Percepcija i stavovi studenata prema biometrijskoj tehnologiji

Szombathelyi, Donata

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:142:927318

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Dvopredmetni diplomski studij nakladništva i informacijskih tehnologija

Donata Szombathelyi

Percepcija i stavovi studenata prema biometrijskoj tehnologiji

Diplomski rad

Mentorica: izv. prof. dr. sc. Anita Papić

Osijek, 2023.

Sveučilište J. J. Strossmayer u Osijeku

Filozofski fakultet Osijek

Odsjek za informacijske znanosti

Dvopredmetni diplomski studij nakladništva i informacijskih tehnologija

Donata Szombathelyi

Percepcija i stavovi studenata prema biometrijskoj tehnologiji[1]

Diplomski rad

Područje: društvene znanosti; Polje: informacijske i komunikacijske znanosti; Grana: informacijski sustavi i informatologija

Mentorica: izv. prof. dr. sc. Anita Papić

[1] Na temelju istraživanja u sklopu ovog diplomskog rada objavljen je rad na konferenciji Edulearn 2023 u koautorstvu mentorice i studentice uz napomenu da se obrana rada trebala održati u srpnju no održana je u listopadu 2023.

Osijek, 2023.

Prilog: Izjava o akademskoj čestitosti i o suglasnosti za javno objavljivanje

Obveza je studenta da donju Izjavu vlastoručno potpiše i umetne kao treću stranicu završnog odnosno diplomskog rada.

IZJAVA

Izjavljujem s punom materijalnom i moralnom odgovornošću da sam ovaj rad samostalno napravio te da u njemu nema kopiranih ili prepisanih dijelova teksta tuđih radova, a da nisu označeni kao citati s napisanim izvorom odakle su preneseni.
Svojim vlastoručnim potpisom potvrđujem da sam suglasan da Filozofski fakultet Osijek trajno pohrani i javno objavi ovaj moj rad u internetskoj bazi završnih i diplomskih radova knjižnice Filozofskog fakulteta Osijek, knjižnice Sveučilišta Josipa Jurja Strossmayera u Osijeku i Nacionalne i sveučilišne knjižnice u Zagrebu.

U Osijeku, 24.9.2023

Dovatz, 0122225600

Ime i prezime studenta, JMBAG

SAŽETAK

U radu se opisuje biometrija - njezine definicije, važnost te kratki povijesni pregled, od drevnog Egipta pa sve do danas. Nakon toga slijedi opis procesa funkcioniranja biometrijskih sustava. Navode se postojeći trendovi biometrijskih tehnologija kao i ograničenja te opasnosti s kojima su brojni korisnici suočeni, a potom se navode i provedena istraživanja u svijetu. Cilj ovog rada je utvrditi u kojoj mjeri je studentska populacija upoznata s pojmom biometrije, biometrijskim sustavima i tehnologijama, mogućim izazovima te kakve stavove i percepcije imaju po pitanju sigurnosti tih sustava kao i prema korištenju biometrijske tehnologije. Kako bi se dobili odgovori na ova istraživačka pitanja, provedeno je empirijsko istraživanje među studentima Filozofskog fakulteta u Osijeku, Ekonomskog fakulteta u Osijeku, Fakulteta elektrotehnike, računarstva i informacijskih tehnologija, Filozofskog fakulteta u Zagrebu, Filozofskog fakulteta u Zadru teFilozofskog fakulteta Sveučilišta u Mostaru. Rezultati istraživanja su pokazali da studenti kao biometrijsku karakteristiku najviše koriste otisak prsta na mobilnom telefonu. Lakoća i lagodnost korištenja izdvajaju se kao dvije vodeće prednosti biometrijske tehnologije od strane studenata dok se kao nedostatak izdvaja sigurnost osobnih biometrijskih podataka. Svijest o postojećim izazovima biometrijskih tehnologija je vidljiva kod studenata, a kao najveći izazov izdvaja se neovlašteno korištenje fotografije korisnika.

Ključne riječi: biometrija, studenti, tehnologija

SADRŽAJ

1. UVOD

Cilj ovog rada je utvrditi u kojoj mjeri je studentska populacija upoznata s pojmom biometrije, biometrijskim sustavima i tehnologijama, mogućim izazovima te kakve stavove i percepcije imaju po pitanju sigurnosti tih sustava kao i prema korištenju biometrijske tehnologije.

U drugom poglavlju govori se o biometriji općenito, definiraju se esencijalni koncepti vezani uz biometriju te povijesni razvoj te se ukratko opisuju najvažnije povijesne činjenice koje su utrle put pravom razvoju današnje biometrije.

U trećem poglavlju govori se najprije o postojećim biometrijskim metodama, a zatim o biometrijskim sustavima, kako fiziološkim tako i bihevioralnim. Također, navedene su i objašnjene suštinske funkcionalnosti kao što su verifikacija i identifikacije korisnika. Naposljetku, opisuju se primjeri fizioloških biometrijskih sustava (prepoznavanje otiska prsta, šarenice oka, mrežnice oka, uha, lica, termograma lica, vene i DNK) te primjeri bihevioralnih biometrijskih sustava (prepoznavanje glasa, potpisa, mirisa, hoda i prepoznavanje na temelju udarca tipke na tipkovnici).

U četvrtom poglavlju navode se izazovi biometrijske tehnologije, a u petom poglavlju trendovi u razvoju biometrijske tehnologije. Opisani su najvažniji trendovi poput multimodalne autentifikacije korisnika, autentifikacije korisnika bez lozinke, snažnije integracije oblaka, kvantne biometrije te naposljetku biometrije u metaverzumu.

Pregled literature o dosadašnjim istraživanjima u svijetu i kod nas opisuje se u šestom poglavlju. Ovdje se opisuju prije svega već postojeća istraživanja u svijetu - počevši od Njemačke, nakon koje slijedi Grčka, zatim SAD, Indija, Australija, Španjolska te Finska i Brazil. Nakon istraživanja provedenih u svijetu, opisano je ukratko stanje, odnosno jedno provedeno istraživanje u Republici Hrvatskoj.

Empirijski dio rada vezan uz istraživanje percepcije i stavova studenata o biometrijskim tehnologijama predstavljen je u sedmom poglavlju nakon čega slijedi rasprava i zaključak.

2. BIOMETRIJA

2.1. O biometriji općenito

Prema Centru za informacijsku sigurnost biometrija dolazi od grčke riječi *bios*, što označava život, dok riječ *metron* označava mjeru te se može definirati kao skup određenih automatiziranih metoda čija je svrha jedinstveno prepoznavanje ljudi, temeljeno na samo jednoj ili pak većem broju njihovih fizičkih i ponašajnih obilježja.[1] Takva obilježja nisu ništa drugo nego biometrijski podaci, a kad je riječ o najvažnijoj vrsti, to je onda DNK podatak, iza kojeg slijede otisak prsta, mrežnica oka i primjerice struktura lica. Pojam biometrije naveden u Enciklopediji Britannici upućuje na povezanost s kriminalistikom i forenzikom jer se spomenuti pojam "može koristiti za proučavanje identifikacije osumnjičenika pomoću različitih jedinstvenih bioloških markera."[2] S druge pak strane, Nacionalni Institut za standarde i tehnologiju (National Institute of Standards and Technology) navodi kako je biometrija jednom riječju mjerenje fizioloških karakteristika, kao što je otisak prsta, šarenica oka ili lica koje može pomoći u identifikaciji pojedinca. Poznata računalna tvrtka Kaspersky Lab biometriju definira kao biološka mjerenja za identifikaciju pojedinca.[3] Potreba za sve većim korištenjem biometrijskih podataka danas je prisutna u mnogim područjima znanosti. Biometrija se može podijeliti na dvije vrste - fiziološku i bihevioralnu biometriju. Fiziološka podrazumijeva korištenje fizičke biometrijske karakteristike, te se može odnositi primjerice naprepoznavanje otiska prsta, mrežnice i šarenice oka, lica, DNK itd. S druge strane, bihevioralna biometrija podrazumijeva mjerenje obrazaca ljudskog ponašanja te se može odnositi primjerice na prepoznavanje hoda, glasa, tipkanja na tipkovnici itd. Navedeni primjeri objašnjeni su u drugom poglavlju.

