrlo je plodonosno razdoblje za razvoj biometrijskog raspoznavanja. Ranih godina dvadesetog stoljeća u Americi se osnivaju prvi uredi za otiske prstiju u sklopu policijskih postaja i kaznionica. 1936. godine oftalmolog Frank Burch otkriva mogućnost identifikacije korištenjem uzorka očne šarenice, a 1960. švedski profesor Gunnar Fant započeo je prve korake metode prepoznavanja govora. Krajem šezdesetih, na inicijativu FBI-a započinje se razvoj automatiziranog sustava za raspoznavanje otisaka prstiju, s obzirom da je ručno uspoređivanje otisaka bilo neefikasno. Sedamdesetih godina dolazi do pomaka u razvoju metoda prepoznavanja govora i do prvog prototipa sustava za prepoznavanje govora. Razvija se tehnologija prepoznavanja lica, a dolazi i do prvog komercijalnog sustava za identifikaciju pomoću geometrije dlana. Osamdesetih je godina patentirana identifikacija putem geometrije dlana i putem vaskularnog uzorka. Osnovan je i NIST Speech Group sa ciljem razvijanja tehnologije prepoznavanja govora. Devedesetih godina osniva se konzorcij za biometriju sa ciljem razvoja biometrijskih tehnologija, a patentira se i metoda prepoznavanja očne šarenice. 1994. godine nastaje IAFIS- Integrirani automatizirani sustav za identifikaciju otiska prstiju čiji je cilj omogućiti prikupljanje i obradu otisaka prstiju. Na olimpijskim igrama u Atlanti 1996. godine pristup olimpijskom selu kontrolirao se pomoću biometrijske tehnologije

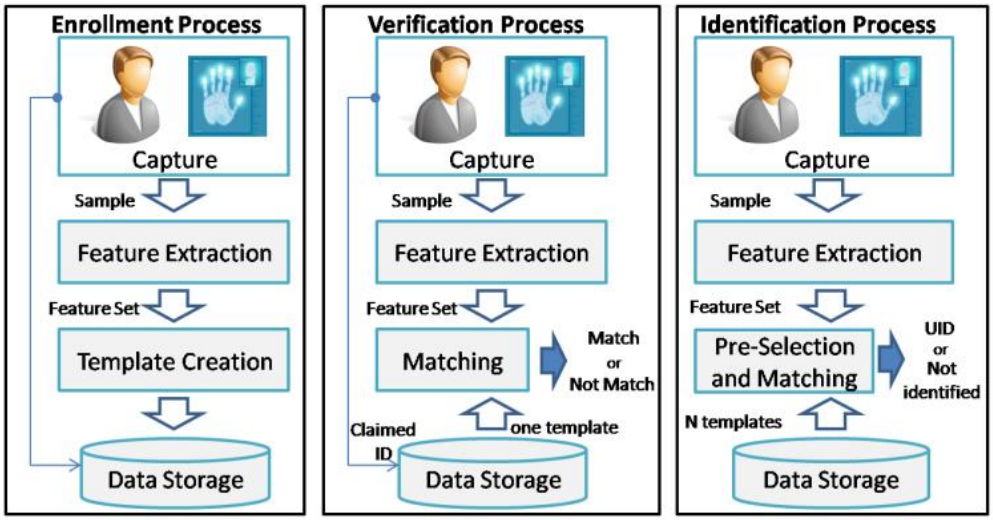
geometrije dlana. Više desetaka tisuća ljudi bilo je registrirano, što u znači da je sustav za vrijeme igara procesuirao korisnike sveukupno više od milijun puta. Godinu dana kasnije izlazi i prvi standard za biometrijsku tehnologiju koji postaje osnova onima koji će nadolaziti. Posljednje godine dvadesetog stoljeća razvijen je FBI-jev IAFIS sustav. Razvoj standarda sustava bio je potreban kako bi se omogućilo uspoređivanje otisaka prstiju iz različitih sustava u kojima su pohranjeni. 21. stoljeće donosi brže i bolje sustave i sve veću prihvaćenost tehnologije prepoznavanja lica, koja se 2001. koristila čak i tijekom SuperBowl-a. Također, implementacija biometrijske tehnologije u mobilne telefone počinje biti sve raširenija. Biometrijska tehnologija počinje se izučavati čak i kao studijski program, a aktivno se radi i na danjem razvoju standarda vezanih za korištenje biometrije. 2004. godine odjel obrane implementirao je ABIS – automatizirani biometrijski identifikacijski sustav sa ciljem nadzora nad ljudima koji su okarakterizirani kao opasni za državnu sigurnost. Sustav je pohranjivao biometrijske podatke ljudi koje su smatrali sumnjivima, a iste godine 3 su američke savezne države otvorile bazu podataka za otiske dlanova za potrebe policije. 2008. godine Google implementira mogućnost pretraživanja pomoću glasa, dok FBI proširuje svoju biometrijsku bazu podataka dodavajući i druge značajke, osim otiska prsta. 2018.-u godinu obilježava veća komercijalna uporaba biometrijskih tehnologija kao što je npr. MasterCard biometrijska kartica kao i Bytonov električni automobil sa integriranim biometrijskim tehnologijama. U suvremeno doba, biometrijska tehnologija postaje sve razvijenija. U sljedećim godinama očekuje napredak tehnologija prepoznavanja hoda i tehnologija srčanog ritma, a neki smatraju da bi do 2030. društvo moglo u potpunosti prestati koristiti lozinke (Recfaces b.d.).

4.2.Otisak prsta

Prema Yang et al. (2019.) otisak prsta je najpoznatija i najšire primijenjena metoda identifikacije u svijetu.

Ljudska se koža razlikuje na različitim dijelovima našega tijela. Upravo na jagodicama prstiju nalaze se karakteristične brazde na koži koje, uz svoje primarne biološke funkcionalnosti, mogu poslužiti i kao sredstvo za raspoznavanje pojedinaca. Smatra se da su uzorci brazda sa jagodica prstiju jednoznačni za svakog pojedinca i nepromjenjivi, ukoliko se ne radi o težim ozljedama koje će u konačnici rezultirati ožiljcima. Radi li se o lakšim ozljedama, koža sa jagodica prstiju ima tendenciju zacijeljivanja uz obnavljanje uzorka brazdi na jagodici. Policija i njoj bliske institucije već naširoko koriste praksu identifikacije pojedinaca putem otisaka prstiju, a razvoj tehnologije omogućio je i stvaranje AFIS-a, automatiziranog sustava za

identifikaciju otisaka prstiju. Otisak prsta i mogućnosti koje on donosi već su naširoko poznate po cijelom svijetu (Jain et al., 2011.).



Slika 7: Proces pristupa, verifikacije i identifikacije

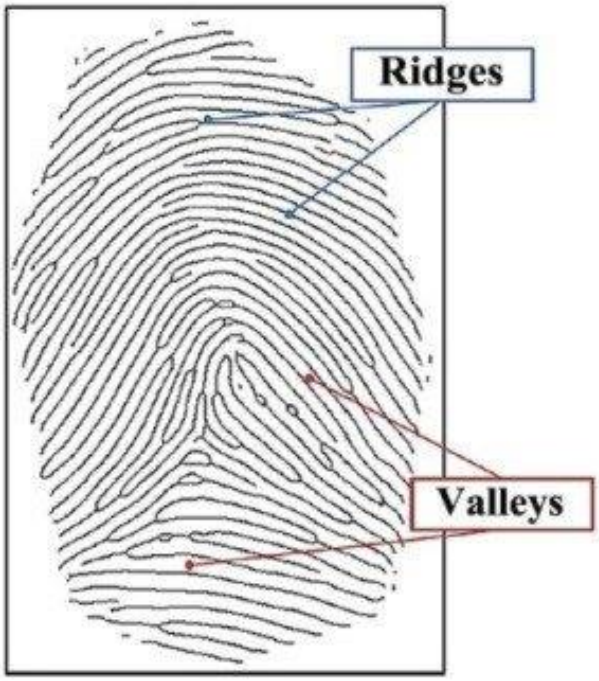
Izvor: Turroni (2012.)

Biometrijski sustav može operirati kao identifikacijski i verifikacijski (autentikacijski) sustav. Identifikacijski sustav jest onaj koji uzorak pristupnika uspoređuje sa svim pohranjenim uzorcima u bazi podataka tražeći onaj koji se podudara sa pristupnikovim, dok verifikacijski sustav uspoređuje pristupnikov uzorak sa samo jednim uzorkom u bazi podataka, a to je onaj s kojim se pristupnik prvi puta registrirao. Kao što je vidljivo na slici 7, verifikacijski proces se odnosi samo na jedan uzorak, dok identifikacijski proces obrađuje *n* broj uzoraka (Turroni, 2012.).

Za praksu uzimanja i uspoređivanja otisaka prstiju postoje dvije metode: metoda bazirana na uzorku i metoda bazirana na slici. Metoda bazirana na uzorku funkcionira na način da prepoznaje te izvlači karakteristične detalje iz slike otiska prstiju oji kasnije služe za usporedbu, dok se metoda bazirana na slici, kako joj i samo ime sugerira, bazira na uspoređivanju slike otiska prstiju koje ne uključuje izvlačenje detalja iz otiska prsta. Također, postoje i tri razine uzorkovanja otiska prsta, od kojih je prvi onaj najgrublji dok treći uzima u obzir najviše detalja (Jain et al., 2011.).

Prema Jain et al. (2011.) prva razina uzimanja uzorka obuhvaća najmanje detaljno analiziranje uzorka, a pritom se otisak prsta prikazuje kao „orijentacijska mapa brazdi“ (engl. *ridge orientation map*). Orijentacijska mapa brazdi „bilježi lokalnu orijentaciju brazde na svakom dijelu otiska“. Također bilježi i mapu frekventnosti brazdi koja bilježi „lokalnu frekventnost

brazdi na svakoj lokaciji u otisku“. Brazde i „doline“ između tih brazdi vidljivi su na slici 8 gdje su plavim linijama označene brazde, a crvenim udubljenja između njih. Pomoću orijentacije i frekventnosti brazdi na otisku mogu se odrediti oblik i struktura tiska. Na različitim razinama uzorkovanja fokus je na različitim detaljima. Na prvoj razini promatraju se samo „tok brazdi i frekventnost brazdi, dok su detalji o dimenzijama i lokaciji brazdi izostavljene“. Orijentacijska mapa brazdi sadrži i lokacije gdje se smjerovi tj. orijentacije brazdi „naglo mijenjaju“, a takve se lokacije nazivaju točkama jedinstvenosti ili singularnim točkama (engl. *singular points*). Dvije su vrste singularnih točaka tj. točaka jedinstvenosti, engleskih naziva „loop“i „delta“, a razlika u njihovom izgledu je naočigled prepoznatiljiva, kao što prikazuje slika 9. „Loop“ (zvana još i „core) je točka koju karakteriziraju brazde prepoznatljive po svojem usmjerenju, kao što je vidljivo na slikama 9 i 10. Loop točke su one u kojima „brazda ima ulaznu putanju iz jednog smjera, a potom izlaznu putanju prema tom istom smjeru.“ „Delta“ vrsta singularne točke karakteriziraju 3 niza brazdi koji se naočigled stapaju jedan sa drugim. Vizualno, delta ostavlja dojam trokuta, kao što je vidljivo na slici 9. Na temelju broja loop i delta singularnih točaka i njihovih pozicija na otisku, otisak se može grupirati po klasama. Postoji 6 glavnih klasa otisaka. Valja spomenuti i da se loopovi i delte na otisku prsta pojavljuju u parovima, a njihov je broj jednak 0,2 ili 4 (Jain et al., 2011.). Vrste i izgled klasa otisaka vidljiv je na slici 11.



Slika 8: Brazde i udubljenja na otisku prsta

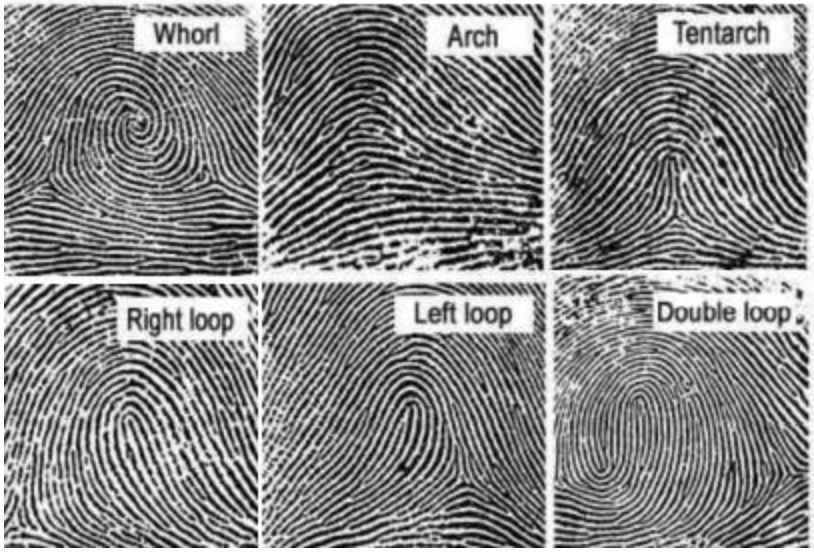
Izvor: (Shawkat et al., 2018)

Slika 9: Otisak prsta sa loop i delta regijama

Izvor: (Bahgat et al., 2013.)

Slika 10: Detalji na otisku prsta

Izvor: Ogbuokiri i Agu (2015.)

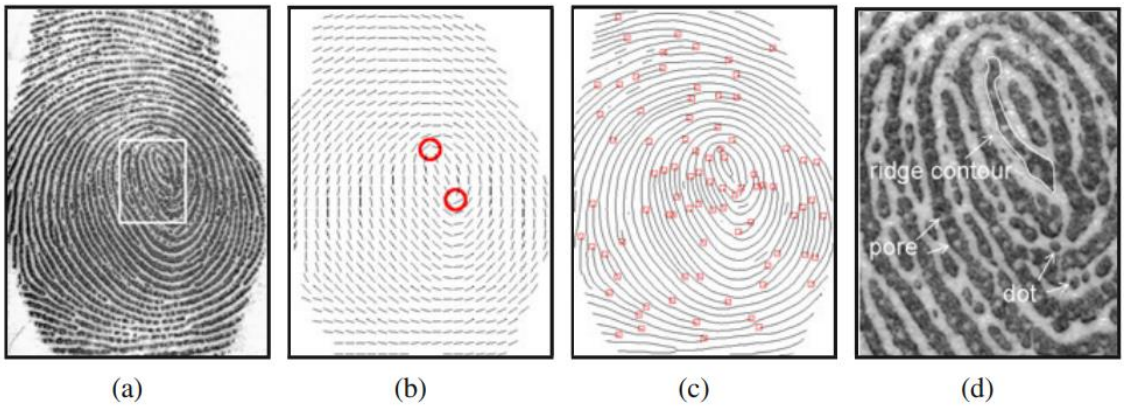


Slika 11: glavne vrste otiska prsta

Izvor: (Topaloglu, 2013.)

Drugu ili srednju razinu karakterizira prikaz otiska kao „kostura brazdi otiska prsta u kojem je svaka brazda široka samo 1 piksel“ (Jain et al. 2011.). Na ovoj razini „bilježi se točna lokacija brazdi, ali se izostavljaju geometrijski i dimenzionalni detalji brazdi“. „Lokacije na kojima se brazde pojavljuju, završavaju, dijele se ili spajaju nazivaju se detaljima“ (Jain et al., 2011.).

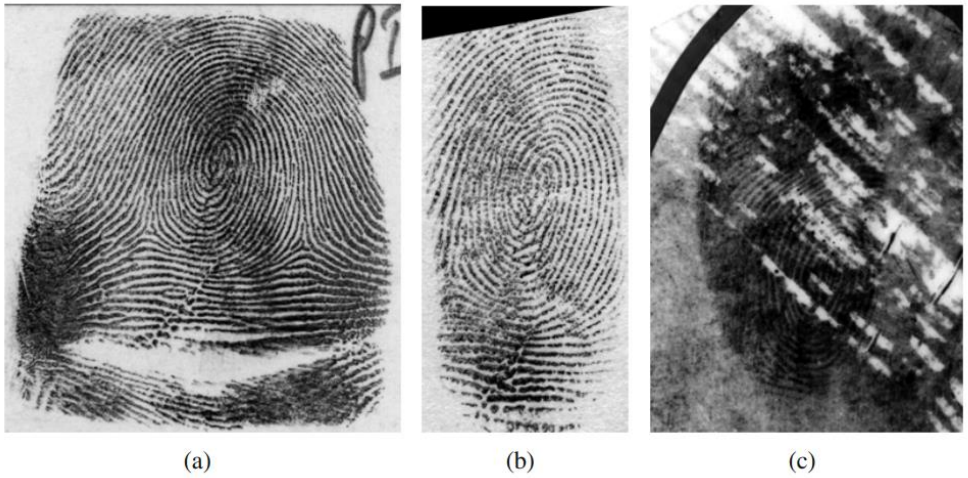
Dvije su osnovne vrste detalja: terminacija i bifurkacija, odnosno „završavanje“ i „račvanje“. Budući da slika govori tisuću riječi, za razumijevanje osnovnih tipova detalja promotriti sliku 10. Lokacija na slici otiska, smjer i vrsta parametri su po kojima se mogu opisivati detalji. Broj detektiranih detalja na slici podložan je osciliranju. Npr., na slici 13 nalaze se tri otiska prsta koji su uzeti sa tri različite metode. Prvi otisak uzet je metodom „rolanja“ (umakanjem prsta u tintu i ostavljanjem otiska na papiru na način da se prst rotira po papiru), drugi otisak je preuzet metodom pritiska prsta na papir (također pomoću tinte) dok je treća metoda tzv. „latentni“ otisak koji se ne preuzima direktno sa prsta, već sa površine na kojoj se prst ostavio tragove, kao što je to slučaj kad forenzičari traže otiske na mjestu zločina. Koristeći komercijalni komparator otisaka, na prvom otisku bilo je registrirano 136 detalja dok se na drugom otisku pronašlo samo njih 56. Treći otisak obrađen putem posebnog ispitivača za latentne otiske otkrio je svega 18 detalja, što potvrđuje činjenicu da su latentni otisci najmanje kvalitete. Detalji koji se izdvajaju na drugoj razini sadrže mnogo podataka po kojima se otisci mogu razlikovati prilikom identifikacije, efikasni su za pohranjivanje, a njihovo izvlačenje je otporno na različite izvore oštećenja, stoga se naširoko koriste u automatiziranim sustavima za prepoznavanje otisaka prstiju (Jain et al., 2011.).



Slika 12: Značajke na različitim razinama detalja

Izvor: Jain et al. (2011.)

Na slici 12 prikazani su detalji otiska prsta na sve 3 razine detalja. Detalji prve razine prikazani su pod slovom (b), druga razina pod slovom (c) i treća razina pod slovom (d).



Slika 13: Različite vrste otiska istog prsta

Izvor: Jain et al. (2011.)

Treća razina izdvaja „unutarnje rupe tj. pore za izlučivanje znoja i vanjske konture brazdi“. Na ovoj razini značajke brazdi se promatraju u detalje uključujući „početne brazde“ i „točke“. Početne su brazde tanje od običnih i bez pora za izlučivanje znoja, a točke u ovom slučaju predstavljaju brazde vrlo kratke duljine. Značajke treće razine u središtu su pozornosti u kontekstu uspoređivanja latentnih otisaka, s obzirom da su oni najmanje kvalitete, odnosno sadrže najmanje detalja (Jain et al., 2011.).

Uzimanje uzorka otiska prsta može se obavljati off-line ili on-line metodama. Off-line metode su metode kojima se sken prsta ne uzima direktno informatičkim putem već se koristi posredno sredstvo (npr. papir) preko kojeg se slika onda učitava u računalo. On-line metode su one koje koriste senzore i tehnologiju pomoću koje se otisak prsta direktno preslikava u sustav (Jain et al., 2011.).

Nakon što računalni sustav uzme uzorak i odredi detalje otiska, pomoću algoritma pohraniti će informacije o otisku u jedinstveni numerički kod. Svaka daljnja usporedba otiska prsta u svrhu autentikacije zapravo će biti uspoređivanje kodova koje imaju pristupnici ili korisnici nekog sustava sa numeričkim kodovima koji su pohranjeni u sustavu. Na temelju toga podudaraju li se kodovi sustav će donijeti odluku o dozvoli za pristup ili o odbijanju pristupa (Woodford, 2022.).

4.3. Prepoznavanje očne šarenice

Očna šarenica, kako joj i sam naziv sugerira, dio je oka koji je „šaren“ odnosno, karakterizira ga određena boja. U šarenici se nalaze mišići koji svojom aktivnošću utječu na zjenicu i kontroliraju količine svjetla koja ulazi u oko (Cleveland clinic b.d.).

Izučavanje strukture očne šarenice kao metode za identifikaciju započelo je jo 1936., a ideja je patentirana 57 godina kasnije. 1992. pojavljuje se prvi automatizirani sustav za prepoznavanje očne šarenice. Dr. John Daugman, jedan od dvojice koji je radio na razvoju sustava, izradio je algoritme za prepoznavanje šarenice koji su doživjeli uspjeh u komercijalnoj upotrebi, a njegov angažman postao izuzteno cijenjen (Abidin, 2021.).

Abidin (2021.) navodi nekoliko temeljnih sastavnica sustava za prepoznavanje očne šarenice koje se baziraju upravo na Daugmanovom pristupu: preuzimanje slike, segmentacija, ekstrakcija i komparacija. Preuzimanje slike tj. akvizicija predstavlja prvi korak u kojem se „pomoću kamere ili bliskom infracrvenog senzora od pristupnika uzima sken tj. slika njegovog oka“. Jain et al. (2011.) navodi da se blisko infracrveno svjetlo koristi kako bi se osvijetlila šarenica, a sustav zatim uslikava nekoliko slika šarenice od kojih uzima one najkvalitetnije za danju obradu.

U procesu segmentacije se, prema Jain et al. (2021.) šarenica izdvaja od ostalih elemenata oka koje mogu biti obuhvaćene skeniranjem te se svi drugi elementi isključuju. U procesu segmentacije određuju se i granice same šarenice koje su unutarnje i vanjske. Također, ističe se krucijalnost ovog koraka u procesu jer nekvalitetnom segmentacijom posljedično se ozbiljno

narušava performansa sustava prilikom usporedbe uzoraka. Normalizacija predstavlja proces u kojemu se dobivena slika očne šarenice pretvara u sliku pravokutnog oblika koristeći numeričke matematičke parametre, a taj se proces još neslužbeno naziva i „odmotavanje šarenice“.

Važne značajke dobivene procesom normalizacije kodiraju se kroz proces ekstrakcije čime se dobiva kod šarenice (engl. *irisCode*) u binarnoj formi. Posljednji korak jest korak komparacije u kojem se dobiveni kod uspoređuje sa ranije pohranjenim kodovima kako bi se donijela odluka o tome je li korisnik autentičan ili nije, navodi Abidin (2021.).

Prema Ye et al. (2020.), prednosti metode prepoznavanja očne šarenice su beskontaktnost tj. korisnik ne treba ostvariti izravan fizički kontakt sa opremom za vrijeme procesa preuzimanja, što zasigurno zvuči kao zanimljiva karakteristika u današnjem pandemijskom ili post-pandemijskom svijetu. Ističe se i i jedinstvenost tj. unikatnost očne šarenice te njezina stabilnost tijekom životnog vijeka čovjeka. S druge strane, nedostaci se očituju u skupocjenoj opremi, velikim hardverskim zahtjevima te poteškoćama pri procesuiranju očiju crne boje, a također za dobre performanse sustava potrebno je osigurati odgovarajuće količine svjetlosti.

4.4. Prepoznavanje lica

Prepoznavanje lica još je jedna od metoda biometrijske identifikacije koja se bazira, kako joj i samo ime govori, na karakteristikama ljudskog lica. Prednosti metode prepoznavanja lica, prema Jain et al. (2011.), očituju se u mogućnosti skeniranja ljudskog lica beskontaktnim putem odnosno sa određene udaljenosti. Također, „lice ne odražava samo identitet, već i emocionalno stanje pojedinca (npr. sreća ili ljutnja) kao i određene biografske karakteristike (npr. spol, dob, rasa itd...) (Jain et al.,2011.).

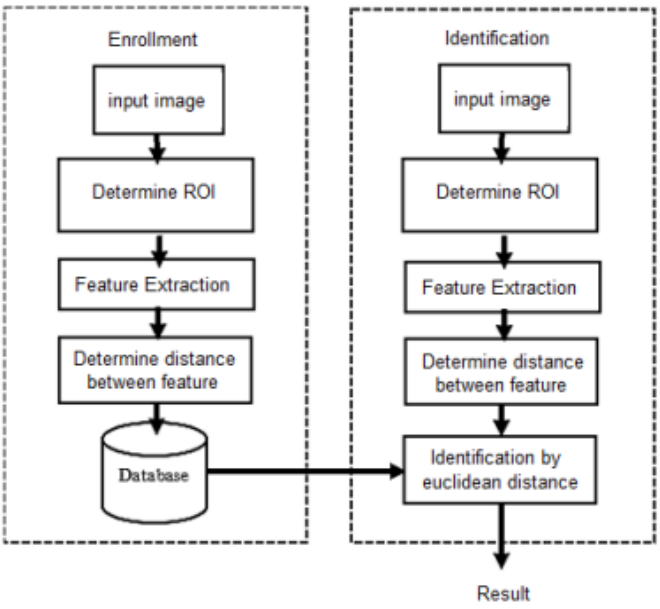
Jain et al. (2011.) nadalje ističu kako je se u javnosti naslućuje pozitivan stav prema korištenju lica kao metode za identifikaciju jer se ljudi osjećaju slobodno dijeliti svoje slike u javnom prostoru što dokazuju činjenicom da društvo generalno voli koristiti društvene mreže i ne zaziru od povezivanja svoje fotografije sa svojim identitetom.

Metoda prepoznavanja lica segmentira ljudsko lice na tri razine specifičnosti pomoću kojih otkriva njegove detalje potrebne za identifikaciju. Detalji na prvoj razini su oni koji se uočavaju vrlo lako kao npr. oblik lica i boja kože. Na ovoj razini moguće je odrediti oblik lica i npr. spol osobe sukladno specifičnostima koje na licu budu detektirane. Fokus druge razine promatranja su elementi na ljudskom licu (oči, nos, usta) te njihov međusobni odnos. Na ovoj razini oblik

lica podliježe dubljoj analizi. Treća razina jest „najfinija“ razina gdje se uočavaju oni najmanji detalji na licu kao što su madeži, ožiljci i slično (Jain et al., 2011.).

Proces preuzimanja uzorka sastoji se od nekoliko koraka: preuzimanje slike, detektiranje lica i ekstrakcije detalja lica. Tri su pristupa komparaciji uzoraka: pristup baziran na izgledu, pristup baziran na modelu i pristup baziran na teksturi (Jain et al., 2011.). Prema Ye et al. (2020.), složenost tehnologije prepoznavanja lica zahtijeva kooperaciju sa drugim digitalnim tehnologijama. Prema istom izvoru, prednosti tehnologije prepoznavanja lica su jednostavnost korištenja, njezina beskontaktna primjena te mogućnost identificiranja više osoba od jednom. S druge strane, jedan od nedostataka očituje se u mogućnosti da se sustav prevari kroz izmijenjene karakteristike ljudskog lica ostvarene kroz šminku i sl. Nadalje, nedostaci su velika osjetljivost na položaj lica tijekom skeniranja, kao i na količine svjetlosti koje mogu utjecati na rezultate. U konačnici, cijena potrebna za kvalitetan sustav uvrštava se također pod negativnu stranu.

Kroz sljedeći konkretan primjer iz znanstvene studije promotrit će se postupak identifikacije putem prepoznavanja lica. Na slici 14 prikazan je hodogram procesa koji obuhvaća fazu u kojoj pristupnik po prvi puta pristupa identifikaciji nakon čega se njegov uzorak sprema u bazu podataka (lijeva strana) i fazu redovite identifikacije prilikom koje se preuzeti uzorak pristupnika uspoređuje sa ranije spremljenim uzorkom u bazi podataka.



Slika 14: Dijagram procesa identifikacije

Izvor: Widodo & Adi (2019.)

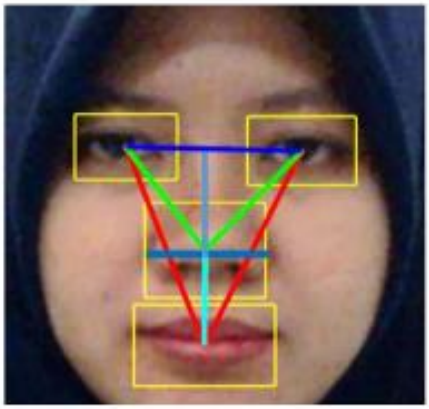
Nakon što je slika lica preuzeta, slijedi korak segmentacije, što bi odgovaralo koraku detektiranja lica kojeg navodi Jain et al. (2021.). U tom koraku određuje se „područje interesa“ (ROI; engl. *region of interest*) pomoću Viola-Jones algoritma. Nakon uspješno određenih detalja na licu određuje se središnja točka svakog detalja koje se zatim linijama povezuju te sa računa njihova međusobna udaljenost. Matematičkim operacijama i komparacijama udaljenosti detalja dobiva se konačan rezultat potreban za komparaciju uzoraka (Widodo & Adi, 2019.).

Slika 15: Primjer rezultata preuzimanja slike

Izvor: Widodo & Adi (2019.)

Slika 16: Određivanje ROI (lijevo), slika nakon izrezivanja (desno)

Izvor: Widodo & Adi (2019.)



Slika 17: Primjer 8 linija između značajki

Izvor: Widodo & Adi (2019.)

4.5. Ostale biometrijske metode

U prethodnim poglavljima obrađene su tri metode biometrijske identifikacije koje su prema opsegu korištenja možda i najzastupljenije. Biometrijskih metoda ima mnogo te opseg ovog rada ne dozvoljava detaljnu obradu svake pojedine metode. U ovom odjeljku ukratko će se objasniti biometrijske metode koje su bile navedene u sklopu istraživanja o stavovima i percepciji biometrijske tehnologije u društvu, koje je sastavni dio ovog rada.

Prepoznavanje glasa biometrijska je metoda koja se u suštini ne odnosi na ono što korisnik jest, već na ono što on producira pa je po tome slična metodi dinamike tipkanja ili biometrijskog potpisa. Prepoznavanje glasa metoda je kojom se uz pomoć računalnih programa ljudski glas konvertira u digitalni zapis podataka. Važno je istaknuti kako se prepoznavanje glasa (engl. *Voice recognition*) i prepoznavanje govora (engl. *speech recognition*) ne odnose na istu stvar. Naime, prepoznavanje glasa biometrijska je metoda identifikacije, dok je prepoznavanje govora tehnologija kojom software prepoznaje naredbu izrečenu govorom umjesto npr. upisivanjem pojma u internet tražilicu te se ponekad koristi i naziv „glasovna naredba“ (engl. *Voice command*). Ipak, metoda prepoznavanja glasa pred sobom ima mnoge izazove. Prepoznavanje glasa još ne ostvaruje precizne rezultate kao što je to slučaj sa nekim drugim biometrijskim metodama. Također, preuzimanje uzorka glasa vrlo je problematično ako se osoba nalazi u okruženju sa mnogo buke. Na kraju, ljudski glas se može promijeniti ovisno o zdravstvenom stanju osobe, što stavlja još jedan upitnik nad samu metodu prepoznavanja glasa (Nec, b.d.).

Prepoznavanje geometrije ruke metoda je koja se koristi od ranih sedamdesetih godina 20.st. Koristi se u nekim nuklearnim elektranama, graničnim prijelazima, rekreacijskim centrima. Uglavnom se koristi u svrhu autentikacije jer u svrhu identifikacije pokazuje lošije rezultate. U svrhu bolje preciznosti može se koristiti u višefaktorskim modelima uz otisak prsta i dlana, pokazuju studije. Preuzimanje slike može se odvijati kontaktno i beskontaktno, ovisno o sustavu. Također, o sustavu ovisi i hoće li se dlan okrenuti prema gore ili prema dolje (Jain et al., 2011.).

Biometrijski potpis počiva na ideji da svaki pojedinac ima posebni način potpisivanja, karakterističan za sebe. Potrebno je razlikovati statički i dinamički potpis. Statički se odnosi na samu sliku potpisa, dok dinamički potpis prati različite parametre zbog kojeg ga se može nazivati biometrijskim. Uređaj na kojem se korisnik potpisuje prati dinamiku njegovog potpisivanja što uključuje brzinu, kut, poteze i druge karakteristike potpisa (Thakkar, 2022.).

Dinamika tipkanja metoda je koja se temelji na načinu tipkanja pojedinca na tipkovnici. Spada u bihevioralne biometrijske metode. Rani tragovi dinamike tipkanja kao biometrijske metode dolaze još iz razdoblja drugog svjetskog rata. Zbog vrlo malih ulaganja koja su potrebna (tipkovnice nisu pretjerano skup proizvod), dinamika tipkanja možda je i najbolja opcija za višefaktorsku autentikaciju. Mjere koje se koriste u ovoj metodi uključuju „vrijeme pritiska prsta o tipku na tipkovnici“ te „vrijeme između otpuštanja pritiska sa tipke do sljedećeg pritiska tipke“ (Biometric solutions, b.d.).

Prepoznavanje oblika uha još je jedna metoda biometrijske identifikacije. Primamljiva je jer ne zahtijeva slikanje ljudskog lica, razvoj uha se smatra linearnim još od djetinjstva, a nije podložan promjenjivosti s obzirom na starenje. Također, uho nema veliku sklonost promijeni svojeg izgleda prilikom promjena grimasa na licu što bi moglo utjecati na preciznost procjene. Koraci u procesu identifikacije slični su onim standardnim koracima biometrijske identifikacije (Jain et al., 2011.).