2.2. Povijesni pregled razvoja biometrije

Premda se možda ne doima tako, ali sama biometrija postoji već tisućama godina. Prvi dokazi koji se mogu čak nazvati biometrijskim sustavom datiraju još od 500. g. pr. Kr., odnosno u doba Babilona, gdje su se otisci prstiju koristili kao oznaka osobe te za potrebe poslovnih transakcija na glinenim pločicama.[4] Osim toga, u vrlo ranoj egipatskoj povijesti, trgovci su bili identificirani premanjihovim fizičkim karakteristikama kako bi se uspjela napraviti razlika između pouzdanih trgovaca

[1] Usp. Biometrija. URL: https://www.cis.hr/www.edicija/Biometrija.html (2022-12-17)
[2] Usp. Biometrics. Enciklopedia Britannica. URL: https://www.britannica.com/science/biometrics (2023-01-04)
[3] Usp. What is Biometrics? How is it used in security?. URL: https://www.kaspersky.com/resource-center/definitions/biometrics (2023-01-04)
[4] Usp. History of Biometrics | Biometric Update. URL: https://www.biometricupdate.com/201802/history-of-biometrics-2 (2022-12-18)

poznate reputacije i prethodnih uspješnih transakcija te onih novih koji se pojave na tržištu.[5] Stoljećima kasnije, u Bologni 1686. godine profesor Marcello Malpighi zabilježio je također jednu vrstu biometrijskog sustava, a to su grebeni i spirale. S druge pak strane, godine 1788. njemački liječnik J. C. A. Mayer napisao je djelo "Anatomske bakrene ploče s prikladnim objašnjenjima",koje su sadržavale crteže kožnih uzoraka tarnih grebena, napominjući kako je tarna koža grebena jedinstvena.[6] Sve do sredine 19. stoljeća, zahvaljujući urbanizaciji i napretku industrijske revolucije, jednostavno je jačala potreba za popisivanjem i identifikacijom ljudi, osobito kod trgovaca. Tako je 1858. godine zabilježeno prvo sustavno snimanje slika ruku, dok je 1870. godine započeo razvoj antropometrije, znanosti koja sustavno mjeri i bilježi mjerenje ljudskog tijela.[7] Razvivši se u 19. stoljeću, antropometriju su koristili antropolozi za proučavanje ljudskih varijacija i evolucije kako u živim, tako i u izumrlim populacijama. Drugim riječima, antropometrijska mjerenja kroz povijest koristila su se kao sredstvo za povezivanje ne samo rasnih, već kulturnih i psiholoških atributa s fizičkim svojstvima.[8] Prema tome, antropomorfna mjerenja uključuju veličinu kao što je primjerice visina, težina, površina, volumen, struktura i sl. Najveće zasluge antropometrije pripadaju Iphonesu Bertillonu, liječniku i ujedno osnivaču pariškog antropološkog društva, kojeg mnogi nazivaju i ocem antropometrije jer je razvio sustav klasifikacije, poznatiji kao antropometrijski sustav. Radeći u pariškoj policiji, Bertillon je prepoznao problem koji se vrlo često ponavljao, a to je teža identifikacija prijestupnika.[9] Ondašnji kazneni dosjei bili su pohranjeni i poredani abecednim redom te su kriminalci često smišljali pseudonime kako bi prevarili sustav i time izbjegli kazne. Bertillon se vodio pretpostavkom da je gustoća kostiju fiksna nakon dobi od 20 godina, a ljudske dimenzije intrinzično vrlo varijabilne.[10] Morfološke karakteristike koje se koriste u ovoj klasifikaciji jesu visina, širina, veličina stopala, širina i duljina glave i sl. Na taj se način identificirana osobaklasificira kao mala, srednja ili velika te su se uz to dodavale i fotografije osobe - frontalna i profilna.[11] Korištenje ovog antropometrijskog sustava kasnije je nazvano "*Bertillonage*" koje sebrzo proširilo svijetom tijekom kasnih 1800-ih i ranih 1900-ih godina. Međutim, 1903. godine zaključilo se kako je ovaj sustav klasifikacije neadekvatan iz razloga što su osuđeni kriminalci, jednojajčani blizanci, imali iste mjere prema Bertillonom sustavu.[12] S vremenom su se znanstvenici sve manje oslanjali na ovu vrstu tradicionalne tehnike identifikacije prijestupnika, tako da se

[5] Isto.
[6] Isto.
[7] Isto.
[8] Usp. Anthropometry - Definition, History and Applications | Biology Dictionary. URL: https://biologydictionary.net/anthropometry/ (2022-12-30)
[9] Isto.
[10] Isto.
[11] Isto.
[12] Isto.

proučavanje dimenzija ljudskog tijela, razvoj biometrije i njezinih tehnologija polako odvijao u nešto drugačijem smjeru. Danas se svi spomenuti postupci mogu učinkovitije provesti pomoću trodimenzionalnih skenera tijela, koji mogu pružiti dostatan broj antropometrijskih podataka nego neke određene konvencionalne tehnike.[13] Prema tome, za identifikaciju se počinju koristiti druge morfološke karakteristike, kao što je šarenica oka, koju predlaže oftalmolog Frank Burch 1936. godine. Daljnjim razvojem i proučavanjem biometrijskih sustava, u praksi se sve više počinju implementirati tehnike za prepoznavanje lica. Tako se 1988. godine uveo prvi poluautomatski sustav za prepoznavanje lica, gdje su se koristili kompozitni crteži ili pak video slike osumnjičenih sa svrhom pretraživanja baza podataka digitaliziranih fotografija.[14] Iste godine razvijena je tehnika Eigenface, od strane znanstvenika Kirby i Sitovich, koja primjenjuje u sebi linearnu algebru kod prepoznavanja lica osobe.[15] Eigenface se smatra prekretnicom iz razloga što se pokazalo kako je potrebno puno manje od stotinu vrijednosti za aproksimaciju slike lica.[16] Nadalje, 1992. godine osnovan je Biometrijski konzorcij u Sjedinjenim Američkim Državama koji je brzo pridobio članice s ciljem uključivanja i širenja zajednice, a uloga mu je stvaranje ključne veze i rasprava između Vlade i akademskih zajednica. Eksplozijom biometrijskih aktivnosti u ranim 2000-im godinama, brojne aktivnosti integrirane su u neke druge organizacije kao što su INCITS (International Committee for Information Technology Standards), ISO (International Standardization forStandardization) i NSTC (National Science and Technology Center). Također, od 2008. godine počelo se raditi na novoj generaciji biometrijskih baza podataka, koje uključuju podatke o šarenici, dlanu, licu te o otiscima prstiju[17], a od 2013. godine tvrtka Apple počinje implementirati elektroničke otiske prstiju (eng. “touch ID”) u pametne telefone. Krenuvši od verzije iPhone 6S funkcionalnost otključavanja zaslona, kao i kupnje na App store-u, touch ID postao je značajka gotovo svih mobilnih uređaja današnjice, kako Android tako i iOS mobilnih uređaja.

[13] Usp. Current state of the art and enduring issues in anthropometric data collection. URL: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532016000300003 (2023-02-06)
[14] Isto.
[15] Isto.
[16] Isto.
[17] Isto.

3. BIOMETRIJSKI SUSTAVI

Sustav dolazi od grčke riječi *sistem*, što označava udruživanje i cjelinu te se može definirati kao skup određenih elemenata koji su povezani u jednu funkcionalnu cjelinu - primjerice Sunčev sustav, koordinatni sustav, dišni ili krvožilni sustav i sl.[18] Prema tome, biometrijski sustav bi zato podrazumijevao organizirani skup morfoloških karakteristika (biometrijskih podataka) pojedinca koji se koriste s određenom svrhom. Svaki biometrijski sustav ima određene komponente, čiji broj varira od sustava do sustava, no najčešće je to funkcionalna kombinacija pet komponenti.