Iako još uvijek nije široko prihvaćena metoda, ona je i dalje predmet istraživanja kao npr. u svrhu identifikacije pacijenata u bolnici (Etter et al., 2019.).

Prepoznavanje otiska dlana metoda je identifikacije slična otisku prsta jer se bazira na detaljima na koži, iako ima puno užu primjenu. Uz otisak dlana, također vrijedi spomenuti i otisak stopala koji se također smatra unikatnim detaljem na ljudskom tijelu, no ono se koristi možda i jedino kod identifikacije novorođenčadi jer ih je mnogo jednostavnije preuzeti u usporedbi sa otiskom dlana. (Jain et al., 2011.)

Kao biometrijske metode prepoznavanja koje su primjenjene u praksi ili barem predmetom izučavanja valja navesti i prepoznavanje ljudskog hoda (Jain et al., 2011.), prepoznavanje vene u prstu (Kono, 2002. kako je navedeno u Shaheed et al., (2018.) i analiziranje EKG-a ljudskog srca (El_Rahman, 2019.). Široka lepeza različitih biometrijskih metoda ostavlja dojam da su otkrića novih, za svakog čovjeka jedinstvenih značajki na tijelu, i dalje moguća.

4.6. Prednosti i izazovi

Važan faktor uspjeha biometrijske tehnologije zasigurno leži u odgovorima na postojeće sigurnosne probleme koji su pratili konvencionalne metode identifikacije. S druge strane, biometrijska tehnologija je za sobom donijela neke nove probleme oji su diskutirani u sljedećem poglavlju.

Govoreći o biometriji, Chapple (2022.) navodi kako se u kontrolama pristupa koristi biometrija kako bi „precizno identificirali i/ili autenticirali pojedinca“.

Jain et al. (2011.) navode prednosti biometrijske tehnologije uspoređivajući ih sa karakteristikama metoda korisničkog imena i lozinke. Pritom ističe kako upravo „lozinke, tokeni i identifikacijske karte mogu biti lako zaboravljene, izgubljene ili ukradene“. Biometrijske su karakteristike prirodno urođene u pojedinca, a time i teže dostupne trećim stranama. Nadalje navodi kako prilikom biometrijske identifikacije pristupnik mora biti fizički prisutan što smanjuje mogućnost prijevare prilikom identifikacije. U istom smjeru idu i Szűcs et al. (2020) koji ističu kako kod metoda koje se baziraju na onome što korisnik ima i onome što korisnik zna, sustav provjerava zna li pristupnik ili ima li pristupnik ono što bi trebao znati ili imati. Međutim, ne provjerava je li vlasnik te određene lozinke ili kartice uistinu ta ista osoba koja pokušava dobiti pristup sustavu. Rješenje tog problema pronalaze upravo u biometrijskoj tehnologiji. Prema Pagnin and Mitrokotsa (2017.), jedna od najvećih prednosti biometrijske tehnologije leži u slobodi od pamćenja lozinki i nošenja uređaja za fizičku identifikaciju.

Shahnewaz (2015.) ističe kako je prednost biometrije jednostavno to što sa visokom pouzdanošću može diferencirati pojedince na temelju njihovih biometrijskih karakteristika. Nadalje, smatra da biometrijska tehnologija štedi vrijeme, a generalno je jeftinija i može pronaći svoju primjenu u različitim područjima. Khan and Efthymiou (2021.) u svojem radu koji se bavio implementacijom biometrijske tehnologije u zračnim lukama navode kako je

implementacija biometrije dovela do „bržeg procesuiranja putnika, kraćih redova čekanja i, kao rezultat toga, većeg zadovoljstva putnika."

Napredak u sigurnosti i pouzdanosti biometrijskih sustava bilježe Lee i Jeong (2021.) koji u svojem radu opisuju korištenje blockchain tehnologije zajedno sa biometrijskim sustavima.

S druge strane, biometrijska tehnologija kao ozbiljno suvremeno rješenje za pitanja osobne identifikacije legitimno je podložna adresiranju svojih nedostataka i izazova, kao što bi trebao biti slučaj sa svime s čime se neko društvo susreće.

Determiniranjem izazova bavili su se National Research Council et al. (2010.) koji već na prvim stranicama navode probabilistički karakter biometrije kao problem. Probabilistički karakter govori kako se biometrijski sustav ne bazira na apsolutnoj, 100-postotnoj točnosti, već na vjerojatnosti. Ova činjenica, ako ćemo biti iskreni, ipak donosi val nemira i nesigurnosti u čovjekovu svijest, pogotovo ako su u pitanju osobnosti koje nisu sklone svoje živote podrediti vjerojatnosti već traže svojevrsnu sigurnost u svemu. Samim time što je biometrijski sustav temeljen na vjerojatnosti, znači i da je pogrješiv. Vjerojatnost za pogrešku može biti reducirana, ali nikada u potpunosti isključena. Osoblje koje radi na razvoju sustava mora biti spremno očekivati i reagirati na pogreške iako one mogu biti svedene na minimum. Nadalje, uzme li se pogrješivost sustava kao činjenica koja se veže za biometrijske tehnologije, to može dobiti preveliki naglasak što će rezultirati negativnim konotacijama biometrijske tehnologije u društvu.

National Research Council et al. (2010.) nadalje navode razne faktore koji mogu utjecati na volatilnost biometrijskih značajki kod čovjeka. Navodi se faktor starenja koji je neizostavno prisutan kod čovjeka, a čovjek je nositelj biometrijskih značajki. Starenjem je biometrijska značajka podložna promjenama, a na promjene također mogu utjecati promjene zdravstvenog stanja, stres, uvjeti u okruženju i drugi aspekti. Kako je bitna kvaliteta biometrijske značajke na čovjeku, tako je bitna i kvaliteta uređaja koji tu značajku preuzima. Na umu treba imati i ostale uvjete koji mogu utjecati na kvalitetu preuzetnog uzorka, a nisu vezane uz samog čovjeka već uz uređaj. Primjer tome može biti razina svjetlosti u okruženju prilikom preuzimanja uzorka. Kao izazove navodi i razlike u postojećim algoritmima za ekstrakciju detalja iz uzorka koji mogu utjecati na konačnu funkcionalnost samog sustava.

Daljnji izazovi mogu se uvidjeti kroz usporedbu relativno nove tehnologije sa onim starijima (možemo li ih nazvati konvencionalnima?). U ovom slučaju to se odnosi na usporedbu biometrijske tehnologije sa sustavima temeljenima na lozinkama ili tokenima. Kako ističu

National Research Council et al. (2010.), prilikom gubitka ili provale u sustav koji je baziran na lozinkama ili tokenima, vrlo se lako izdaje nova lozinka ili novi token koji na neki način „oporavljaju“ sustav i iznova osiguravaju korisnika koji je u ovom slučaju bio žrtva napada. Međutim, ukoliko se kompromitira sustav temeljen na biometrijskim značajkama, problem nije tako lako rješiv. Biometrijska je značajka ono što čovjek ne može promijeniti i u tim slučajevima postoji opasnost od krađe identiteta na što pažnju ukazuju Pagnin i Mitrokotsa (2017.) kao i Yang et al. (2019.).

Problem postaje još veći kada postoji više sustava koje korisnik koristi, a pristup svakome je temeljen na biometriji. Tada incident u jednom sustavu (krađa biometrijskog podatka) predstavlja ranjivost i za druge sustave jer varalica taj podatak može koristiti za pristup ostalim sustavima. Usporedimo li takvu potencijalnu situaciju sa principima sigurnosti vezanih za sustave temeljene na lozinkama, uviđa se kako ovakav razvoj situacije ne bi imao previše potencijala jer bi korisnik posjedovao različite lozinke za različite sustave kojima pristupa i na taj način bio osiguran. Na kraju poglavlja o izazovima biometrijske tehnologije, valja navesti da National Research Council et al., (2010.) smatraju da „niti jedna biometrijska karakteristika nije dovoljno pouzdana za identifikaciju pojedinca u obujmu svjetske populacije“, a kao razlog tome navode pojedince koji iz nekog razloga ne posjeduju određenu biometrijsku karakteristiku, pojedince koji su vrlo slični drugim pojedincima te učinke ekstrakcije tih uzoraka koji mogu narušiti kvalitetu uzorka. Također, kroz slikoviti primjer u kojem je analizirana funkcionalnost mjera FMR i FNMR (False match rate i false nin-match rate) zaključuje kako korištenje tih mjera će u velikoj mjeri precijeniti povjerenje koje bismo trebali imati u sustav (National Research Council et al., 2010.).

4.7. Primjeri korištenja biometrijske tehnologije

U bolnicama za antiretroviralnu terapiju u afričkoj državi Malavi napravljeno je istraživanje na temu biometrijske identifikacije. Implementacija biometrijske tehnologije tada je bio novi projekt Ministarstva zdravstva u Malaviju te je pred njima zadatak da se razviju procedure i pravila vezana za implementaciju sustava. Cilj istraživanja bio je uvidjeti stajališta o korištenju biometrije sa etičkog aspekta nutar zdravstvenog sustava u Malaviju, kao i prepoznavanje najboljih rješenja. U istraživanju su sudjelovali klijenti bolnice, ljudi koji surađuju sa tamošnjim ministarstvom zdravstva na implementaciji biometrijskih sustava (implementatori) te dužnosnici iz ministarstva. Sveukupno je u istraživanju sudjelovalo 30 ljudi, a kroz intervjue

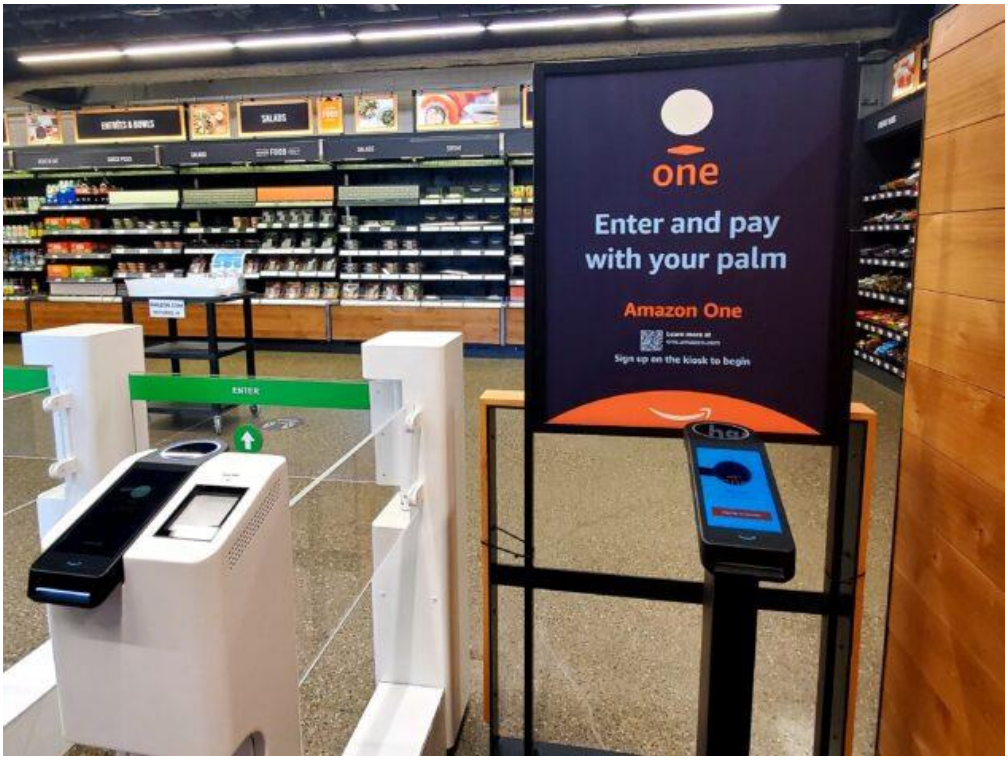
razgovaralo se o biometrijskoj tehnologiji i temama koje se na nju nadovezuju (Mwapasa et al., 2020.).

Istraživanje je pokazalo da je generalna razina poznavanja biometrijske tehnologije niska, a kod klijenata bolnice je čak i interes za poznavanje nizak zbog toga što je njima ipak najvažnije da prime potrebne terapije, a u takvim okolnostima malo tko će biti zainteresiran za biometrijsku tehnologiju. U Malaviju, otisak se prsta koristi u slučajevima nepismenih ljudi koji nisu sposobni potpisati se na dokument. Zbog toga klijenti koji su dolazili u bolnicu isprva nisu niti razumjeli pravi razlog sakupljanja otisaka prstiju u zdravstvenoj ustanovi. Također, u Malaviju zdravstveni sustav još uvijek funkcionira po zdravstvenim kartonima u fizičkom obliku što dovodi do situacija da neki pojedinci iz nekoga razloga imaju po pet ili šest kartona istovremeno, što uvelike otežava kontinuirano praćenje njegovog zdravstvenog stanja. Digitalizirani kartoni bazirani na biometriji bi vjerojatno imali potencijal dovesti reda u takvo stanje. Prema ispitanim klijentima, trenutačno stanje sa zdravstvenim kartonima narušava njihovu privatnost i povjerljivost zbog toga što karton sadrži podatke o HIV statusu osobe i dovodi ih do stigmatiziranosti u društvu. Upravo to navode i kao razlog zašto neki imaju po dva zdravstvena kartona: jedan u kojem piše stvarni HIV status, a drugi koji ne sadrži HIV status. Biometrijska bi tehnologija uz digitalizaciju zdravstvenih podataka mogla smanjiti izloženost HIV pozitivnih osoba da budu društveno stigmatizirani. S druge strane, implementatori sustava izrazili su skeptičnost prema korištenju biometrije i elektroničkih zdravstvenih podataka zbog ranjivosti sustava i mogućih krađa podataka. I klijenti i implementatori složili su se o prednostima uvođenja biometrije i elektroničkih zdravstvenih zapisa jer bi postojala jedinstvena mreža koja bi povezala medicinske zapise od različitih pružatelja medicinskih usluga te bi klijent, gdje god da se nalazio, znao da onaj tko mu pruža medicinsku uslugu ima sav uvid u njegovu dokumentaciju, što do sada nije bio slučaj. Također, ispitanici su potvrdili da je biometrijska tehnologija donijela benefite u pogledu bržeg protoka pacijenata i kraćeg vremena čekanja u klinikama. Naravno, potrebno je samo spomenuti i druge izazove koji se trebaju uzeti u obzir u ovakvom projektu, kao što je to obučenost osoblja, odnos troškova i koristi i dr. Na kraju, implementatori su zaključili kako je potrebno daljnje istraživanje i analiziranje kako bi se odredilo treba li proširiti korištenje biometrijske tehnologije i elektroničkih zdravstvenih zapisa u Malaviju (Mwapasa et al., 2020.).

Kompanija Amazon bavi se trgovačkim djelatnostima te se odlučila na primjenu biometrijske tehnologije u svrhu plaćanja u svojoj trgovini. Prva ovakva trgovina otvorena je u Seattleu u Sjedinjenim Američkim Državama. Amazon se odlučio koristiti tehnologiju beskontaktnog

prepoznavanja otiska dlana, iako i ne samo dlana već i uzoraka vene na dlanu istovremeno. Razlog preferencije ove metode naspram ostalih je povećana razina privatnosti. Podaci koji su potrebni da korisnik može započeti sa ovakvom metodom plaćanja jesu broj mobitela i broj kredine kartice (Warren, 2020.).

Poznavajući već principe, razloge i ciljeve korištenja biometrijskih tehnologija u različite svrhe, lako je razumjeti operativni proces ove inovacije i ono što se događa u pozadini. Biometrijski podaci, koji su ovom slučaju otisak dlana (i uzorci vene) jednoznačno identificiraju kupca koji je registriran u Amazonov sustav. Identificirajući kupca, sustav povlači njegove podatke o kreditnoj kartici kako bi uspješno odradio transakciju odnosno naplatio račun. Zapravo, sam sustav ovdje igra nekakvu ulogu blagajnika, a za kupca je proces kupovine mnogo jednostavniji. Naravno, kao i svaka druga biometrijska tehnologija, ili tehnologija autentikacije općenito, ima svoje prednosti i nedostatke od praktičnih do sigurnosnih razloga. Biometrijski podaci koje organizacija preuzima od svojih klijenata pohranjeni su u računalnom oblaku (engl. *cloud*) što je samo po sebi podiglo pitanja o sigurnosti pohranjivanja tako osjetljivih identifikacijskih podataka. No, kako ističe Reuben Binns (Vincent, 2020.), profesor iz područja zaštite podataka, Amazon gradi cijeli sustav koji počiva na cloud tehnologiji te je zbog toga u ovom slučaju teško očekivati bilo kakvo drugo rješenje osim clouda, a pitanje sigurnosti takvoga rješenja smatra posebnom temom. Što se tiče same biometrijske metode identifikacije, Binns pojašnjava kako je „prednost ta što je taj podatak uvijek sa vama, nije nešto što možete izgubiti, ali je isto tako i nedostatak jer ga ne možete promijeniti“ (Vincent, 2020.).



Slika 18: Amazon One registracijski skener (desno) i ulazni skener (lijevo)

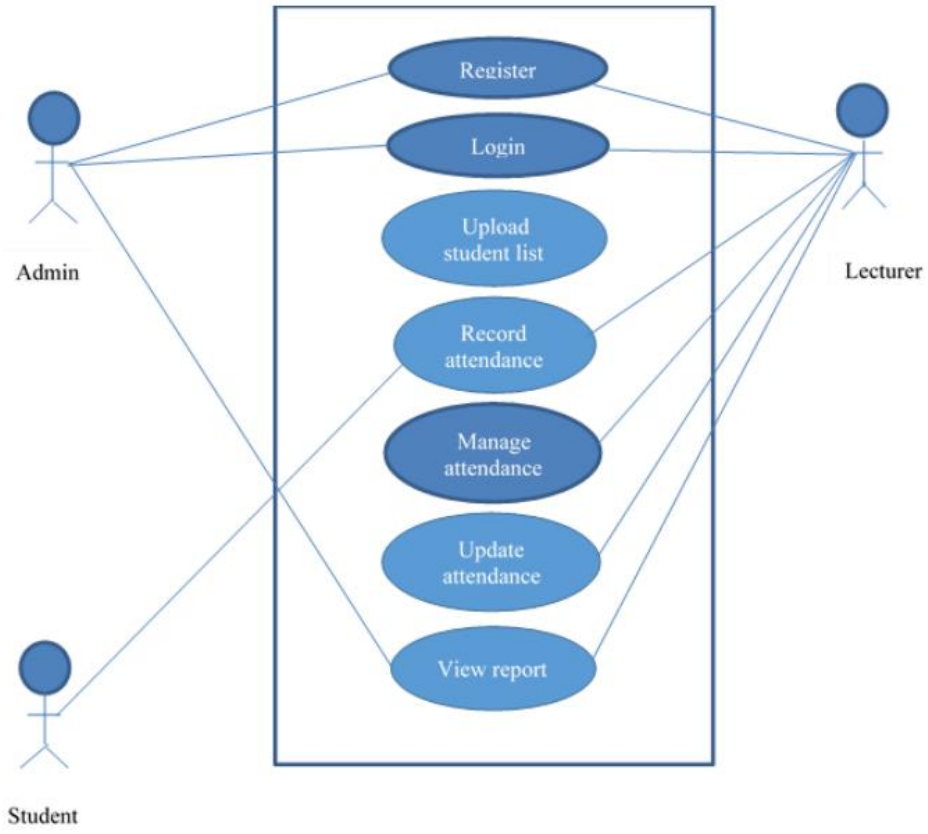
Izvor: Bishop, T. (2022.)

Sveučilište u Kuala Lumpuru odlučilo je pratiti prisutnost studenata na nastavi pomoću biometrijske tehnologije.

Naime, istraživanja pokazuju kako se biometrijskom identifikacijom pojednostavlja proces prijave tj. potpisivanja studenata kako bi označili svoju prisutnost na nastavi, a također se i smanjuje mogućnost prevare tako što studenti više ne bi mogli popisivati kao prisutne one koji su zapravo odsutni sa nastave (Banerjee et al., 2012. i Dey, 2018., navedeno u Lamin et al., 2021.).

Proces popisivanja prisutnih studenata izgledao je isto kao što je to slučaj na većini fakulteta u Hrvatskoj, a to je putem potpisne liste. Početkom predavanja predavač bi listu sa imenima studenata poslao da kruži po učionici te bi se svaki student trebao potpisati pored svog unaprijed isprintanog imena kako bi potvrdio svoju pristunost. Na kraju predavanja predavač bi provjerio je li broj potpisanih studenata jednak broju prisutnih studenata na nastavi. Korištenjem biometrijske tehnologije studenti bi se identificirali otiskom prsta na uređaju prilikom ulaska u učionicu što bi uvelike pojednostavilo proces praćenja prisutnosti. U

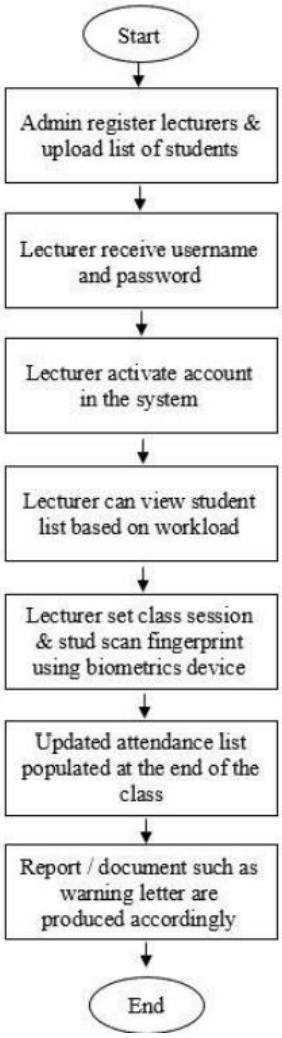
nastavku slijedi prikaz use-case dijagrama i dijagrama slijeda aktivnosti i objašnjenje funkcioniranja sustava (Lamin et al., 2021.).



Slika 19: Use-case dijagram

(Lamin et al., 2021.)

Use-case dijagram prikazuje skup aktivnosti nužnih za funkcionalnost sustava te su aktivnosti povezane sa ulogama koje ih odrađuju. Administrator sustava uloga je koja djeluje u aktivnostima registracije, prijave i pregledavanja zapisnika. Student je uloga sa najmanje dodijeljenih aktivnosti tj. samo jednom, a to je samo aktivnost prijave da je prisutan na nastavi, što se u konačnici odnosi na pružanje otiska prsta uređaju za skeniranje. Profesor odnosno predavač uloga je sa najviše dodijeljenih aktivnosti: registracija i prijava, aktivnost označavanja prisutnosti na nastavi te uređivanje i osvježavanje liste prisutnosti te uvid u zapisnike.



Slika 20: Dijagram slijeda aktivnosti

(Lamin et al., 2021.)

Dijagram slijeda aktivnosti prikazuje širi proces funkcioniranja sustava koji je podijeljen na manje korake koji sačinjavaju taj proces. Proces započinje pripremom sustava od strane administratora i sagledavajući ga u kontekstu akademskih perioda, može se zaključiti kako se radi o početku semestra. Razlog tome je što je u prvom koraku administrator koji osvježava liste predavača te liste studenata koji su upisali određeni kolegij, a te se aktivnosti obično izvršavaju početkom semestra. Sljedeća aktivnost je dodijeljivanje korisničkog imena i lozinke profesoru tj. predavaču koji će biti odgovoran za bilježenje prisutnosti putem za to predviđenog uređaja. Potom će predavač u trećem koraku aktivirati svoj korisnički profil u sustavu. Vjerojatno prvom prijavom u sustav taj će korak biti odrađen. Sada profesor ima uvid u liste studenata koji su upisali njegov predmet. Od njih se očekuje prisutnost na nastavi. Daljnji koraci odnose se na aktivnosti koje se događaju neposredno prije, tijekom i nakon predavanja.

Prvi od tih koraka odnosi se na aktivaciju uređaja prije predavanja koje će omogućiti studentima prijavu putem biometrijske tehnologije. Potom će taj sustav biti aktivan tijekom cijelog predavanja i bilježiti studente koji se registriraju. Na kraju predavanja profesor će zaključiti prijave, osvježiti listu registriranih te objaviti upozorenja studentima ukoliko je detektiran njihov izostanak.

Eksperiment zaključuje kako je implementacija biometrijske tehnologije pokazala mnoge prednosti, ali i sugerira daljnja unaprjeđenja ako bi sustav bio još efikasniji (Lamin et al., 2021.).

Zračne luke u Dublinu i Sjedinjenim Američkim Državama mjesto su na kojem se implementirala tehnologija prepoznavanja lica. Zračne luke od velike su državne značajnosti što ih može svrstati i u kategoriju kritične nacionalne infrastrukture (Brooks, 2016., navedeno u Khan & Efthymiou, 2021.).

Golem rast avioindustrije zahtijeva sofisticiranija rješenja kontrole protoka ljudi u svrhu minimiziranja potencijalnih opasnosti (podsjetnik na malezijski „nestali“ zrakoplov 370 u kojem su bila dva putnika sa ukradenim putovnicama). U ovom istraživanju fokus je bio na metodi prepoznavanja lica kao metode za identifikaciju osoba. Ovu metodu karakteriziraju jednostavnost prikupljanja i prihvaćenost u društvu, ali i visoka mogućnost da bude zloupotrijebljena prevarom te niska distinktivnost. Tehnologija je implementirana u sklopu američke granične kontrole (engl. CBP – Custom and border protection) u zračnim lukama. Prednosti biometrijske tehnologije u ovom kontekstu odnose se na brži protok putnika kroz luku i njihovog ukrcavanja na let. Izazovi s kojima se tehnologija susrela bili su različiti (Khan & Efthymiou, 2021.).

Prema Khan & Efthymiou (2021.), tehnologija se susrela sa nepravilnostima u podudaranju fotografija pri čemu su putnici mlađi od 29 godina činili 18% putnika, a čak 36% onih kojima su fotografije bile pogreškom odbijene. Mlađi od 29 godina i stariji od 70 godina imali su niže stope podudarnosti. Ovaj bi se problem mogao pripisati dugačkom periodu vremena koji je prošao od inicijalnog preuzimanja fotografije (a to su vjerojatno one koje su u putovnici) pa do pristupanja sustavu za prepoznavanje lica. Kroz dugački vremenski period lice se moglo izmijeniti u dovoljnoj mjeri da zbuni sustav za prepoznavanje, a neki navode i ulogu osvjetljenja kao faktora koji može uvelike izmijeniti kvalitetu slike lica prilikom preuzimanja (Zou et al., 2007, navedeno u Khan & Efthymiou, 2021.). U istom je istraživanju također primjećena i razlika u stopama podudarnosti kada se uspoređuju američki državljani sa stranim

državljanima, što se pripisuje ulozi digitalnih galerija gdje su slike stranih državljana bile često dostupne. Nadalje, Khan & Efthymiou ističu da je problem bio i u tome što je tijekom pilot faze za čak 15% putnika sustav nije mogao detektirati podudarnost, što se objašnjava „tehničkim problemima“. Dostupnost bežičnog interneta koji je od krucijalne važnosti za osoblje također je utjecalo na konačne performanse sustava. Zbog poteškoća koje se pojavljuju u procesu, mnoge aviokompanije odustaju od biometrijske identifikacije putnika i vraćaju se na konvencionalne metode identifikacije. Od ostalih izazova valja spomenuti prezaposlenost osoblja, potrebu za podrškom od strane stakeholdera (zračne luke i aviokompanije) te zabrinutost oko privatnosti od strane putnika (Khan & Efthymiou, 2021.).

5. Istraživanje: biometrijska tehnologija i društvo

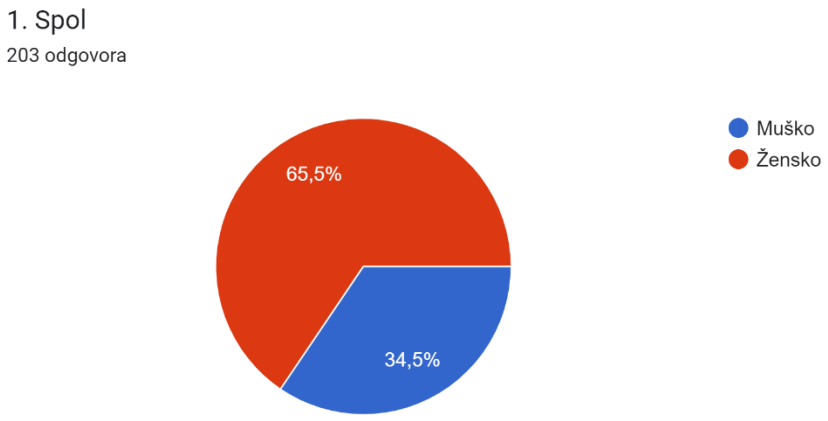
5.1. Anketni upitnik o biometrijskoj tehnologiji

U sklopu pisanja diplomskog rada provedeno je istraživanje o percepciji biometrijske tehnologije u društvu. Istraživanje se provodilo pomoću anketnog upitnika koji je sadržavao 22 pitanja. Pitanja su jednim dijelom preuzeta iz prošlih istraživanja (ORC International, 2002; Furnell i Evangelatos, 2007; German i Barber, 2018), a neka su pitanja autorovo vlastito djelo. Istraživanje je provedeno na populaciji bez dobnog ograničenja, iako se kao ciljna skupina uzimaju mladi tj. grupa od 18 do 30 godina starosti. Njihovi rezultati su dobiveni kasnijom ekstrakcijom od sveukupnih prikupljenih podataka. Anketu je ispunilo 203 osobe koje spadaju u ciljanu dobnu skupinu, a prikupljani su u razdoblju od 15 dana tijekom srpnja 2022. godine. Anketa je podijeljena na društvenim mrežama (uglavnom Facebook) i to u grupe sa velikim brojem članova. To su uglavnom bile grupe koje okupljaju stanovnike određenog naselja, grupe studenata određenog fakulteta te grupe koje okupljaju članove određenih studentskih domova. Također, anketa je podijeljena u grupu širih poznanika autora rada u kojoj su prevladavali studenti.

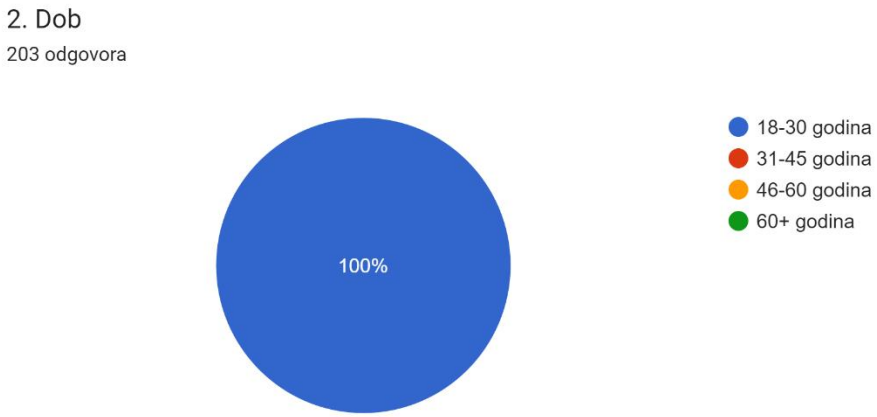
Mladež je upravo onaj segment društva koji se najviše služi internetom i uređajima koji su povezani na internet, a i najlakše im je prilagoditi se na inovacije koje, dapače, željno iščekuju. Često se zna reći „na mladima svijet ostaje“ stoga valja dobiti uvid u perspektivu mladih o biometrijskog tehnologiji i sigurnosti na internetu. To su neki od razloga zašto je baš ovaj segment društva odabran kao ciljna skupina istraživanja.

Anketa je prikupila 203 odgovora. Poštujući objektivnost koja je nužna u znanstvenim istraživanjima te samu statistiku kao znanstvenu disciplinu bez koje mnoga istraživanja ne bi niti mogla biti provedena, valja istaknuti kako je veličina uzorka premala da bi se s velikom pouzdanošću mogli donositi zaključci o cjelokupnoj populaciji. Ipak, to ne potkopava relevantnost istraživačkog rada, već naglašava njegov orijentacijski karakter. Tome u prilog idu i određene pravilnosti u odgovorima ispitanika kada se uspoređuje ovo istraživanje sa prošlim istraživanjima u kojima je postavljeno isto ili vrlo slično pitanje. Ta pravilnost ocrtava određeni obrazac mišljenja u društvu.