Funkcioniranje se odvija uz pomoć pet komponenti, odnosno pet faza[19]:

Faza 1 - Prikupljanje podataka (prepoznavanje i upis korisnika)

Prva faza sastoji od dvije sporedne faze, dakle upisa i tzv. priznavanja korisnika. Tijekom faze upisa, biometrijski podaci prikupljaju se od korisnika putem senzora te se prezentiraju i potom pohranjuju u bazu podataka zajedno s njegovim identitetom.[20] Karakteristično je da se prikupljeni biometrijski podaci korisnika obrađuju kako bi se mogle izdvojiti one istaknute i specifične značajke. Vrlo je čest slučaj da se izdvojeni (ekstrahirani) biometrijski podaci obrađuju, dok se oni neobrađeni jednostavno odbacuju. Kod faze prepoznavanja, biometrijski podaci ponovno se prikupljaju od pojedinca i zatim uspoređuju s pohranjenim podacima.[21]

Faza 2 - Obrada signala (rad senzora i izdvajanje značajki)

Rad senzora zahtjeva standardizirano i intuitivno korisničko sučelje. Kao i za svaki drugi dio softvera, dobar dizajn korisničkog sučelja ključ je uspješne implementacije svakog biometrijskog sustava. Ako se primjerice radi o optičkom senzoru za otisak prsta, potrebno je stvoriti što bolje ergonomsko sučelje kako bi korisnik jednostavno mogao unijeti svoj uzorak dobre kvalitete u biometrijski sustav.[22] Sama kvaliteta biometrijskih uzoraka (podataka) ovisi o aspektima senzorakoji se koristi. U većini slučajeva svi neobrađeni biometrijski podaci postanu dvodimenzionalna slika (npr. šarenica oka), no postoje i iznimke. Iznimke mogu biti glasovi prikazani kao amplituda, miris ili čak DNK korisnika.[23] Kod svih biometrijskih podataka koji se temelje na slici veliku ulogu igra razlučivost slike, ali i osjetljivost kamere.[24] Osim ovih tehničkih karakteristika koji utječu na

[18] Usp. sustav. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. http://www.enciklopedija.hr/Natuknica.aspx?ID=58904 (2023-01-30)
[19] Usp. Biometric System Architecture - GeeksForGeeks. URL: https://www.geeksforgeeks.org/biometric-system-architecture/ (2023-01-30)
[20] Usp. Jain, Ross, Nandakumar. Introduction to Biometrics. Str. 4.-9.
[21] Isto.
[22] Isto.
[23] Isto.
[24] Isto.

prijenos biometrijskih podataka, valja uzeti u obzir i čimbenike poput cijene, veličine i trajnosti koji također utječu na dizajn i rad samog senzora.[25] .

Faza izdvajanja značajki je najsloženija. Ovdje se neobrađeni biometrijski podaci sa senzora moraju podvrgnuti određenim operacijama obrade prije nego što započne proces izdvajanja značajki. Postoje tri uobičajeno korištena koraka obrade, a to su *procjena kvalitete, segmentacija i poboljšanje*.[26] Kako bi se uspjela utvrditi prikladnost daljnje obrade, potrebno je najprije pristupiti kvaliteti dobivenog biometrijskog podatka.[27] S obzirom da je kvaliteta ključ svega, biometrijski sustavi reagiraju na način da pokušaju ponovno nabaviti korisnikov podatak ili pokrenuti iznimku. Pokretanje iznimke odnosi se na prikazivanje alarma, gdje se aktiviraju pripadajući alternativni postupci kao što je ručna intervencija sustava.[28] Segmentacija kao drugi postupak obrade odvaja sve potrebne biometrijske podatke od tzv. pozadine, a dobar primjer može biti prepoznavanje lica naslici koja ima puno predmeta iza korisnika. Nakon što se biometrijski podaci segmentiraju, moraju se podvrgnuti algoritmu za poboljšanje kvalitete signala.[29] Za razliku od toga, slikovni podaci mogu npr. primijeniti algoritam poboljšanja, kao što je izjednačavanje histograma i to podrazumijeva treći postupak obrade.[30] Shodno tome, cjelokupni proces izdvajanja značajki zapravo podrazumijeva proces generiranja izražajnog i kompaktnog digitalnog prikaza - predloška. Nastali predložak trebao bi sadržavati samo one najvažnije dijelove sitnih točaka kako bi se korisnik mogao identificirati.[31] Prilikom upisa, svaki predložak pohranjuje se ili u središnju bazu podataka biometrijskog sustava ili se bilježi na tokenu (npr. pametnoj kartici) koji se izdaje korisniku, ovisno o biometrijskom softveru.[32] U trenutku prepoznavanja, predložak se mora dohvatiti iz baze podataka i zatim usporediti sa skupom značajki koji su izvedeni iz novog biometrijskog podatka dobivenog odkorisnika.[33] Spomenuti skup značajki naziva se upit ili unos i važno je istaknuti kako se predložak može izdvojiti iz samo jednog biometrijskog podatka ili generirati obradom više njih, koji suprikupljeni tijekom upisivanja.[34] Danas biometrijski sustavi često pohranjuju više predložaka kako bi se uzelo u obzir više varijacija istog podatka. Tako primjerice, sustavi za prepoznavanje lica uglavnom mogu pohraniti više predložaka korisnika jer svaki predložak označava drugačiju pozulica u odnosu na kameru koja bilježi.[35]

---

[25] Isto.
[26] Isto.
[27] Isto.
[28] Isto.
[29] Isto.
[30] Isto.
[31] Isto.
[32] Isto.
[33] Isto.
[34] Isto.
[35] Isto.

Faza 3 - Pohrana podataka u bazi

Zadaća baze podataka biometrijskog sustava je biti spremište svih biometrijskih podataka. Završetkom procesa upisa, skup značajki koji se izdvaja iz neobrađenog predloška treba se pohraniti u bazu zajedno s određenim informacijama korisnika, kao što su ime ili OIB, a jedinstveni su za svakoga. Također, da bi cjelokupni proces dobro funkcionirao, važno je odlučiti kakav će se tip bazekoristiti - centralizirani i decentralizirani. Centralizirana baza podataka (slika) nalazi se, pohranjuje iodržava na samo jednom mjestu te se njome upravlja upravo sa tog jednog mjesta.[36] To podrazumijeva da se bazi pristupa putem internetske veze kao što je npr. LAN ili WAN, a mogu je koristiti institucije ili velike organizacije. S druge pak strane, decentralizirana baza podataka dijeli radno opterećenje između više sustava te koristi sofisticirane algoritme za balansiranje dolaznih i odlaznih zahtjeva klijenata, odnosno korisnika.[37] Ova vrsta baze podataka korisna je u situacijama kada postoji više podataka koje je potrebno pohraniti nego što se može fizički spremiti na jednom fizičkom računalu.

Faza 4 - Usporedba

Sam cilj biometrijskog podudaranja (eng. *biometric matching*) jest usporedba značajki upita s pohranjenim predlošcima kako bi se uspjeli generirati rezultati podudaranja, a dobiveni rezultat je zapravo mjera sličnosti između predloška i upita.[38] Što je veći rezultat podudaranja, to je veća sličnost između predloška i upita. Također, postoji tzv. rezultat udaljenosti, a on ukazuje na mjeru različitosti između dva skupa značajki, pa samim time, manji rezultat podudaranja, treba ukazati na veću sličnost između predloška i upita.[39]

Faza 5 - Odluka

Odluka predstavlja posljednju, petu fazu u funkcioniranju biometrijskog sustava te se ovdje biometrijski podatak kao rezultat koristi kao ulazna točka u proces usporedbe, kako bi se odvila ili verifikacija ili autentifikacija korisnika. Savršen biometrijski sustav trebao bi u pravilu uvijekprikazati dobre odluke, no u stvarnosti to nije lako postići.[40] Odluka je ovisna o nekoliko čimbenika
- ovisno o tome na koji način rade algoritmi u biometrijskim sustavima te ovisi o količini korisnih informacija koje su dostupne u danim uzorcima i koje pomažu karakterizaciji objekata. Primjerice,

[36] Usp. Difference between Centralized Database and Distributed Database - GeeksforGeeks. URL: https://www.geeksforgeeks.org/difference-between-centralized-database-and-distributed-database/ (2023-01-04)
[37] Usp. What is a decentralized database? | VentureBeat. URL: https://venturebeat.com/business/what-is-a-decentralized-database/ (2023-01-04)
[38] Isto.
[39] Isto.
[40] Usp. Understanding Biometric Performance Evaluation. URL: https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf (2023-02-24)

veličina senzora - je li velika ili mala, razlučivost i kvaliteta dobivene slike, preklapanje nekih uzoraka i sl.[41] Kada je riječ o funkcionalnostima biometrijskih sustava, važno je napomenuti da postoje dvije vrste koje se smatraju procesom autentifikacije:[42]

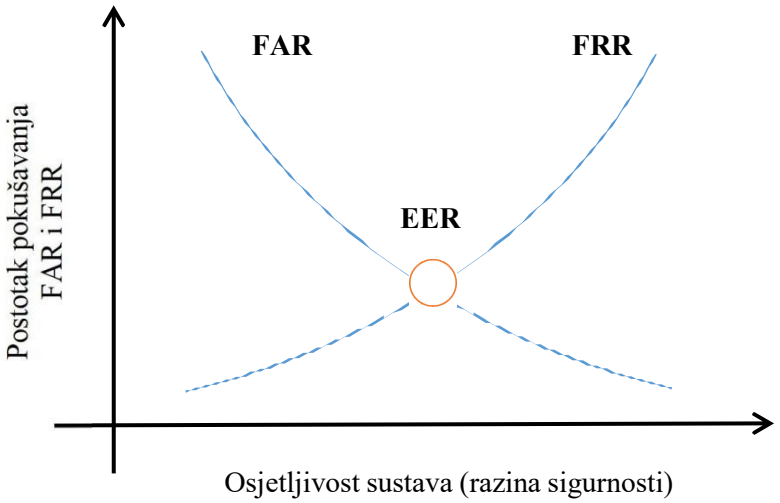
Identifikacija - određivanje identiteta korisnika; odgovara na pitanje koji korisnik se želi prijaviti u postojeći sustav (veza 1:N);

Verifikacija - provjeravanje; odgovara na pitanje jesu li dobiveni podaci povezani s korisnikom koji se prijavljuje (veza 1:1).