5.2. Rezultati ankete

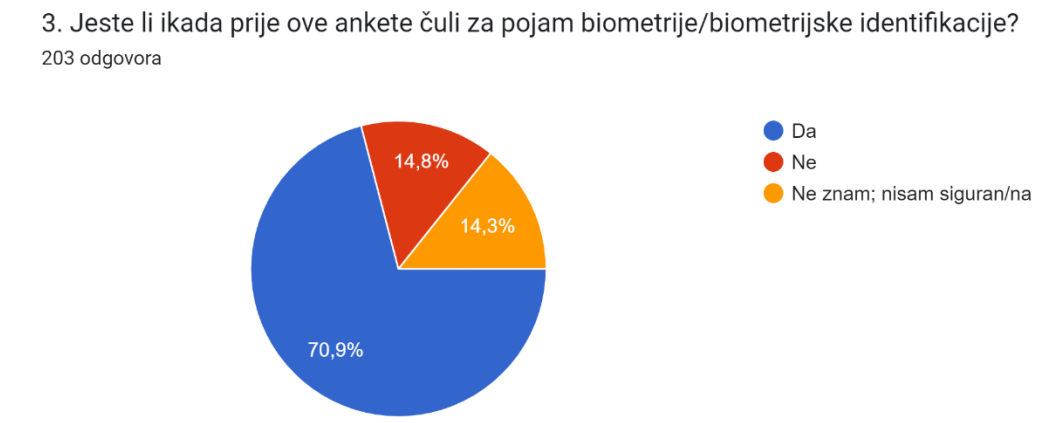


Slika 21: Pitanje 1



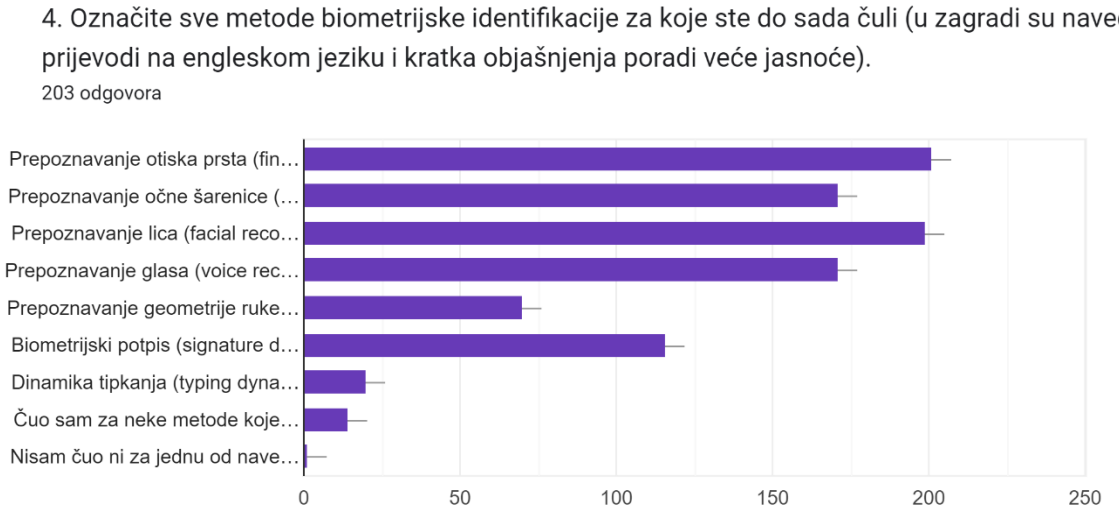
Slika 22: Pitanje 2

Na slici 21 vidljiva je spolna struktura anketiranih osoba. Ženski spol bio je u gotovo dvotrećinskoj većini naspram muškog spola. Slika 22 dokazuje da su 203 ispitanika bili u starosnoj dobi koja odgovara ciljanoj skupini.



Slika 23: Pitanje 3

Treće pitanje čije rezultate vidimo na slici 23 odnosilo se na poznavanje pojma biometrije tj. biometrijske identifikacije. Po rezultatima može se zaključiti kako je poznavanje pojma biometrije među mladima na relativno niskoj razini. No, usporedimo li ove rezultate sa rezultatima iz sljedećeg pitanja, interpretacija i konačno značenje rezultata bit će uvelike pojednostavljeni.

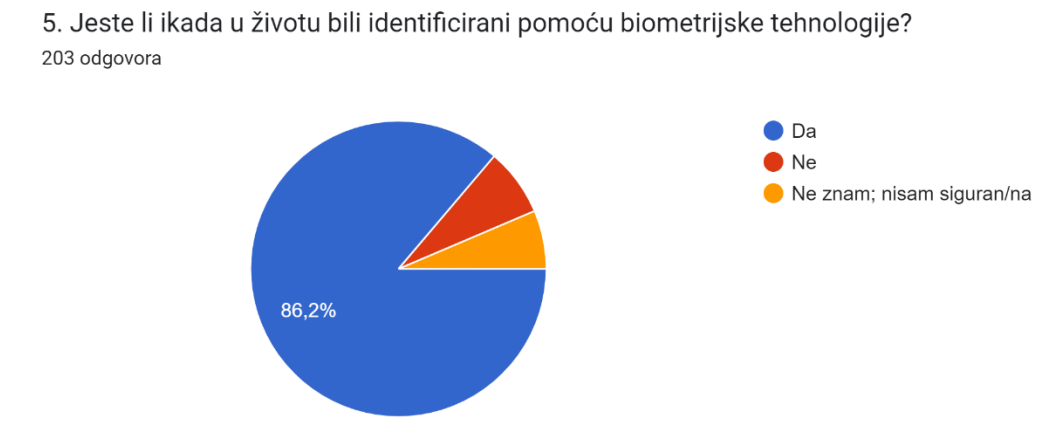


Slika 24: Pitanje 4

Četvrto pitanje čije rezultate vidimo na slici 24 odnosilo se na poznavanje konkretnih primjera biometrijske identifikacije. Prije samog pitanja, ispitanicima je dano sljedeće objašnjenje pojma biometrijske identifikacije:

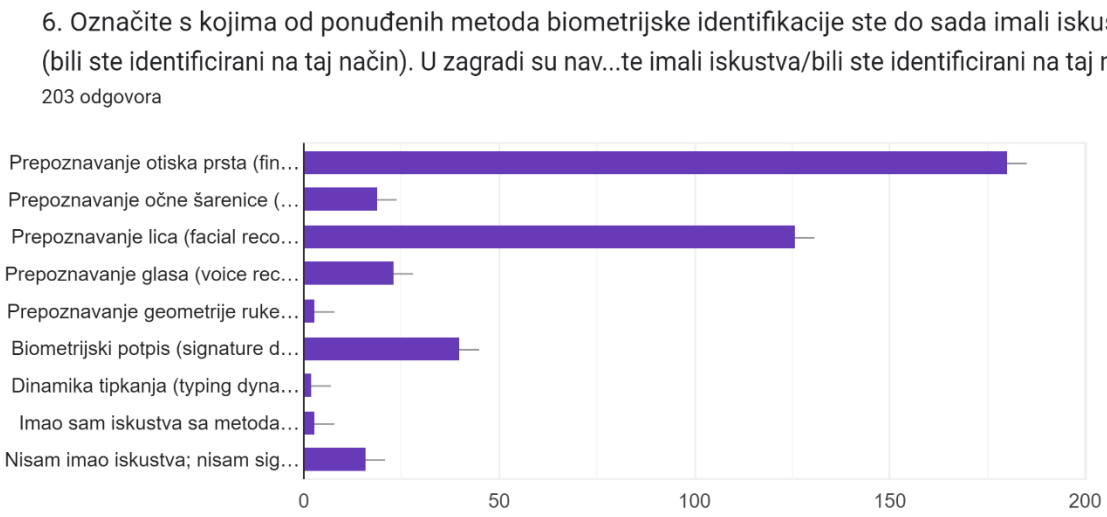
Biometrijska identifikacija odnosi se na potvrđivanje Vašeg identiteta pomoću neke fizičke ili bihevioralne karakteristike koju posjedujete, odnosno koja je dio Vas. Zbog svojih posebnosti i specifičnih detalja, neki dijelovi našeg tijela čine nas gotovo jedinstvenima u usporedbi sa drugima (kao npr. otisak prsta). Biometrijska tehnologija funkcionira način da uzme uzorak sa Vaše biometrijske osobine (npr. otisak prsta ili sliku očne šarenice), nakon čega taj uzorak pretvara u matematički zapis i pohranjuje ga u sustav. Sljedeći put kada trebate potvrditi svoj identitet (npr. za pristup nekim dokumentima), ponovno dajete svoj uzorak kojeg računalni sustav uspoređuje sa onim već pohranjenim u sustavu te na temelju podudarnosti tih uzoraka potvrđuje ili opovrgava Vaš identitet.

Od ispitanika se tražilo da označe biometrijske metode za koje su do sada čuli. Čak 201 osoba, odnosno 99% ispitanih označilo je prepoznavanje otiska prsta kao metodu za koju su već čuli, a 98% njih čulo je i za metodu prepoznavanja lica. 171 ispitanik, odnosno 84,2% ispitanih čulo je za prepoznavanje očne šarenice i prepoznavanje glasa. Sada vrijedi objasniti na koji način ovi rezultati pomažu interpretirati rezultate iz prethodnog pitanja. Naime, sudeći po prethodnom pitanju, samo je 70% ispitanih čulo za pojam biometrije, dok se po rezultatima iz ovog pitanja zaključuje kako je zapravo čak 99% ispitanih upoznato barem sa jednom od metoda biometrijske identifikacije. Prema tome, valja zaključiti kako se ovdje radi samo o nepoznavanju termina „biometrije“ u samoj njenoj teoriji. Ispitanici su naveliko čuli za biometrijske tehnologije, no gotovo 30% njih ne poznaje naziv „biometrija“ koji u teoriji objedinjuje sva njihova evidentna znanja i iskustva o tome području. Potrebno je istaknuti i ono kratko objašnjenje koje je stajalo prije samog pitanja. Možda je upravo to objašnjenje „upalilo lampice“ u glavama ispitanika pa je njihova reakcija bila: „aha, pa ja znam za to“ te je tako čak 99% njih označilo kako su čuli za prepoznavanje otiska prsta. Komu ili čemu se ovakav debakl informiranosti mladih o biometriji može prepisati zgodna je tema za neko sljedeće istraživanje. Valja još istaknuti kako svega 0,5%, odnosno jedan jedini ispitanik nije čuo ni za jednu od navedenih metoda biometrijske identifikacije, dok je njih 6,9% čulo za metode koje nisu ponuđene u odgovoru (to može biti npr. prepoznavanje vene)



Slika 25: Pitanje 5

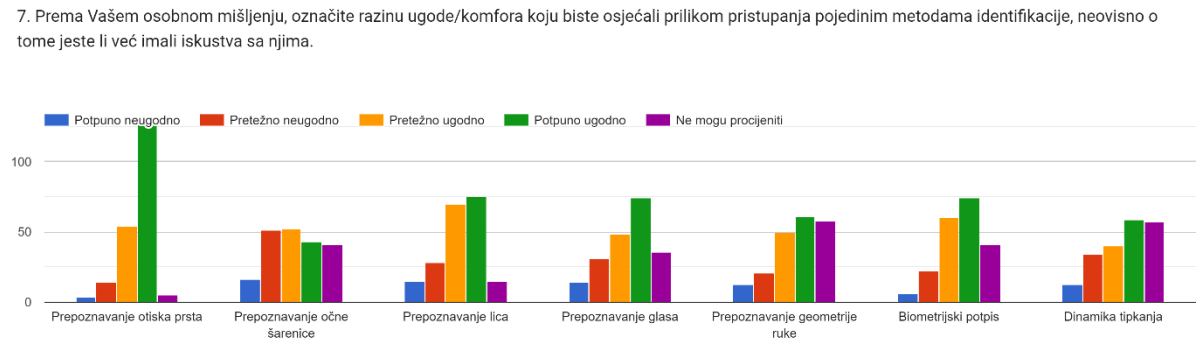
Peto pitanje na slici 25 pokazuje kako je velika većina u životu barem jednom bila identificirana pomoću biometrijske tehnologije. Objašnjenje o biometrijskoj tehnologiji uvelike je pomoglo da ispitanici prepoznaju o čemu se zapravo radi. Ako je njih 70% čulo za biometrijsku identifikaciju (pitanje 3), onda bi pozitivnih odgovora na ovo pitanje moglo biti samo manje od 70% jer ako nisu čuli za biometrijsku identifikaciju teško da mogu znati jesu li ikada u životu bili njome identificirani.



Slika 26: Pitanje 6

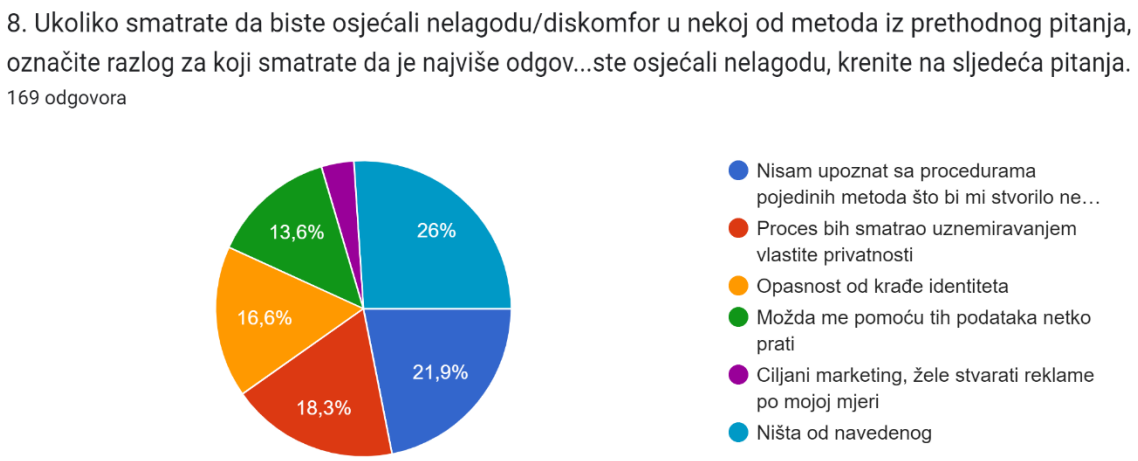
Šesto pitanje prikazano na slici 26 odnosi se na iskustva sa korištenjem biometrijske tehnologije. Ispitanici su trebali označiti sve metode sa kojima su do sada imali iskustva. Na prvom mjestu je očekivano bila metoda prepoznavanja otiska prsta. Zasluge za iskustva

ispitanika vjerojatno pripadaju suvremenim mobilnim telefonima koji danas imaju mogućnost otključavanja pomoću biometrijske tehnologije. Nakon nje slijedi metoda prepoznavanja lica što također možemo pripisati mobilnim telefonima. Na trećem mjestu, pomalo neočekivano, stoji metoda biometrijskog potpisa sa gotovo 20% ispitanika koji su imali iskustva s tom metodom. Valja uzeti u obzir kako postoji mogućnost nesporazuma. Naime, ispitanici su mogli biti u situaciji gdje su davali elektronički potpis, kao što je to npr. slučaj u bankama. Klijent na šalteru potpis daje posebnom olovkom na zaslon tableta. Međutim, to ne služi za identifikaciju ili verifikaciju, barem ne u biometrijskom smislu. Stoga, valja napomenuti mogućnost zabune kod ispitanika koji su, zbog slabe informiranosti, biometrijski potpis zamijenili elektroničkim. Usporedimo li rezultate sa istraživanjem navedenim na početku poglavlja, može se prepoznati kako je otisak prsta uvjerljivo najučestalija i najpoznatija metoda identifikacije.



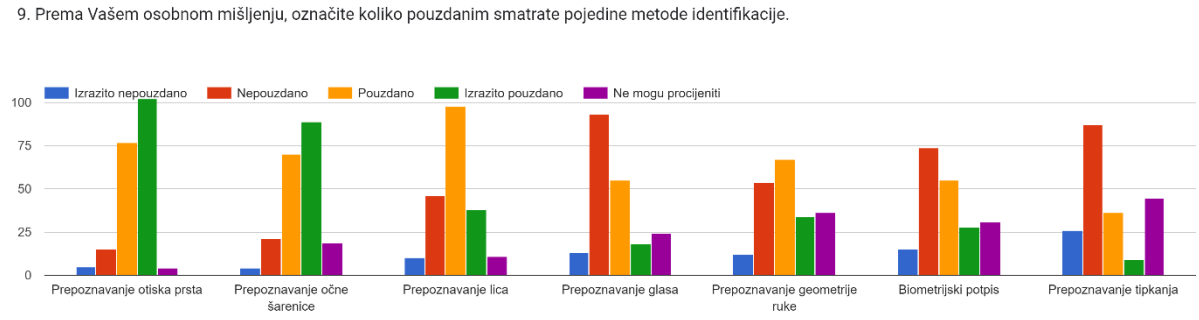
Slika 27: Pitanje 7

Sljedeće pitanje prikazano na slici 27 tiče se razine komfora prilikom pristupanja pojedinim metodama neovisno o tome radi li se o već doživljenom iskustvu ili o slobodnoj procjeni ispitanika. Ponovno je prepoznavanje otiska prsta metoda koja odskače od ostalih te možemo reći kako je najprihvatljivija metoda u javnosti. U prošlim istraživanjima navedenim na početku poglavlja metoda otiska prsta također je ona koja odskače po ovom pitanju, dok se god drugih prepoznaju slične distribucije odgovora. Također se primjećuje kako su mladi najzatvoreniji prema metodi prepoznavanja očne šarenice, s obzirom na to da je jedina metoda kojoj ocjena „potpuno ugodno“ nije dominantna.



Slika 28: Pitanje 8

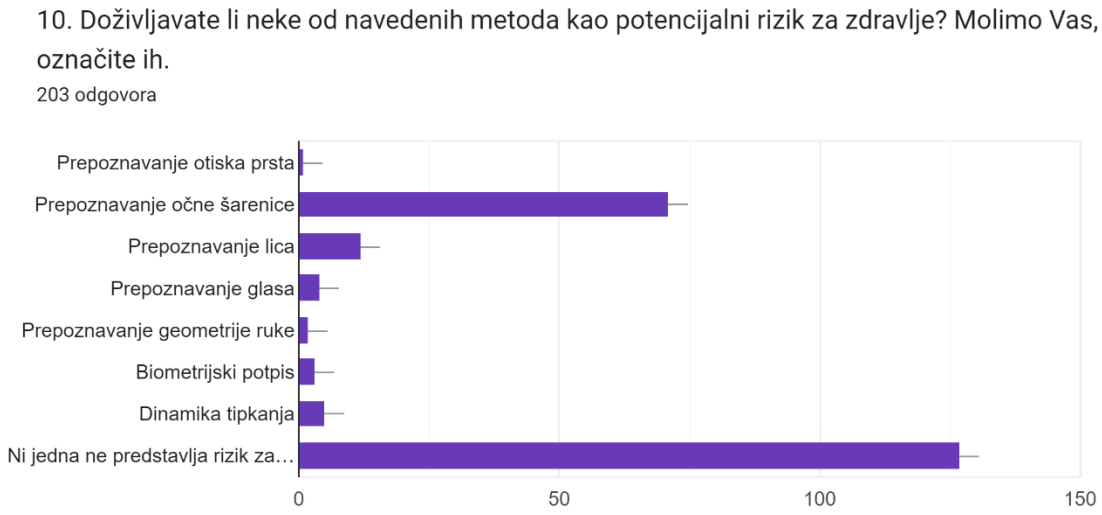
Osmo pitanje (slika 28) odnosilo se na razloge nelagode koju bi ispitanici osjećali prilikom pristupanja biometrijskoj identifikaciji. Na ovo pitanje je odgovorilo 169 ispitanika, a distribucija odgovora je prilično disperzivna. Više od četvrtine ispitanika osjećalo bi nelagodnu, ali niti jedan od ponuđenih odgovora nije razlog njihovoj nelagodi. Najviše ispitanika nelagodu bi osjećali zbog nepoznavanja procesa preuzimanja uzorka u pojedinim metodama što bi im stvorilo nemir i uzbuđenje.



Slika 29: Pitanje 9

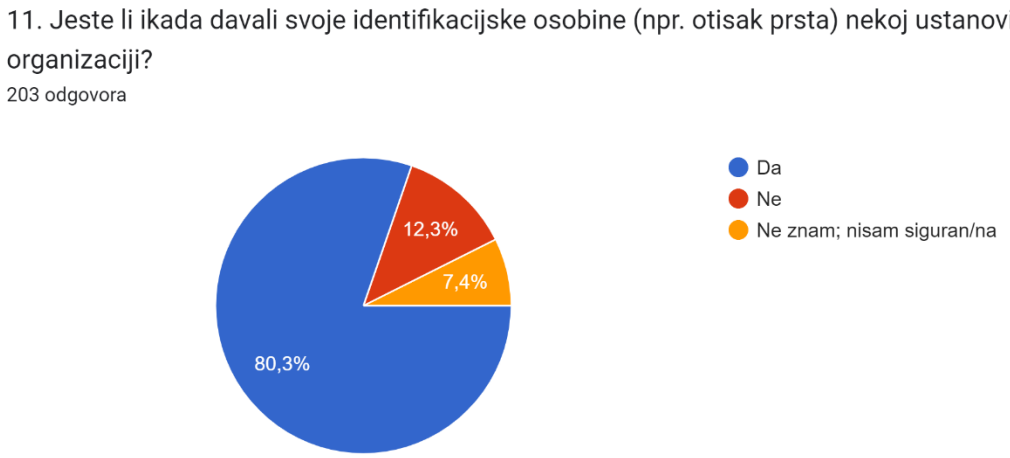
Slika 29 prikazuje percepciju pouzdanosti pojedinih metoda identifikacije. Ispitanici su mogli rangirati svoja mišljenja u četiri razine („izrazito nepouzdano“, „nepouzdano“, „pouzdano“, „izrazito pouzdano“). Ukoliko nisu mogli odlučiti između tih odgovora, mogli su označiti i neutralni odgovor („ne mogu procijeniti“). Iz grafova se može zaključiti kako se u društvu samo dvije ponuđene metode percipiraju najvećim dijelom kao izrazito pouzdane, a to su metoda prepoznavanja otiska prsta te metoda prepoznavanja očne šarenice. Čak 88% ispitanika smatra metodu otiska prsta pouzdanom ili izrazito pouzdanom, dok velikih 78% ispitanika

smatra metodu prepoznavanja očne šarenice pouzdanom ili izrazito pouzdanom. Među pouzdanije metode možemo ubrojiti i metodu prepoznavanja lica, dok su prema ostalim metodama ispitanici mnogo više skeptični. Uspoređujući rezultate sa rezultatima iz istraživanja (Furnell, S. i Evangelatos, K., 2007.), primjećuje se kako su otisak prsta i očna šarenica biometrijske značajke koje javnost smatra najpouzdanijima, a valja kazati i kako je metoda dinamike tipkanja ona kojoj se, u oba slučaja, najmanje vjeruje.



Slika 30: Pitanje 10

Deseto pitanje čiji je graf vidljiv na slici 30 pokazuje kako mladi uglavnom ne smatraju biometrijske tehnologije rizikom za zdravlje. Ipak, jedna se od njih ističe, a to je metoda prepoznavanja očne šarenice. Čak 35% ispitanika doživljava tu metodu kao potencijalni rizik za zdravlje. To možemo pripisati karakteristikama ljudskog oka: ono je vrlo osjetljivo te samim time otvara pitanja rizika za zdravlje ljudskog oka prilikom identificiranja očne šarenice. Javnost je vjerojatno zabrinuta zbog potencijalno negativnog djelovanja uređaja za skeniranje oka u smislu zračenja, svjetlosti i ostalih stvari pomoću kojih uređaj možda funkcionira. Iza očne šarenice, iako u puno manjoj mjeri, zabrinuti su metodom prepoznavanja lica što se također može pripisati njegovoj osjetljivosti, a i samo oko se nalazi na licu. Usporedimo li ove rezultate sa rezultatima iz drugih istraživanja (Furnell, S. i Evangelatos, K., 2007.) uočava se gotovo ista distribucija odgovora i velika skeptičnost prema skeniranju očne šarenice u kontekstu pitanja rizika za zdravlje.

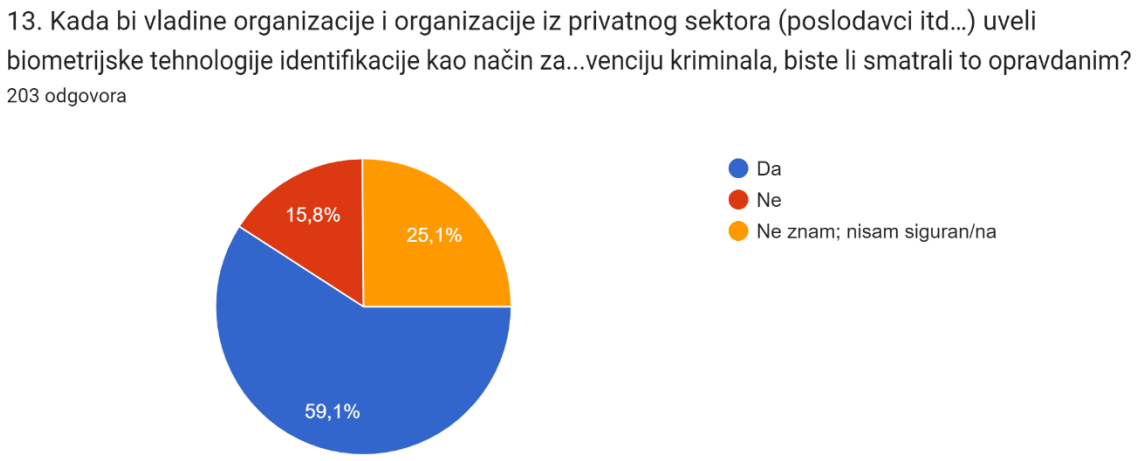


Slika 31: Pitanje 11

Slika 32: Pitanje 12

Jedanaesto pitanje (slika 31) pokazuje da je više od 80% ispitanika davalo svoje identifikacije podatke nekoj organizaciji ili ustanovi. Radi li se ovdje uglavnom o davanju otiska prsta u policiji (što je praksa prilikom izrade osobne iskaznice) ili korištenju otiska prsta za otključavanje mobitela (što je danas vrlo rašireno) može se samo pretpostavljati. Od 160 ispitanika koji su davali svoje biometrijske podatke nekoj ustanovi ili organizaciji, njih 133 smatra da je takav zahtjev bio primjeren (slika 32), a samo njih 8 (5%) da takav zahtjev nije bio primjeren. U američkom istraživanju koje je sadržavalo slično pitanje („Jeste li davali biometrijske podatke nekoj organizaciji u svrhu biometrijske komparacije?“), samo je 35,6% ispitanika odgovorilo pozitivno, a čak 58% negativno. Razlog tome, kako se navodi u tom istraživanju, može biti taj što ispitanici nisu percipirali otključavanje mobilnog telefona

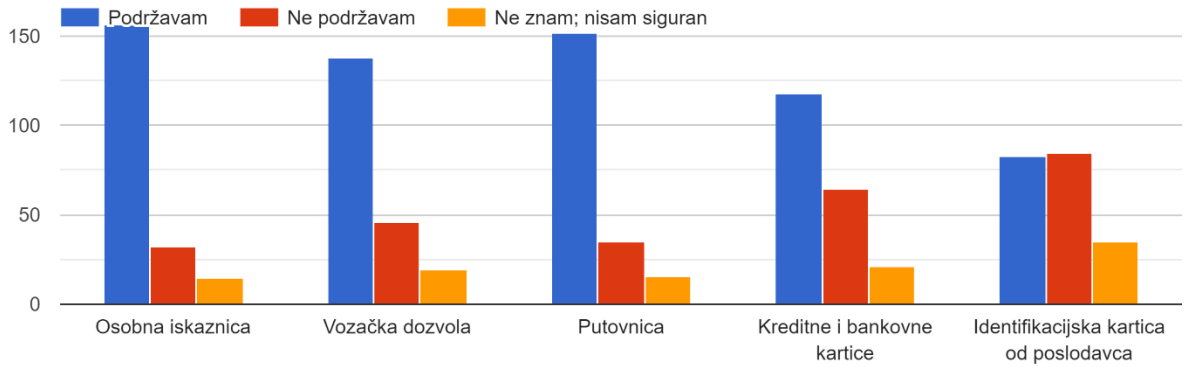
pomoću otiska prsta kao davanje svojih podataka organizaciji. U drugom istraživanju, doduše iz 2002. godine, 66% ispitanika odgovorilo je pozitivno i taj je zahtjev za njih 90% bio primjeren.



Slika 33: Pitanje 13

Trinaesto pitanje vidljivo na slici 33 ispitivalo je mišljenje ispitanika o opravdanosti uvođenja biometrijske tehnologije u privatni i javni sektor u svrhu prevencije kriminala. Niti 60% ispitanika nije imalo pozitivan stav prema uvođenju biometrijske tehnologije u svrhu prevencije kriminala, što ukazuje na ipak nezanemariv postotak skeptičnosti ili nesigurnosti prema biometrijskoj tehnologiji. Američko istraživanje iz 2002. godine koje je sadržavalo gotovo isto pitanje pokazuje da je čak 80% smatralo uvođenje biometrije u svrhu prevencije kriminala u najmanju ruku donekle opravdanim. Razlozi zašto mladi u hrvatskoj imaju čak 20 postotnih poena nižu razinu odobravanja prema ovom pitanju ostaju nepoznata, iako mogući odgovor na to pitanje može ležati u slaboj informiranosti mladih (25% ispitanih „ne zna“ ili „nije sigurno“) ili o povećanoj zabrinutosti za sigurnost vlastitih podataka.

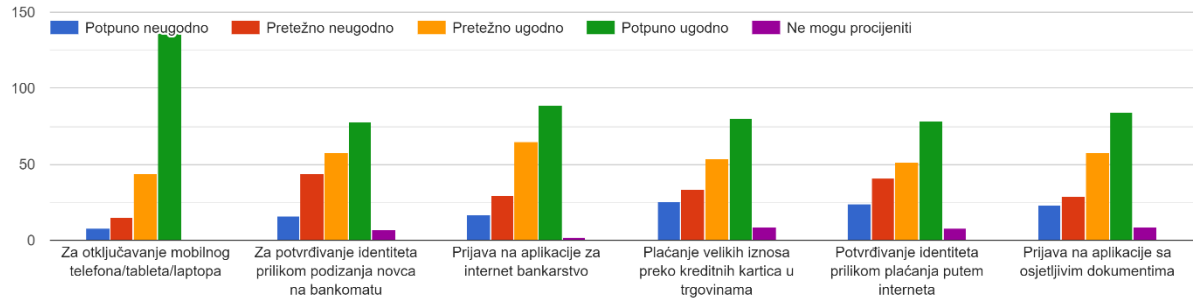
14. Označite biste li podržali dodavanje biometrijskih podataka na identifikacijske dokumente kao što su:



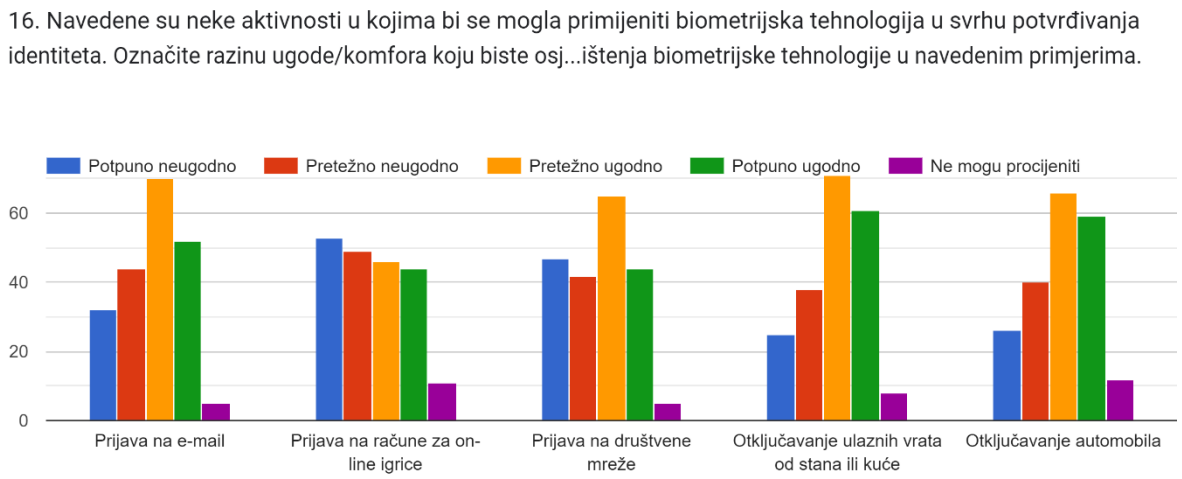
Slika 34: Pitanje 14

Pitanje broj 14 (slika 34) ispituje stavove mladih o dodavanju biometrijskih podataka na identifikacijske dokumente. Primjećuje se veća podrška dodavanju biometrijskih podataka na dokumente koji su uistinu pravno identifikacijski (izdaje ih država), a to su osobna iskaznica, vozačka dozvola i putovnica. Manju podršku bilježe kreditne i bankovne kartice, a većina ispitanika ne bi podržala dodavanje identifikacijskih podataka na kartice koje izdaje njihov poslodavac.

15. Navedene su neke aktivnosti u kojima bi se mogla primijeniti biometrijska tehnologija u svrhu potvrđivanja identiteta. Označite razinu ugode/komfora koju biste osjećali prilikom korištenja biometrijske tehnologije u navedenim primjerima.