Proces identifikacije inače se klasificira na pozitivnu i negativnu. Kad je riječ o pozitivnoj identifikaciji, korisnik se tada pokušava pozitivno identificirati u biometrijski sustav, točnije rečeno, ovo se odnosi na podudaranje jedan naprama više.[43] Za razliku od toga, negativna identifikacija zapravo prikriva svoj pravi identitet pa se često naziva i screening, čiji je cilj dokazati da osoba nije onakva kakva smatra da nije.[44] Dakako, sama svrha negativne identifikacije je ta da se spriječe problemi višestrukih prijava, odnosno spriječiti korisnika da se više puta prijavi pod različitim imenom. Prilikom procesa verifikacije sustav želi provjeriti je li korisnik onaj koji se predstavlja. Ovakav se scenarij uspoređuje samo s onim predloškom koji odgovara tom traženom identitetu, što bi u prijevodu označavalo podudaranje jedan na jedan.[45] Provjera identiteta izvediva je primjerice uz korištenje OIB-a, PIN-a ili primjerice tokena i ako ima zaista visok stupanj sličnosti, onda se korisnikov zahtjev smatra istinitim, u suprotnom se smatra lažnim i takav pristup naziva se neovlaštenim. Što se tiče implementacije biometrijskih sustava, potrebno je proučiti kakva je zapravo točnost biometrijskih sustava. Pri procjeni se koriste tri tehnike - stopa lažnog odbijanja (eng. False Rejection Rate = FRR), stopa lažnog prihvaćanja (eng. False Acception Rate = FAR) te stopa jednake pogreške (eng. Equal Error Rate). S jedne strane, stopa lažnog odbijanja može se dogoditi kada biometrijski sustav odbije ovlaštenog korisnika, točnije rečeno, smatra ga neovlaštenim.[46] Ova stopa pripada grešci tipa I. S druge strane, lažna stopa prihvaćanja pripada greškama tipa I. te se događa kad biometrijski sustav nekog neovlaštenog korisnika prihvati kao ovlaštenog. Jednostavno rečeno radi se o prijevarama. Naposljetku, treća stopa odnosi se na ukupnu

[41] Isto.
[42] Usp. Biometrics Authentication vs Verification - Javatpoint. URL: https://www.javatpoint.com/biometrics-authentication-vs-verification (2023-01-04)
[43] Usp. Jain, Ross, Nandakumar. Nav.dj.
[44] Isto.
[45] Isto.
[46] Usp. Domain 5: Identity and access management (controlling access and managing identity). URL: https://www.sciencedirect.com/science/article/pii/B978012811248900005X (2023-04-30)

točnost biometrijskog sustava, a grafički gledano, ona opisuje točku u kojoj su FAR i FRR jednaki čiji je odnos vidljiv na Grafičkom prikazu 1.



Grafički prikaz 1. Odnos između FAR, FRR i EER[47]

Grafički prikaz 1 prikazuje kako se broj lažnih prihvaćanja (FAR[50]) smanjuje, a broj lažnih odbijanja (FRR[51]) raste i obrnuto.[48] Vidljiva točka u kojoj se linije sijeku odnosi se na jednaku stopa pogreške (EER) te je ovdje postotak lažnih prihvaćanja i lažnih odbijanja isti.[49] Prema tome, stope lažnog prihvaćanja i lažnog odbijanja mogu se izračunati na sljedeći način:

$$FAR = \frac{broj\ lažnih\ prihvaćanja}{broj\ pokušaja\ identifikacije}$$

$$FRR = \frac{broj\ lažnih\ odbijanja}{broj\ pokušaja\ identifikacije}$$

[47] Isto. Str. 122.
[48] Usp. Everything about FAR and FRR | Recogtech. URL: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience (2023-02-24)
[49] Isto.
[50] Isto. Str. 121.
[51] Isto.

Kako bi biometrijski sustavi funkcionirali, postoje određene metode - *kontaktne i beskontaktne, fizičke i ponašajne te meke i tvrde*. Navedeni primjeri bit će daljnje objašnjeni u narednim potpoglavljima. Kontaktne metode zahtijevaju fizički kontakt između korisnika i biometrijskog senzora ili uređaja. Tijekom procesa identifikacije, korisnik mora dodirnuti ili doći u neposrednu blizinu senzora kako bi se prikupili podaci. Primjeri kontaktnih biometrijskih metoda uključuju prepoznavanje otiska prsta, dlana i prepoznavanje geometrije ruke. Nasuprot tome, beskontaktne biometrijske metode ne zahtijevaju fizički kontakt između korisnika i senzora. Ove metode hvataju biometrijske podatke iz daljine bez ikakvog izravnog dodira. Primjeri ovakvih biometrijskih metoda uključuju prepoznavanje lica, šarenice i primjerice glasa. Nadalje, što se tiče fizičkih metoda, one podrazumijevaju urođene fizičke atribute koji su relativno stabilnitijekom cijelog životnog vijeka osobe. To mogu biti otisci prstiju, dlanova, uzorci šarenice, crte lica, geometrija ruke ili pak uzorci vena. Obično se koriste za provjeru identiteta jer ostaju relativno konstantni tijekom vremena. S druge strane, biometrijske karakteristike ponašanja, temelje se na obrascima ponašanja ili radnjama koje izvodi sam korisnik. One se za razliku od fizičkih metoda mogu mijenjati tijekom vremena i na njih utječu čimbenici kao što su stres, raspoloženje i zdravlje korisnika. Primjeri bihevioralnih biometrijskih karakteristika uključuju dinamiku potpisa, dinamiku pritiska tipke, prepoznavanje hoda i prepoznavanje glasa. Povrh toga,čvrste metode koriste se za opisivanje razine razlikovnosti i postojanosti biometrijskih osobina. One su vrlo karakteristične i relativno stabilne tijekom vremena. Primjeri čvrstih biometrijskih karakteristika uključuju otiske prstiju, uzorke šarenice i DNK. Te je značajke teško krivotvoriti ili promijeniti, što ih čini vrijednima za sigurnosne softvere. Za razliku od njih, meke biometrijske karakteristike manje su karakteristične i mogu se mijenjati tijekom vremena. Često se koriste u dodatne ili sekundarne svrhe identifikacije kako bi se povećala točnost biometrijskih sustava. Meke biometrijske značajke uključuju atribute poput dobi, spola, visine, težine i izraza lica. Iako mogu pružiti dodatne informacije, nisu tako pouzdane kao čvrste biometrijske karakteristike za primarnu identifikaciju. Za sve navedeno, izbor metoda ovisi o čimbenicima kao što su praktičnost, higijena i zahtjevi specifičnog softvera.

3.1. Fiziološki biometrijski sustavi

3.1.1 Prepoznavanje otiska prsta

Najčešće korištena biometrijska metoda prepoznavanja jest otisak prsta *(eng. fingerprint)*. Primjeri se odnose na pametne tipkovnice, koje zahtijevaju od korisnika da koristi vlastiti otisak prsta kako bi otključao svoje računalo.[52] Da bi sama autentifikacija mogla uspjeti, podaci koji se očitavaju s otiska prsta moraju biti zaista mali. Takvi podaci su zapravo jedan matematički prikaz, koji opisuju pojedinosti otiska prsta - poput tzv. grebena, bifurkacije, petlje i sl.[53] Da se biometrijski sustavi razvijaju relativno brzo potvrđuje i činjenica da Fingerprint Cards AB I Flywallet, poznate svjetske biometrijske tvrtke, nastoje lansirati što više biometrijskih proizvoda za europsko tržište.[54] Njihovi dobri senzori za otiske prstiju dizajnirani su tako da budu višenamjenski kako bi korisnicima mogli omogućiti korištenje s ciljem poboljšanja kako privatnosti, tako i korisničkog iskustva.[55]

3.1.2 Prepoznavanje šarenice oka

Šarenica oka (eng. iris) podrazumijeva biometrijsku metodu identifikacije. Ona uzima one jedinstvene uzorke koji se nalaze unutar područja, u obliku prstena koji okružuje zjenicu u oku.[56] Njezina povijest je relativno mlada, a započela je 1936. godine nakon što su identificirane razlike između ljudskih šarenica od strane njemačkog oftalmologa Franka Burcha.[57] Skeniranje šarenice se odvija na način da se ljudsko oko osvjetljava infracrvenim svjetlom, a koristi se posebna kamerakoja može snimiti položaj trepavica, kapaka, zjenice i šarenice. Zahvaljujući skenerima, može se prikupiti više od 240 biometrijskih značajki čija je kombinacija jedinstvena za svako oko.[58] Nakon što se biometrijski uzorak snimi, on postaje matematički koji se pohranjuje u bazi podataka.[59] Biometrijski sustav ovakve vrste dosegao je svoj uspon zahvaljujući tehnologiji, koja je ubrzo postala komercijalizirana, a neke od najpoznatijih tvrtki koje se bave proizvodnjom ovakvih sustava jesu BioID, Aware, IriTech, Iris ID itd.[60]

---

[52] Isto.
[53] Isto.
[54] Usp. Fingerprints and Flywallet developing wearable biometric payment & access products for Europe. URL: https://www.fingerprints.com/2023/02/24/fingerprints-and-flywallet-developing-wearable-biometric-payment-access-products-for-europe-2302240800/?utm_source=iseepr&utm_medium=NEWS&utm_campaign=Flywallet (2023-02-24)
[55] Isto.
[56] Usp. Iris Recognition Technology - How it Works. URL: https://www.innovatrics.com/iris-recognition-technology/ (2023-02-24)
[57] Isto.
[58] Usp. Iris Recognition | Electronic Frontier Foundation. URL: https://www.eff.org/pages/iris-recognition (2023-02-25)
[59] Usp. Iris Recognition Technology. Nav.dj.
[60] Isto.

3.1.3 Prepoznavanje mrežnice oka

Prepoznavanje mrežnice oka predstavlja oblik biometrijske identifikacije koja postoji otprilike pedeset godina te se u tom razdoblju ova ovakva vrsta biometrije značajno razvila.[61] No, bez obzira na to, određeni procesi prepoznavanja na neki način su spriječili da mrežnica postane glavni oblik biometrije.[62] Kao prvo, mrežnica se može definirati kao skup krvnih žila koje vode u tzv. disk oka, gdje se vizualne informacije prenose u mozak. Također, postoje i dva različita fotoreceptora unutar mrežnice, a to su štapići i čunjići. Dok čunjići (svako oko sadrži otprilike 6 milijuna) pomažu u raspoznavanju različitih boja, štapići (125 milijuna po oku) olakšavaju noćni i periferni vid.[63] No, ono što se smatra temeljem za prepoznavanje mrežnice jest uzorak krvnih žila. Postupak skeniranja odvija se kao i u drugim biometrijskim sustavima, a sastoji se od tri koraka - prikupljanje i obrada signala, retinalno podudaranje te reprezentacija. Prva faza najviše ovisi o suradnji korisnika i može trajati i do jedne minute što je zapravo prilično dugo jer se snimaju uglavnom tri do pet slika mrežnice, kako bi usporedba u sustavu bila bolja.[64] Druga faza odnosi se na identifikaciju i verifikaciju korisnika, a treća faza na stvaranje predložaka iz jedinstvenih biometrijskih uzoraka. Prepoznavanje mrežnice nije previše korištena metoda biometrije, no kao takvo koristi se u slučajevima kad sigurnost treba biti najveći prioritet.

3.1.4 Prepoznavanje uha

Prepoznavanje uha inače pripada novijim biometrijskim tehnologijama. Za razliku od ljudskog lica, promjene na uhu nisu vidljive jer je boja konstantna na cijelom uhu (na licu šminka ostavlja učinak). Prepoznavanje se sastoji od tri faze - detekcija uha, izdvajanje značajki te klasifikacija biometrijskog uzorka.[65] Prva faza odnosi se na lociranje samog uha, njegovih rubova i spirala, dok se druga faza može podijeliti na još dvije, a to su poboljšanje slike i segmentacija iste. Prilikom obrađivanja slike, izoštravaju se dijelovi uha, njegovih rubova te se nastoji poboljšati slika i općenito dinamika svih skeniranih značajki.[66] S druge strane, segmentacija slike odnosi se na proces dijeljenja digitalne slike u više segmenata (npr. piksela) kako bi se pojednostavio i analizirao prikaz.[67] Naposljetku, treća faza koja se tiče klasifikacije, nastoji klasificirati biometrijski uzorak koji se kasnije pohranjujeu bazu. Kao dobar primjer softvera može se navesti je HELIX SDK koji se koristi u raznim

---

[61] Usp. Retinal Recognition: the Ultimate Biometric. URL: https://www.rootstrap.com/blog/retinal-recognition-the-ultimate-biometric (2023-02-24)
[62] Isto.
[63] Isto.
[64] Isto.
[65] Usp. Abaza, Ayman et al. Ear recognition: A Complete System. URL: http://www.wvhtf.org/wpcontent/uploads/2015/08/EarSystem3_1.pdf (2023-02-24)
[66] Usp. Saranya, M et al. An Approach towards Ear Feature Extraction for Human Identification. IEE, 2016. Chennai. URL: 10.1109/ICEEOT.2016.7755636 (2023-04-24)
[67] Isto.

industrijama, a omogućuje korisnicima integraciju s već postojećom aplikacijom na svom telefonu.[68]

3.1.5 Prepoznavanje lica

Prepoznavanje lica danas je uz otisak prsta najkorištenija metoda autentifikacije. Funkcionira tako da skener prvo identificira crte lica korisnika, a potom ih i izmjeri. To je moguće postići preko fotografija i videozapisa, gdje se uspoređuju lica među velikom skupinom drugih.[69] Prema tome,kao prva prednost ovakve autentifikacije može se izdvojiti učinkovita sigurnost, jer u usporedbi s korištenjem PIN-a ili lozinke, manje je dodirnih točaka između korisnika i biometrijskog sučelja.[70] Osim toga, poboljšana je točnost detekcije i lakša integracija s drugim sigurnosnim softverima. Što se tiče samog procesa identifikacije preko lica korisnika, odvija se slično kao u ostalim biometrijskim sustavima - proces ima tri faze: detekcija, analiza i podudaranje. Prva faza, odnosi se na pronalaženje lica na slici na kojoj može biti jedna ili više osoba, snimljeno frontalno ili iz profila.Da bi ovaj postupak uspio, računala koriste složene tehnike umjetne inteligencije pa "računalni vid" obavlja ekstrakciju, analizu i potom klasificira dobivene biometrijske podatke iz slikovnih.[71] U fazi analize, biometrijski sustav analizira sliku lica korisnika, odnosno postojeću geometriju i crte, koje su ključni element u razlikovanju drugih. Ono što se najviše uzima u obzir su razmak između očiju, udaljenost od čela pa do brade, udaljenost između usta i nosa, dubina očnih duplji, oblik jagodica te kontura usana, ušiju i brade.[72] Nakon toga, sustav pretvara dobivene biometrijske podatke u niz brojeva ili točaka koji se naziva otisak lica.[73] Informacije dobivene na ovaj način mogu se također koristiti i za digitalnu rekonstrukciju lica osobe.[74] Posljednja faza referira se na podudaranje. Primjerice, podudara li se lice snimljeno mobilnom kamerom sa licem na osobnoj iskaznici ili iskaznici vozačke dozvole.[75] Algoritmi koji ovo otkrivaju u idealnim uvjetima bi trebali imati savršenu točnost, no teško je predvidjeti je nijedna snimljena fotografija nije kompletno savršena.[76]

3.1.6. Termogram lica

Još jedan primjer fizioloških biometrijskih sustava jesu termogrami lica koji se posljednjih godina koriste kao alternativa vizualnom prepoznavanju korisnika. Koristeći infracrvenu svjetlost stvara se

---

[68] Usp. HELIX SDK - Ear Recognition Software for the Enterprise. URL: http://www.descartesbiometrics.com/helix-sdk/ (2023-02-24)
[69] Usp. What is Facial Recognition? - Face Recognition Software and Face Analysis Explained - AWSURL: https://aws.amazon.com/what-is/facial-recognition/ (2023-02-24)
[70] Isto.
[71] Isto.
[72] Isto.
[73] Isto.
[74] Isto.
[75] Isto.
[76] Isto.