Slika 35: Pitanje 15

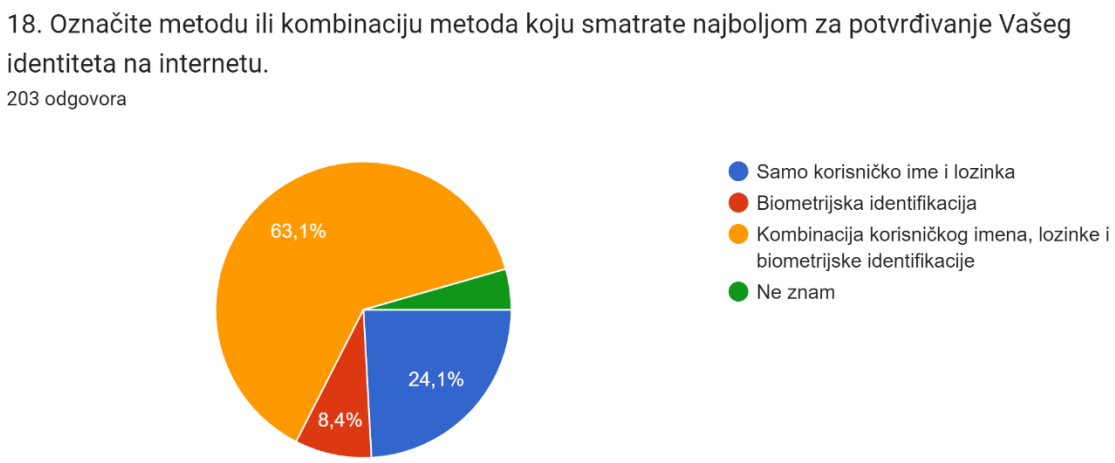


Slika 36: Pitanje 16

Pitanja broj 15 i 16 (slike 35 i 36) ispituju ispitanike o razini ugode koju bi osjećali pri određenim aktivnostima s pretpostavkom da u njima koriste biometrijske tehnologije za identifikaciju. Pitanja su podijeljena u dva seta radi lakše preglednosti prilikom ispunjavanja ankete. Gotovo 89% ispitanika osjećalo bi se pretežno ili potpuno ugodno za korištenje biometrije prilikom otključavanja mobilnog telefona ili prijenosnog računala. Vjerojatan razlog toga jest što se ova metoda već naširoko primjenjuje u navedenoj aktivnosti. U ostalim aktivnostima iz pitanja broj 15 također prevladava potpuna otvorenost prema primjeni biometrijskih tehnologija, ali je ta razlika manje izražena nego u prvom slučaju. U drugom setu aktivnosti, pod pitanjem broj 16, ispitanici su bili skloniji odgovoru „pretežno ugodan“ nego „potpuno ugodan“. Prema tome se može zaključiti kako su ispitanici u nekoj mjeri skeptičniji prema aktivnostima iz drugog seta nego prema onima iz prvog. Također, ispitanici su u većoj mjeri izražavali osjećaj potpune neugode naspram prvog seta pitanja. Prijava na račune za on-line igrice proizišla je kao aktivnost u kojoj bi se ispitanici osjećali najmanje ugodno koristiti biometrijsku tehnologiju. Više od 50% ispitanika smatra potpuno ili pretežno neugodnim koristiti biometrijsku tehnologiju u toj aktivnosti. Gotovo 44% ispitanika smatra pretežno ili potpuno neugodno koristiti biometrijsku tehnologiju prilikom prijavljivanja na društvene mreže.

Slika 37: Pitanje 17

Pitanje 17 (slika 37) odnosilo se na zlouporabu podataka. 66,5% ispitanika nije nikada bilo žrtva zlouporabe osobnih podataka. 24,6% ispitanika ne zna je li ikada bilo žrtvom zlouporabe osobnih podataka.

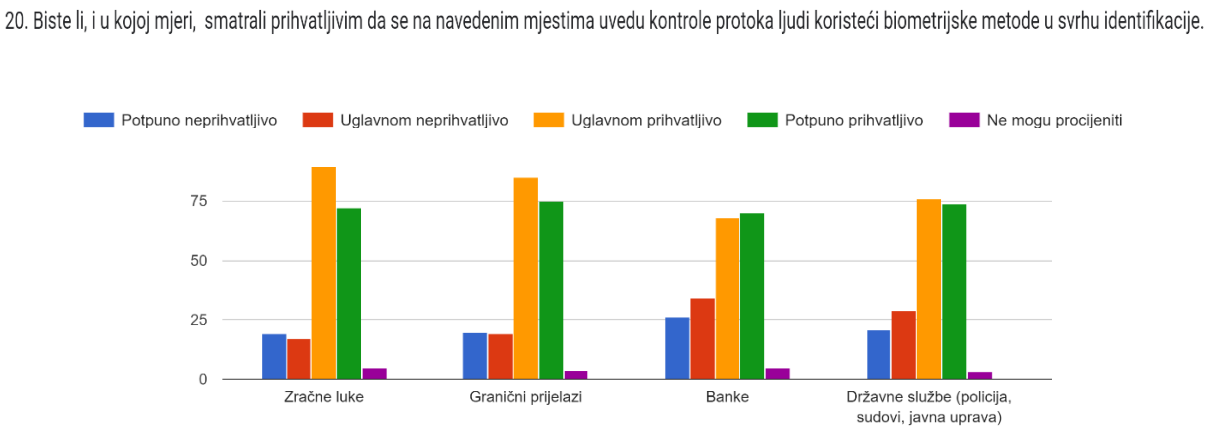


Slika 38: Pitanje 18

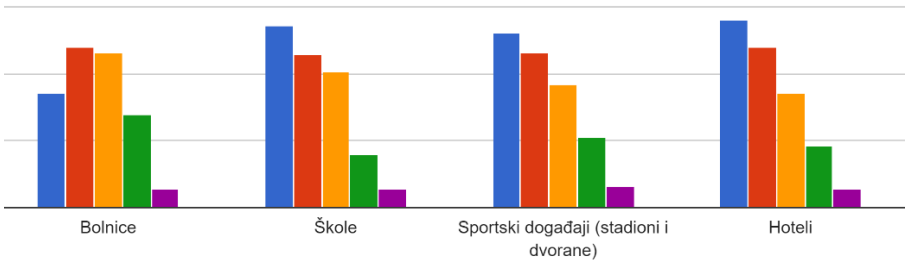
Pitanje broj 18 (slika 38) odnosilo se na preferencije metoda identifikacije na internetu. Ponuđeni odgovori su vidljivi na legendi na desnoj strani slike br 39. 63% ispitanika smatra kombinaciju biometrijske tehnologije zajedno sa metodom korisničkog imena i lozinke najboljom metodom za identifikaciju na internetu. Možda zanimljiviji podatak od toga jest taj da gotovo četvrtina ispitanih ostaje vjerna metodi korisničkog imena i lozinke bez upotrebe biometrijskih tehnologija. U američkom istraživanju od prije nekoliko godina, na pitanje o preferencijama metoda autentikacije čak 58% ispitanika odgovorilo je kako preferira koristiti samo korisničko ime i lozinku, bez biometrije.

Slika 39: Pitanje 19

Devetnaesto pitanje (slika 39) odnosilo se na percepciju ispitanika o uzimanju otiska prsta, gdje su ponuđene dvije varijante odgovora. Čak 80% ljudi smatra da uzimanje otiska prsta pomaže zaštiti od prijevara, a samo 3,9% smatra takvu aktivnost tretiranjem ljudi kao da su kriminalci, dok je više od 15% ostalo neodlučno. U prethodnim istraživanjima iz SAD-a, 77% ispitanika se složilo sa prvom tvrdnjom, ali čak 20% je smatralo da je uzimanje otiska tretiranje ljudi kao da su kriminalci, dok 4% nije znalo koji bi odgovor odabrali. Distribucija pozitivnih odgovora je gotovo jednaka, dok se promatranjem preostala dva odgovora može zaključiti da su Amerikanci odlučniji.



Slika 40: Pitanje 20 (a)



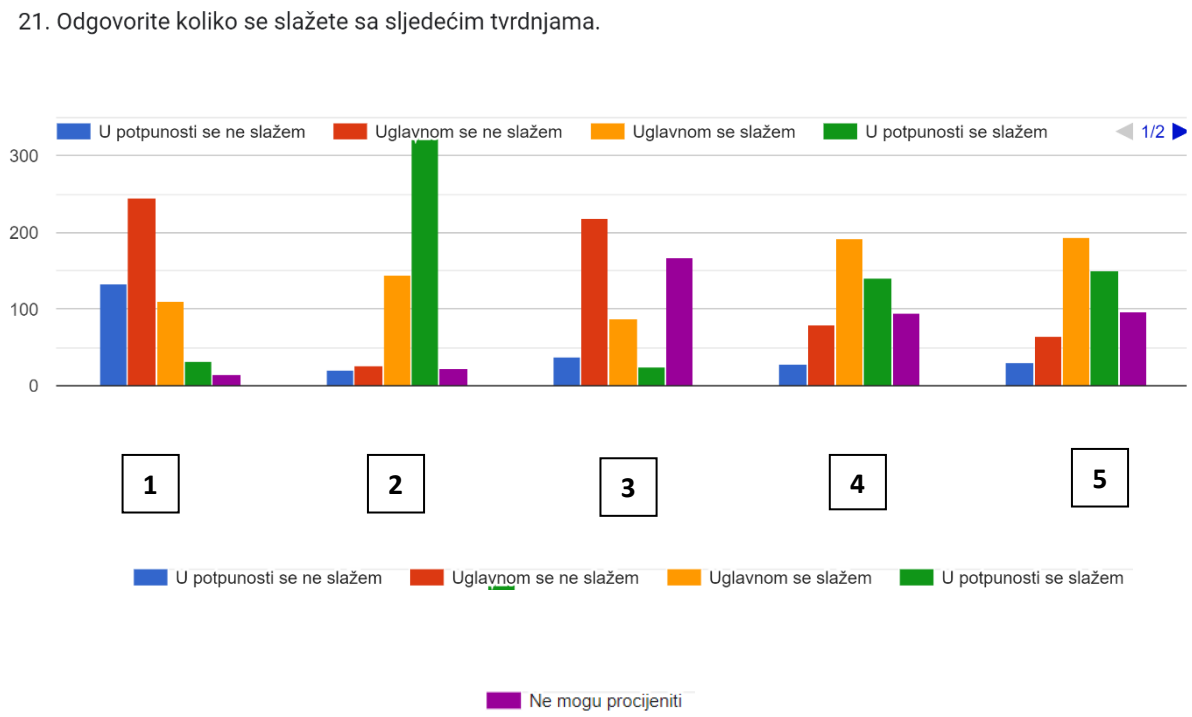
Slika 41: Pitanje 20 (b)

Dvadeseto pitanje (slike 40 i 41) ponudilo je određene lokacije na kojima bi se mogla uvesti biometrijska kontrola protoka ljudi, a od ispitanika se tražilo da označe u kojoj mjeri smatraju prihvatljivim da se takva kontrola uvede na pojedinim mjestima. Ističe se velika prihvatljivost uvođenja biometrijskih kontrola na lokacijama koje zahtijevaju veću razinu sigurnosti, kao što su to zračne luke, granični prijelazi, banke te državne službe. Najmanje 68% ispitanika smatra uvođenje biometrijskih kontrola uglavnom ili potpuno prihvatljivim na tim lokacijama, a za zračne luke se taj postotak penje na gotovo 80%, slično kao i kod graničnih prijelaza. S druge strane, lokacije namijenjene društvenim aktivnostima bez nekog predznaka visoke razine sigurnosti nisu prepoznate kao potrebite za uvođenje biometrijskih kontrola (sportski događaji i hoteli).

Posljednja dva pitanja (slike 42 i 43) odnosila su se na stavove ispitanika s obzirom na određene tvrdnje. Ispitanici su trebali odgovoriti u kojoj mjeri se slažu ili ne slažu za ponuđenim tvrdnjama. Tvrdnje su zbog preglednosti napisane ispod slike 42 odnosno 43, a rezultati su prikazani na grafičkom prikazu. Gotovo 70% ispitanih se uglavnom ili u potpunosti ne slaže sa tvrdnjom da je društvena svijest o važnosti sigurnosti podataka na internetu na dovoljno visokoj razini. S obzirom na ovakve rezultate, potrebno je informiranje javnosti o temi sigurnosti podataka na internetu kako bi se društvena svijest podigla na višu razinu. Čak 87% ispitanika slaže se da su krađe identiteta ozbiljan problem današnjice. Gotovo 43% ispitanih uglavnom se ne slaže sa tvrdnjom da je biometrijske sustave lako prevariti, dok skoro 30% ispitanih ne može procijeniti jeli biometrijske sustave lako prevariti. To ukazuje na postojeću nesigurnost i nepoznavanje biometrijske tehnologije što podrazumijeva potrebu za objektivnim informiranjem, ali isto tako i promišljenost ispitanika koji vjerojatno ne žele glasati za ili protiv nečega što dovoljno ne poznaju. U prilog tome ide i visok postotak ispitanika koji nisu mogli procijeniti je li biometrijska tehnologija bolja opcija od korištenja korisničkog imena i lozinke. Ipak, gotovo 60% ispitanika slaže se da je biometrijska tehnologija bolja solucija za to pitanje. 65% ispitanika smatra da će uvođenje biometrijske tehnologije generalno povećati razinu

informacijske sigurnosti. Gotovo 18% ispitanika ni za ovu tvrdnju nisu mogli definirati svoj osobni stav, što je još jedan pokazatelj potrebe za informiranjem javnosti o biometrijskoj tehnologiji i principima informacijske sigurnosti.

78% ispitanika smatra da će tijekom sljedećih 10 godina biometrijska tehnologija uvelike zamijeniti dosadašnje metode identifikacije. U gotovo jednakim omjerima ispitanici smatraju odnosno ne smatraju biometrijsku tehnologiju kontroverznom. 37% je onih koji su skloniji reći da ona jest kontroverzna, dok 41% smatra da nije kontroverzna. U sličnim omjerima ispitanici su odgovorili na tvrdnju da im uzimanje biometrijskih podataka zvuči pomalo zastrašujuće.



Slika 42: Pitanje 21

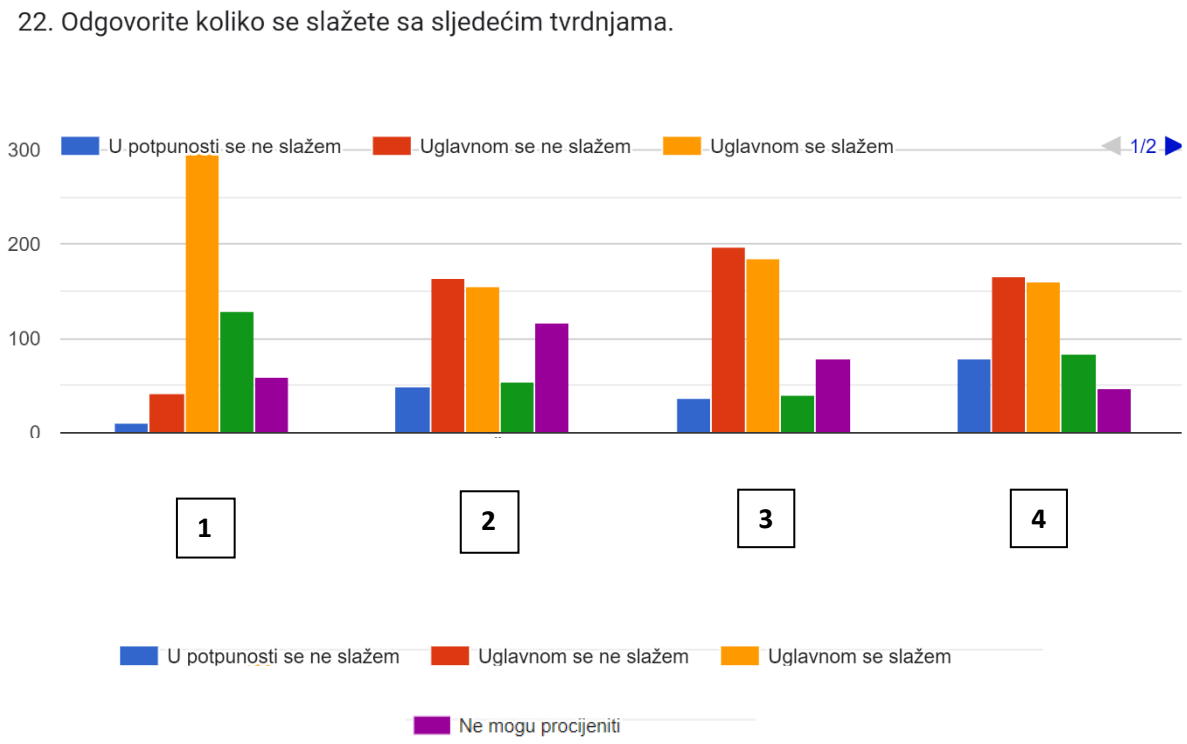
1: Društvena svijest o važnosti sigurnosti podataka na internetu je na dovoljno visokoj razini.

2: Krađe identiteta predstavljaju ozbiljan problem današnjice.

3: Biometrijske sustave je lako prevariti.

4: Biometrijska tehnologija je bolja opcija od korištenja korisničkog imena i lozinke.

5: Uvođenje biometrijskih tehnologija generalno će povećati razinu informacijske sigurnosti



Slika 43: Pitanje 22

1: Tijekom sljedećih 10 godina biometrijska tehnologija će uvelike zamijeniti ostale metode identifikacije

2: Biometrijska tehnologija je zapravo kontroverzna.

3: Širu uporabu biometrijske tehnologije društvo će lako prihvatiti.

4: Uzimanje biometrijskih podataka mi zvuči pomalo zastrašujuće.