toplina kojom se ozrači lice, koja nastaje na osnovu vrele krvi korisnika. Funkcioniranje ovakvog biometrijskog sustava vrlo je slično drugim vrstama, a uključuje sljedeće: snimanje termograma, normalizacija, ekstrakcija (izdvajanje) značajki te autentifikacija.[77] Biometrijska karakteristika, odnosno njezina temperatura, snima se pomoću kamere koja se postavlja na visinu od 2 m.[78] Korisnici trebaju stati ispred kamere kako bi se skeniralo lice korisnika, a ono mora biti cijelo pokriveno te rezolucija slike treba biti 480 x 640. Stvorena slika najprije bude binarna.[79] Kako bi slika bila što kvalitetnija, slike koje se snime na sobnoj temperaturi trebaju se usporediti sa slikama snimljenih u vanjskim uvjetima.[80] Ovakva biometrijska karakteristika nije pouzdana u različitim temperaturnim uvjetima te zbog toga nije previše korištena.[81]

3.1.7. Prepoznavanje vene

Prepoznavanje vene može se definirati još kao vaskularna biometrija, čija je svrha mjeriti dijelove krvožilnog sustava korisnika pa je zbog toga primjena ovakvog biometrijskog sustava vrlo raširena u medicini.[82] Vaskularnom biometrijom mogu se skenirati vene na dlanu, prstu ili pak očnoj jabučici. S obzirom da se radi o unutarnjoj značajci prstiju, vene je poprilično zahtjevno skenirati uređajem bez infracrvenog svjetla. Zbog toga je važno koristiti određenu fotoosjetljivu kameru, koja uz prisutnost infracrvenog svjetla deoksidira hemoglobin iz krvi.[83] Dok infracrveno svjetlo može proći kroz korisnikov prst, hemoglobin je bolji, odnosno učinkovitiji u apsorpciji svjetlosti od drugih tvari kao što su mišići i kosti.[84] Skeniranje vene korisnika smatra se izrazito uspješnom tehnikom autentifikacije, a to omogućuju sljedeće značajke: visoka razina točnosti i preciznosti, teža mogućnost lažiranja (jer je unutarnja biometrijska karakteristika) i teža mogućnost neovlaštenog stjecanja. Proces skeniranja odvija se u tri faze, kao i kod drugih biometrijskih sustava - obrada i dobivanje slike, predprocesiranje, izdvajanje značajki te podudaranje.[85] Faza predprocesiranja ima značajan utjecaj na ishode prepoznavanja, dok je faza izdvajanja značajki podijeljena u dva dijela - prvi dio odnosi se na vaskularnu geometriju vene dlana, dok se drugi dio temelji na holističkom povratu ulaganja, koje uzima skeniranu sliku kao cjelinu te izravno koristi informacije iz te slike.[86]

---

[77] Isto.
[78] Isto.
[79] Isto.
[80] Isto.
[81] Usp. Hanmandlu, M et al. Online Biometric Authentication Using Facial Thermograms. IEE, 2012. Washington. URL: 10.1109/AIPR.2012.6528223 (2023-04-28)
[82] Usp. Vein Recognition. URL: https://findbiometrics.com/solutions/vein-recognition/ (2023-04-28)
[83] Usp. Research on Technology of Finger Vein Pattern Recognition Based on FPGA . URL: https://iopscience.iop.org/article/10.1088/1742-6596/1453/1/012037/pdf (2023-04-28)
[84] Usp. Matsui, Y. et al. Global Deployment of Finger Vein Authentication. URL: https://www.hitachi.com/rev/pdf/2012/r2012_01_108.pdf (2023-04-28)
[85] Isto.
[86] Usp. Wu, Wei et al. Review of palm vein recognition. URL: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2019.0034 (2023-04-28)

Bez obzira na sve navedeno, vaskularna biometrija sadržava i određene nedostatke, kao što su jeftina i minijaturizacija slika vena na dlanu, slike vena s niskim kontrastom, visokim šumom i neravnomjernim osvjetljenjem te procjena kvalitete slike vene dlana.[87]

3.1.8. Prepoznavanje DNK

DNK biometrijska karakteristika smatra se dobrim biometrijskim identifikatorom jer nije pod utjecajem starenja ili nezgode, jedinstvena je, univerzalna, prikupljiva (mjerljiva) te što je najvažnije - ima najveću točnost, odnosno najpouzdanija je metoda autentifikacije. Nakon otiska prsta, identifikacija korisnika pomoću DNK često je prisutna u forenzici i kriminalistici.[88] Ona se dobiva biološkim putem u laboratoriju te je potrebno i do pet sati za njezinu obradu.[89] Budući da svaka DNK ima svoja "ponavljanja", ono zapravo predstavlja esenciju za stvaranje jedinstvenog profila.[90] Na temelju podudaranja, jedinstveni profil može se stvoriti za samo 90 minuta, a njegovi rezultati pohranjuju se u bazu podataka. Podaci o DNK zabilježeni su u posebnim formatima datoteka pa se na taj način omogućuje interoperabilnost između sustava.[91] No, bez obzira na uspješnuinteroperabilnost, postoje sigurnosni problemi vezani za osiguranje DNK sustava, a to su pravo pristupa, korištenje informacija, povjerljivost koji su detaljnije razjašnjeni u petom poglavlju.

3.2. Bihevioralni biometrijski sustavi

Bihevioralni biometrijski sustavi odnose se na mjerenje jedinstveno identificirajućih i mjerljivih obrazaca u ljudskim aktivnostima.[92] U usporedbi s fizičkim biometrijskim sustavima, bihevioralni su u suprotnosti, jer ne uključuju urođene ljudske karakteristike kao što su otisci prstiju ili primjerice mrežnice očiju.[93] U daljnjem dijelu poglavlja bit će objašnjene autentifikacije pomoću potpisa, glasa, hoda korisnika te pomoću njegovog udarca po tipkovnici.

---

[87] Isto.
[88] Usp. Iloanusi,O et al. Automating DNA Biometric Recognition for Real-Time Person Identification. URL: http://nanotechunn.com/new/wp-content/uploads/2018/09/Nanocon314-29-Ilonusi-Automating-DNA-Biometric-Recognition-for-Real.pdf (2023-04-28)
[89] Isto.
[90] Isto.
[91] Usp. IBIA | Biometric Technologies | DNA . URL: https://www.ibia.org/biometrics-and-identity/biometric-technologies/dna (2023-04-28)
[92] Usp. What is bihevioral bioemtrics? | Definition from TechTarget. URL: https://www.techtarget.com/whatis/definition/behavioral-biometrics (2023-04-28)
[93] Isto.

3.2.1. Prepoznavanje potpisa

Prva vrsta biometrijskog bihevioralnog sustava odnosi se na potpis, a prvi takav mehanizam uveden je 1965.godine.[94] Ova metoda se inače sastoji od olovke i posebnog tableta koji su spojeni na računalo kako bi se usporedili i time provjerili uzorci.[95] Proces autentifikacije se inače odvija na visokokvalitetnom tabletu, koji može uhvatiti karakteristike ponašanja kao što su brzina, pritisak i vrijeme potpisivanja.[96] Inače se sastoji od tri faze, a to su prikupljanje uzoraka (upis), stvaranje profila (rukovanje uzorcima) te provjera odnosno podudaranje uzorka s postojećim uzorcima u bazi podataka.[97] U procesu upisa potrebno je oko šest potpisa koji se mogu jednostavno prikupiti, a korisnik to obavlja onako kao inače kad bi se potpisivao na papiru - olovkom.[98] Kad je to obavljeno, njegovi potpisi se pohranjuju u bazu. Također, važno je naglasiti da određeni biometrijski sustavi mogu dopustiti više od jednog tipa potpisa, primjerice standardni vlastoručni potpis te potpis samo sa korisnikovim inicijalima.[99] Tako npr. ako korisnik prilikom pristupa sustavu provjerava svoj potpis, biometrijski poslužitelj mora najprije usporediti trenutni potpis s postojećim potpisima, koji se mogu promijeniti tijekom vremena.[100] Danas su ovakvi sustavi vrlo cijenjeni jer lako zamjenjuju fizički, a vrhunske IT tvrtke iz dana u dana idu u korak dalje, uvodeći aplikacije i jednostavnije procese koje nitko prije nije mogao zamisliti.[101]