5.3. Zaključak istraživanja

Istraživanje provedeno na uzorku od 203 ispitanika pokazuje visoku razinu poznavanja biometrije kod mladih, iako se primjećuje kako postoji određen postotak ispitanika koji ej svjestan biometrije u praksi, ali ga kognitivno ne povezuje sa pojmom „biometrija“ radi slabe informiranosti. Velika većina (preko 86%) ispitanika već se susrelo sa biometrijskom tehnologijom, a najpoznatije metode su prepoznavanje otiska prsta, očne šarenice, lica i glasa. Po iskustvu sa metodama ističu se otisak prsta i prepoznavanje lica. Otisak prsta ujedno je i

metoda koju društvo najlakše prihvaća i u koju ima najviše povjerenja. Sumiranje svih rezultata ankete dovodi do zaključka kako u društvu postoji određena razina skeptičnosti ili opreza prema biometrijskoj tehnologiji, ali ipak joj se ukazuje dovoljno povjerenja da bismo je mogli vidjeti široko prihvaćenu u nekoj budućnosti, ako bi se pitalo naše ispitanike. U svakom slučaju, daljnje informiranje i educiranje društva o sigurnosti na internetu i o biometrijskim tehnologijama izrazito je potrebno.

6. Zaključak

Jedan od najbrže rastućih, ako ne i najbrže rastući gospodarski sektor u suvremenim ekonomijama jest sektor informacijskih tehnologija ili kraće, IT sektor. Sastavni dio tog rastućeg sektora jest i grana informacijske sigurnosti koja se svakodnevno susreće sa novim izazovima. Također, ona bi danas trebala biti integralni dio svake ozbiljne poslovne organizacije. No, informacijska sigurnost ne tiče se samo puke teorije, znanosti ili poslovanja, već svakog pojedinca koji se služi internetom. Ovaj rad osvrnuo se na razvoj informacijske sigurnosti i ukratko teoretski prikazao neke od njenih koncepata. Kako je i sam naslov sugerirao, jedan od koncepata informacijske sigurnosti odnosi se na metode autentikacije korisnika odnosno kontrole pristupa. Metode autentikacije postoje u nekoliko varijanti, a sve sa ciljem da pristup podacima ograniči samo na one korisnike koji na njih imaju pravo. To ograničavanje provodi se na način da korisnik dokaže sustavu kako je baš on taj koji ima pravo pristupiti podacima, a to dokazuje uz pomoć nečega što zna, nečega što posjeduje ili nečega što jest. Pritom se, naime, misli na lozinke, tokene, kartice ili biometrijske značajke koje pojedinac posjeduje. Sustavi temeljeni na lozinkama najšire su rasprostranjeni, no zbog svojih manjkavosti znanost je razvila naprednije metode koje nazivamo biometrijskim metodama, iako se ni one nisu pokazale savršenima. Upravo su biometrijske metode ušle u fokus ovog rada kao potencijalni „game-changer“ u svijetu informacijske sigurnosti. Biometrijske se tehnologije ne koriste samo u svrhu kontrole pristupa određenim podacima, već i kao jednostavnija metoda identifikacije pojedinca na mjestima gdje je identifikacija potrebna. Proučivši biometrijske metode kroz teoriju, rad se fokusirao na istraživanje percepcije biometrijskih tehnologija među mladima. Iz istraživanja se može zaključiti kako postoji generalno pozitivan stav prema biometriji i povjerenje u njenu pouzdanost, ali se ipak u jednoj manjoj mjeri može osjetiti i skeptičnost prema širem i sveobuhvatnijem implementiranju biometrijskih tehnologija, barem kod određenih situacija. Na kraju, sa sigurnošću se može zaključiti da će biometrija biti još dugo predmetom istraživanja i realno je očekivati njenu širu primjenu u društvu.

Popis literature

1. Abidin Z.Z. (2021.), *Swarm intelligence for iris recognition*, 1. izdanje Amsterdam University Press

2. Arbanas, K., Spremic, M., i Zajdela Hrustek, N. (2021.), Holistic framework for evaluating and improving information security culture, *Aslib Journal of Information Management*, *73*(5), 699–719.

3. Ayyagari, R., Lim, J., i Hoxha, O. (2019.), Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers, *Contemporary Management Research*, *15*(4), 227–245. https://doi.org/10.7903/cmr.19394

4. Assignmenthelp (b.d.), Identity and access management part 2, preuzeto 13. rujna 2022. s https://www.assignmenthelp.net/identity-and-access-management-part-2

5. Bahgat, G., Khalil, A., Abdel Kader, N., i Mashali, S. (2013.), Fast and accurate algorithm for core point detection in fingerprint images, *Egyptian Informatics Journal*, *14*(1), 15–25. https://doi.org/10.1016/j.eij.2013.01.002

6. Biometric solutions (b.d.), Keystroke dynamics, preuzeto 13. rujna 2022. s https://www.biometric-solutions.com/keystroke-dynamics.html

7. Bishop, T. (2020.), Our first-hand experience with Amazon's new palm reader, and what it says about the future of retail, preuzeto 14. rujna 2022. s https://www.geekwire.com/2020/first-hand-experience-amazons-new-palm-reader-says-future-retail/

8. Brook C., (2019.), The biggest incidents in cybersecurity (in the past 10 years) (Infographic), preuzeto 18. kolovoza 2022. s https://digitalguardian.com/blog/biggest-incidents-cybersecurity-past-10-years-infographic

9. Brook, C. (2020.), What is cyber hygiene? A definition of cyber hygiene, benefits, best practices and more, preuzeto 18. kolovoza 2022. s https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

10. Caballero, H. (2022.), A brief review about biometrics systems in modern context, *International Journal of Advanced Research in Computer Science*, *13*(3), 5–10. https://doi.org/10.26483/ijarcs.v13i3.6829

11. Chapple M. (2020.), *Access Control and Identity Management (Information systems security and assurance)*, 3. izdanje, Burlington, MA: Jones & Bartlett Learning

12. Cleveland clinic (b.d.), Iris, preuzeto 25. kolovoza 2022. s https://my.clevelandclinic.org/health/body/22502-iris

13. El_Rahman, S. A. (2019.), Biometric human recognition system based on ECG, *Multimedia Tools and Applications*, *78*(13), 17555–17572. https://doi.org/10.1007/s11042-019-7152-0

14. Etter, L. P., Ragan, E. J., Campion, R., Martinez, D., i Gill, C. J. (2019.), Ear biometrics for patient identification in global health: a field study to test the effectiveness of an image stabilization device in improving identification accuracy, *BMC Medical Informatics and Decision Making*, *19*(1). https://doi.org/10.1186/s12911-019-0833-9

15. Forcepoint (b.d.), What is Bring your own device (BYOD)?, preuzeto 30. kolovoza 2022. s https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod

16. Furnell, S. i Evangelatos, K. (2007.), Public awareness and perceptions of biometrics, *Computer Fraud &Amp; Security*, *2007*(1), 8–13. https://doi.org/10.1016/s1361-3723(07)70006-4

17. Georgiadou, A., Mouzakitis, S. i Askounis, D. (2021.), Working from home during COVID-19 crisis: a cyber security culture assessment survey, *Security Journal*, *35*(2), 486–505. https://doi.org/10.1057/s41284-021-00286-2

18. German, R.L. i Barber K.S., (2018.), Consumer attitudes toward biometric authentication [e-publikacija], preuzeto s https://identity.utexas.edu/sites/default/files/2020-09/Consumer%20Attitudes%20About%20Biometrics.pdf

19. Hajdarevic, K., Allen, P., i Spremic, M. (2016.), Proactive security metrics for Bring your own device (BYOD) in ISO 27001 supported environments, u: *2016 24th Telecommunications Forum (TELFOR)* (str. 41–44), Beograd: IEEE

20. Hrvatski jezični portal (b.d.), Identifikacija, preuzeto 17. kolovoza 2022. s https://hjp.znanje.hr/index.php?show=search_by_id&id=fVtiWxY%3D&keyword=identifikacija

21. Huth, A., Orlando, M., i Pesante, L. (2012.), Password security, protection, and management, *United States Computer Emergency Readiness Team*

22. Jain, A.K., Ross, A.A. i Nandakumar, K. (2011.*), Introduction to biometrics*, Berlin: Springer

23. Khan, N., i Efthymiou, M. (2021.), The use of biometric technology at airports: The case of customs and border protection (CBP), *International Journal of Information Management Data Insights*, *1*(2), 100049. https://doi.org/10.1016/j.jjimei.2021.100049

24. Kim, H., Han, J., Park, C., i Yi, O. (2020.), Analysis of Vulnerabilities That Can Occur When Generating One-Time Password, *Applied Sciences*, *10*(8), 2961. https://doi.org/10.3390/app10082961

25. Kwon, B. W., Sharma, P. K. i Park, J. H. (2019.), CCTV-Based Multi-Factor Authentication System, *Journal of Information Processing Systems*, *15*(4), 904–919. https://doi.org/10.3745/JIPS.03.0127

26. Lamin, N. Z., Jusoh, W. N. A. W., Zainudin, J. i Samad, H. (2021.), Implementing Student Attendance System Using Fingerprint Biometrics for Kolej Universiti Poly-Tech Mara, u: *IOP Conference Series: Materials Science and Engineering* (vol. 1062), Selangor: IOP Science. https://doi.org/10.1088/1757-899x/1062/1/012037

27. Lee, Y. K. i Jeong, J. (2021.), Securing biometric authentication system using blockchain, *ICT Express*, *7*(3), 322–326. https://doi.org/10.1016/j.icte.2021.08.003

28. Lord, N. (2020.), Uncovering password habits: Are users' password security habits improving? (Infographic), preuzeto 18. kolovoza 2022. s https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic

29. Mayhew, S. (2018.), History of biometrics, preuzeto 18. kolovoza 2022. s https://www.biometricupdate.com/201802/history-of-biometrics-2

30. Mwapasa, M., Gooding, K., Kumwenda, M., Nliwasa, M., Kaswaswa, K., Sambakunsi, R., Parker, M., Bull, S. i Desmond, N. (2020.), "Are we getting the biometric bioethics

right?" – the use of biometrics within the healthcare system in Malawi, *Global Bioethics*, *31*(1), 67–80. https://doi.org/10.1080/11287462.2020.1773063

31. National research council (2010.), *Biometric recognition: challenges and opportunities*, Washington, D.C.: National Academic Press

32. Nec (b.d.), How does voice recognition works, preuzeto 31. kolovoza s https://www.nec.co.nz/market-leadership/publications-media/how-does-voice-recognition-biometrics-work/

33. Ogbuokiri, B. i Agu, M. (2015.), Authentication system using face and fingerprint technologies, *IOSR Journal of computer engineering*, 17(-), 2278-661. 10.9790/0661-17637484

34. ORC International (2002.), Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector [e-publikacija], preuzeto s https://www.search.org/files/pdf/Biometricsurveyfindings.pdf

35. Pagnin, E. i Mitrokotsa, A. (2017.), Privacy-Preserving Biometric Authentication: Challenges and Directions, *Security and Communication Networks*, *2017*, 1–9. https://doi.org/10.1155/2017/7129505

36. Panian Ž., (2001.) Kontrola i revizija informacijskih sustava, Zagreb: Sinergija

37. Pedamkar, P. (2021.), Security technologies, preuzeto 31. kolovoza 2022. s https://www.educba.com/security-technologies/

38. Recfaces (b.d.), History of biometrics, preuzeto 18. kolovoza 2022. s https://recfaces.com/articles/history-of-biometrics

39. Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J. i Yin, Y. (2018.), A Systematic Review of Finger Vein Recognition Techniques, *Information*, *9*(9), 213. https://doi.org/10.3390/info9090213

40. Shahnewaz S., (2015.), Top ten mind blowing advantages of biometric technology, preuzeto 13. rujna 2022. s https://www.m2sys.com/blog/guest-blog-posts/top-ten-mind-blowing-advantages-of-biometric-technology/

41. Shawkat, A., Moslah, A. A., i Hazim, R. (2018.), Biometrics Detection and Recognition Based-on Geometrical Features Extraction, u: *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)* (str. 59-63.), Kut: IEEE

42. Shea S., (2013.), Mandatory access control, preuzeto 17. kolovoza 2022. s https://www.techtarget.com/searchsecurity/definition/mandatory-access-control-MAC

43. Spremić, M. (2017.a), *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet

44. Spremić, M. (2017.b), *Digitalna transformacija poslovanja*, Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet

45. Spremic, M., Turulja, L., Bajgoric, N. (2018.), Two Approaches in Assessing Business Continuity Management Attitudes in the Organizational Context, u: Bajgoric, N. (ur.), *Always-on enterprise information systems for modern organizations (str.* 159-183.), Hershey, PA: IGI Global

46. Spremić, M. i Šimunic, A. (2018.), Cyber security challenges in digital economy, u: *Proceedings of the World Congress on Engineering* (str. 341-346), Hong Kong: International Association of Engineers

47. Statista (b.d.), Share of United Kingdom (UK) business where bringing your own device occurs in 2018, preuzeto 30. kolovoza 2022. s https://www.statista.com/statistics/586550/bring-your-own-device-by-united-kingdom-uk-businesses/#statisticContainer

48. Suša Vugec, D., Spremić, M., i Pejić Bach, M. (2017.), IT governance adoption in banking and insurance sector: Longitudinal case study of cobit use, *International Journal for Quality Research*, *11*(3), 691–716. 10.18421/IJQR11.03-13

49. Szűcs, R. K., Őszi, A., i Kovács, T. (2021.), Mobile Biometrics and their Risks, *Hadmérnök*, *15*(4), 15–27. https://doi.org/10.32567/hm.2020.4.2

50. Thakkar, D. (2022.), Identity goes digital with biometric signature verification, preuzeto 13. rujna 2022. s https://www.bayometric.com/biometric-signature-verification/

51. Topaloglu, N. (2013.), Revised: Fingerprint classification based on gray-level fuzzy clustering co-occurrence matrix, *Energy education science and technology part A: Energy science and research*, 31(-), 1307-1316.

52. Turroni, F. (2012.), *Fingerprint Recognition: Enhancement, Feature Extraction and Automatic Evaluation of Algorithms*, doktorski rad, Universitá di Bologna, Bologna

53. Vincent, J. (2020.), Amazon's palm reading starts at the grocery store, but it could be so much bigger, preuzeto 13. rujna 2022. s https://www.theverge.com/2020/10/1/21496673/amazon-one-palm-reading-vein-recognition-payments-identity-verification

54. Vitale, T. (2019.), Access control: identification, authentication and authorization, preuzeto 31. kolovoza 2022. s https://www.thomasvitale.com/access-control-authentication-authorization/

55. Warren, T. (2020.), Amazon One lets you pay with your palm, preuzeto 13. rujna 2022. s https://www.theverge.com/2020/9/29/21493094/amazon-one-palm-recognition-hand-payments-amazon-go-store

56. Whitman, M.E. i Mattord, H.J. (2017.), *Principles of information security*, 6. izdanje, Boston, MA: Cengage Learning

57. Widodo, C. E., i Adi, K. (2019.), Face geometry as a biometric-based identification system, *Journal of Physics: Conference Series*, *1524*. 10.1088/1742-6596/1524/1/012008

58. Woodford, C. (2022.), Biometric fingerprint scanners, preuzeto 25. kolovoza 2022. s https://www.explainthatstuff.com/fingerprintscanners.html

59. Yang, W., Wang, S., Hu, J., Zheng, G. i Valli, C. (2019.), Security and Accuracy of Fingerprint-Based Biometrics: A Review, *Symmetry*, *11*(2), 141. https://doi.org/10.3390/sym11020141

60. Ye, H., Pei, R., Mo, Z., Zheng, Q. i Chen, H. (2020.), Comparison on the security of biometrics, u: *Journal of Physics Conference Series* (vol. 1067), Jinan: IOP Science https://doi.org/10.1088/1742-6596/1607/1/012120

Popis slika

Životopis

Stjepan Nađ rođen je 4. lipnja 1997. godine u Zagrebu. Osnovnu školu pohađao je u OŠ Ante Kovačića u Španskom. Nakon toga upisuje srednju Hotelijersko-turističku školu u Zagrebu u kojoj se upoznaje s ekonomskim predmetima i s nekoliko stranih jezika. Kroz srednjoškolsko obrazovanje odrađuje stručnu praksu u turističkim djelatnostima gdje stječe prvo radno iskustvo. Srednju školu završava 2016. godine nakon čega upisuje Ekonomski fakultet u Zagrebu gdje studira na integriranom studiju poslovne ekonomije. Iste godine, paralelno sa ekonomskim fakultetom, pohađa i teološko obrazovanje na Biblijskom institutu u Zagrebu. 2019. godine počinje biti zaposlen kao student u sportskoj trgovini. Iste godine upisuje diplomski studij menadžerske informatike na Ekonomskom fakultetu u Zagrebu. Tijekom diplomskog studija radio je i u IT sektoru. Nakon dvije godine diplomskog studija upisuje apsolventsku akademsku godinu 2021./2022. tijekom koje se počinje baviti suđenjem rukometnih utakmica, a u proljeće 2022. odlazi na dragovoljno vojno osposobljavanje u vojarnu 123. brigade u Požegi te stječe status pričuvnog vojnika Oružanih snaga RH. Iste se godine posvećuje i pisanju diplomskog rada na temu metoda autentikacije i biometrijske tehnologije. Osobito voli prirodu i sport, a karakterizira ga kompetitivnost, prilagodljivost i spremnost na suočavanje s novim izazovima.