3.2.2. Prepoznavanje glasa

Postoje i biometrijski sustavi koji mogu primati i tumačiti izgovorene upute korisnika te odgovarati na njegove naredbe. Ovakav biometrijski sustav prvotno je integriran u osobna računala, ali sa s većim širenjem pametnih uređaja, postaje sve više dostupniji korisnicima.[102] No već na samom početku, potrebno je razjasniti razliku između prepoznavanja glasa i govora. Prije svega, prepoznavanje glasa odnosi se na prepoznavanje glasa pojedinog korisnika, dok se prepoznavanje govora odnosi na riječi te se još fokusira na prijevod, dakle verbalni u tekstualni.[103] Osim što je dostupan u tražilicama, dostupan je i u mnogim kućanskim aparatima. Postoje dvije vrste ovakvih biometrijskih sustava - oni koji su ovisni o tekstu i oni koji nisu. Prva spomenuta skupina odnosi se

---

[94] Usp. Exploring viability of signature recognition biometrics | Infosec Resources. URL: https://resources.infosecinstitute.com/topic/signature-recognition-biometrics/ (2023-04-28)
[95] Usp. Two Main Types of Biometrics: Physical vs. Behavioral Biometrics | RecFaces. URL: https://recfaces.com/articles/types-of-biometrics#26 (2023-04-28)
[96] Isto.
[97] Usp. Signature verification in Real Time. URL: https://www.xyzmo.com/e-signature-products/signature-verification (2023-04-28)
[98] Isto.
[99] Isto.
[100] Isto.
[101] Isto. Exploring viability of signature recognition biometrics. Nav. dj.
[102] Usp. What is Voice Recognition Technology an Its Benefits - Zesium . URL: https://zesium.com/what-is-voice-recognition-technology-and-its-benefits/ (2023-04-29)
[103] Isto.

na specifični skup riječ koji korisnik izgovara, gdje se pritom provjerava identitet korisnika.[104] To je moguće provjeriti tek kad korisnik izgovori određenu rečenicu. S druge strane, neovisni sustavi ne ovise o tekstu već se sustav oslanja na razgovor između korisnika, tako da prvotna autentifikacija s rečenicom nije potrebna.[105] Ova dva sustava uvelike pružaju podršku i pomoć u provođenju zadataka kao što su primjerice pozivi, zakazivanje sastanaka i sl. Na taj način pojednostavljuje se proces, a samim time povećava se učinkovitost i produktivnost te je korisniku puno lakše pristupiti relevantnim informacijama na puno brži način nego kad bi svoj upit obavio tipkanjem u tražilici.[106]

3.2.3. Prepoznavanje mirisa

Prepoznavanje mirisa tijela podrazumijeva beskontaktnu fizička vrstu biometrije koja ima za cilj potvrditi identifikaciju korisnika analizom olfaktornih svojstava mirisa njegovog tijela i za razliku od drugih biometrijskih sustava, kao što je prepoznavanje lica, koje ima visoku stopu pogrešaka, i tehnologija otiska prsta, koja zahtijeva kontakt, biometrija mirisa daje visoku točnost i to bezkontaktno.[107] S obzirom da ljudsko tijelo emitira dosta složen raspon molekula koje su nehlapljive i hlapljive, znanstvenici su odlučili osmisliti biometrijski sustav koji bi te molekule klasificirao u određene skupine, a postoje tri - znoj, miris koji se oslobađa iz usne šupljine te miris koji se oslobađa iz ljudskih izlučevina (urin).[108] Ovo je moguće postići koristeći određene elektroničke uređaje koji oponašaju ljudske mirisne obrasce te senzore za plin (tzv. “E-nose”), kao što je npr. senzor metalnog oksida koji otkriva hlapljive organske spojeve.[109] Nakon što se E-nosom osjeti kemijski miris, počinje proces prepoznavanja. Proces prepoznavanja kombinira strojno učenje i statističke tehnike za generiranje značajki.[110] Ovaj generator značajki izvlači diskriminatorne značajke iz "mirisa" te može generirati digitalni niz značajki poznat kao biometrijski predložak.[111] Ovaj se biometrijski predložak zatim može koristiti za klasificiranje osobe na temelju njezinog jedinstvenog profila mirisa.[112] Ovakve tehnologije često su povezane s problemima privatnosti, jer mogu zapravo mnogo toga otkriti što se tiče zdravstvenog stanja osobe - je li ona izložena stresu, uzima li lijekove i sl. Briga o privatnosti, ne razlikuje se nimalo od one izražene o prepoznavanju emocija te bi se mogla neetički koristiti protiv korisnika bez njihova znanja.[113]

---

[104] Isto.
[105] Isto.
[106] Isto.
[107] Usp. Could you Unlock Your Phone with Your Body Odor? | by Brinnae Bent, PhD | Medium. URL: https://runsdata.medium.com/could-you-unlock-your-phone-with-your-body-odor-830ae1860481(2023-02-16)
[108] Isto.
[109] Isto.
[110] Isto.
[111] Isto.
[112] Isto.
[113] Isto.

3.2.4. Prepoznavanje hoda

Sustav za prepoznavanje hoda može koristiti oblik ljudskog tijela i način na koji se on kreće s ciljem njegovog identificiranja.[114] Tako npr. softver pomoću CV algoritama ima mogućnost otkrivanja ljudske siluete na videu uz analiziranje pokreta.[115] Ovakve tehnologije koriste više od jednogsenzora za hvatanje biometrijske karakteristike. Kako bi se te karakteristike uspješno prepoznale, prikupljene informacije moraju proći niz koraka.[116] Algoritam koji ovo omogućuje mora znatiprepoznati hod, detektirati sve siluete i ljudske crte hoda korisnika. Bez obzira na to, algoritam moževarirati jedan od drugog, odnosno jedni algoritmi imaju zadaću obraditi video signal, dok drugi moraju koristiti sve podatke dobivene senzorom.[117] Preciznost i uvježbanost u klasificiranju dvije su odlike ovakvih biometrijskih sustava, a inače se sastoje od četiri komponente - hvatanje podataka o hodu, segmentacija siluete, otkrivanje kontura te izdvajanje značajki i njihova klasifikacija.[118] Tehnologije ovakve vrste nisu invazivne te stopa pogreške iznosi 0.7%.[119] Iako se primjenjuju beskontaktno, svejedno postoje neka ograničenja, a ona se odnose na specifične senzorske ploče te na kameru vrlo visoke rezolucije, zbog same kvalitete prepoznavanja.[120] S obzirom da se mogu primijeniti bez pristanka korisnika, dolazi do problema privatnosti i sigurnosti. Osim toga, ovakav sustav može prepoznati samo osobe čiji su podaci unaprijed snimljeni i pohranjeni u bazi, tako dajoš nema dovoljno širok spektar funkcionalnosti.[121]

3.2.5. Prepoznavanje na osnovi udarca tipke na tipkovnici

Iako se mnogi vjerno oslanjaju na otisak prsta, brojni korisnici danas koriste dinamiku svojeg tipkanja kao metodu autentifikacije. Na osnovu pritiska tipke, ovaj biometrijski sustav daje detaljne informacije o vremenu kad je svaka tipka u određeno vrijeme pritisnuta te kad je ona otpuštena.[122] Kod ovakve vrste sustava bitno je naglasiti da se uz pomoć algoritma mjeri vrijeme zadržavanja, koje se odnosi na trajanje u kojemu je tipka pritisnuta te vrijeme leta, koje podrazumijeva trajanje između pritisaka tipki.[123] 2004. godine su znanstvenici s MIT-a (Massachusetts Institute of Technology) zapazili određene prednosti i nedostatke vezane za ovakve sustave. Kao prvo, dinamika tipkanja kao biometrijska karakteristika znatno je pristupačna i nenametljiva biometrija jer

---

[114] Usp. Gait Recognition: How It Works, The System & The Algorithm — RecFaces. URL: https://recfaces.com/articles/what-is-gait-recognition (2023-04-30)
[115] Isto.
[116] Isto.
[117] Isto.
[118] Isto.
[119] Isto.
[120] Isto.
[121] Isto.
[122] Usp. Explainer: Keystroke recognition | Biometric Update. URL: https://www.biometricupdate.com/201612/explainer-keystroke-recognition (2023-04-30)
[123] Isto.

kao takva zahtjeva korištenje malo hardvera, osim tipkovnice. Na taj način se dobro implementira u poduzeća, a i cjenovno je prihvatljiviji od ostalih biometrijskih sustava.[124] No, s druge strane, znanstvenici s MIT-a otkrili su i određene nedostatke. Prvo što su izdvojili jest nedosljednost u obrascu tipkanja jer mnogi korisnici odrade tipkanje zgrčenih mišića ili znojnih ruku što značajno može promijeniti proces autentifikacije.[125] Osim toga, obrasci tipkanja mogu varirati ovisno o vrsti tipkovnice, što ponekad može otežati postupak provjere.[126] Osim toga, ovaj sustav pokazuje osjetljivost na položaj korisnika, jer primjerice, ako korisnik sjedi dok tipka, može doći do lažnog odbijanja (autetifikacije).[127] Koliko god se ovi nedostaci činili zabrinjavajući, ipak to nisu krucijalni problemi jer današnji razvoj algoritama i strojnog učenja mogu brzo otkloniti ovakve učinke.

[124] Isto.
[125] Isto.
[126] Isto.
[127] Usp. What's Your Type? Keystroke Dynamics as Behavioral Biometrics. URL: https://www.aratek.co/news/keystroke-dynamics-as-behavioral-biometrics (2023-04-30)

4. IZAZOVI BIOMETRIJSKE TEHNOLOGIJE

Prijevare

Prema INTERPOL-u, Međunarodnoj kriminalističko-policijskoj organizaciji, lažni dokumenti sredstvo su za provođenje teškog kriminala, uključujući pritom pranje novca i terorizam koji predstavljaju prijetnju građanima, zemljama i globalnoj ekonomiji općenito.[128] Promatrajući statistiku, izvješća navode da se biometrija zapravo smatra faktorom odvraćanja od prijevara, jer je nesofisticirana (barem za sad), a tomu potvrđuje i činjenica da puno manje prevaranata pokušava napasti korisnike preko selfija i videa u usporedbi s drugim dokumentima.[129] Prosječna stopa prijevare s dokumentima u 2021. godini bila je 5.9% u usporedbi s 1.53% (selfiji) i 0.17% (video zapisi).[130] S obzirom da video zapis pruža više zaštite od samog selfija, video korisničko iskustvo samo po sebi odvraća brojne prevarante jer je doista komplicirano prevariti sustav.[131] Također, snimke zaslona najčešće su korišteno sredstvo za biometrijske napade. Prevaranti mogu koristiti čak i ukradeni ID, kako bi uspjeli izvršiti primjerice pretraživanje, pronaći društvenu mrežu i na njoj profilnu sliku koju bi kasnije učitali u sustav i predstavili to kao vlastiti selfie.[132] Međutim, i dalje vlada određena razina nesigurnosti oko toga, odnosno ili su sofisticirane metode napada još uvijek nedostupne većini prevaranata ili se pak brojni prevaranti bore pronaći načine kako zaobići biometrijske provjere svojih meta.[133]

Uporabljivost

Interaction Design Foundation definira uporabljivost kao mjeru koliko dobro određeni korisnik u određenom kontekstu može koristiti proizvod za učinkovito, djelotvorno i zadovoljavajuće postizanje definiranog cilja.[134] Dizajneri biometrijskih softvera uglavnom mjere uporabljivost dizajna tijekom cijelog procesa razvoja softvera - od njegovih početnih skica i prototipa do konačnog isporučenog proizvoda - kako bi se osigurala maksimalnu uporabljivost.[135] Nielsen Norman Group, svjetski poznata tvrtka koja se bavi dizajnom softvera i proučava korisnička iskustva, navodi kako je uporabljivost zapravo druga razina korisničkog iskustva te da uporabljivost dizajna biometrijskog softvera ovisi o tome koliko dobro njegove značajke

[128] Usp. Identity Fraud Report 2022. URL: https://onfido.com/wp-content/uploads/2022/10/identity-fraud-report-2022.pdf (2023-02-17)
[129] Isto.
[130] Isto.
[131] Isto.
[132] Isto.
[133] Isto.
[134] Usp. What is Usability? | IxDF. URL: https://www.interaction-design.org/literature/topics/usability (2023-02-17)
[135] Isto.

odgovaraju potrebama i kontekstu korisnika.[136] Kad je u pitanju uporabljivost, dizajneri trebaju uzeti u obzir sljedeće elemente: efikasnost, učinkovitost, angažman, tolerancija na pogreške i lakoća učenja. Dobra efikasnost podržava korisnike u točnom dovršavanju radnju, dok im kvalitetna učinkovitost omogućuje izvršavanje zadataka što brže.[137] Također, potreban je i dobar angažman kako bi korisnici biometrijski softver mogli smatrati ugodnim i prikladnim za korištenje bilo kad.[138] Osim toga, važno je uzeti u obzir i mogućnost stvaranja pogreški od strane korisnika, odnosno da se prikaže pogreška samo u pravim situacijama koje se mogu postići saznavanjem broja i vrste ozbiljnosti pogrešaka koje mogu nastati.[139] Na greškama se uči, pa samim time korisnici uče i pamte iznova i iznova. Što se tiče samog procesa dizajniranja i upotrebljivosti biometrijskih sustava, on čest zna biti izazovan, osobito kad je u pitanju dizajn čitača za otisak prsta. Čitači otiska prsta mogu biti problematični ako su prsti postavljeni izvan središta skeniranja ili ako se prst pomiče tijekom procesa skeniranja.[140] Takve situacije je zaista važno predvidjeti. Coventry navodi kako je česti neuspjeh autentifikacije zapravo taj što korisnik ne stavi ispravno prst u središte senzora.[141] Postoje bolji čitači koji imaju svoje kanale koji pomažu u pravilnom postavljanju prstiju.[142] Sličan proces skeniranja odvija se i sa šarenicom oka.[143] Skeneri šarenice također dobro reagiraju i prepoznaju nepravilan položaj oka te nastoje ostvariti tzv. poravnanje (usklađivanja) oka s lećom fotoaparata.[144] Rezultati istraživanja prema Patricku, sugeriraju da navedeno usklađivanje ponekad može biti kompliciranо i presudno za uspjeh izrade i primjena biometrijskih softvera.[145] Osim toga, treba imati na umu i ponašanje korisnika. Korisnici su nepredvidljivi i ne razumiju svi toliko puno cjelokupan proces, a sučelja ne objašnjavaju kako se predlošci stvaraju i primjerice dalje pohranjuju.[146] Korisnici često pretpostavljaju da je njihova cjelovita slika biometrijskih karakteristika spremljena, što uglavnom dovodi do povećane zabrinutosti zbog zlouporabe i prikupljanja njihovih podataka.[147]

---

[136] Isto.
[137] Isto.
[138] Isto.
[139] Isto.
[140] Usp. Usability and Acceptability of Biometric Security Systems. URL: file:///C:/Users/Donata/Downloads/Usability_and_Acceptability_of_Biometric_Security_.pdf (2023-02-17)
[141] Isto.
[142] Isto.
[143] Isto.
[144] Isto.
[145] Isto.
[146] Isto.
[147] Isto.

Pristupačnost

Za poželjne karakteristike biometrije mogu se navesti transparentnost, pouzdanost i jednostavnost upotrebe.[148] No, postavlja se pitanje je li zapravo biometrijsko prepoznavanje jednako intuitivno, pristupačno i efikasno za korištenje i korisnicima s teškoćama?[149] Ono je danas predmet brojnih rasprava. Kako bi se bolje razumio ovaj problem, autori Ramon, Chiara, Raul i Richard navode za primjer korištenje mobilne aplikacije u kojoj korisnici trebaju podići novac s fiktivnog bankomata, pri čemu kod autentifikacije korisnici mogu koristiti tri tipa biometrijske karakteristike - svoje lice, glas ili otisak prsta.[150] U suradnji s Centrom za oporavak osoba s tjelesnim i mentalnim invaliditetom u Madridu autori su proveli istraživanje koje je imalo tri cilja, a to su testiranje dostupnosti konvencionalnih modaliteta biometrijske autentifikacije na mobilnom telefonu, usporedba tradicionalnih mehanizama autentifikacije u smislu performansi i pristupačnosti te uspostaviti grupe ispitanika/korisnika s obzirom na pristupačnost te na taj način uspostaviti veze između navedenih grupa korisnika i modaliteta.[151] Eksperiment se sastojao od traženja ispitanika da obave autentifikaciju na aplikaciji kako bi podigli novac s fiktivnog bankomata i time testirali pristupačnost. Ispitanici su bili podijeljeni s obzirom na stupanj invaliditeta, no važno je napomenuti da neki ispitanici imaju više od jednog, tako da su neki uključeni u više od jedne skupine invaliditeta[152]:

U prvoj su skupini[153] tjelesne teškoće:

- potpuna ili djelomična nemogućnost korištenja šake i/ili ruke; očekivanja oko otežane interakcije s mobilnim zaslonom (rukovanje i dodirivanje)
- potpuna ili djelomična nemogućnost hodanja; očekivanja oko oteženog rukovanja s mobilnim telefonom
- poteškoće s vidom - slabovidnost i potpuna sljepoća; očekivanja oko otežane percpecije vizualnih informacija

Druga skupina[154] odnosi se na psihičke poteškoće:

- kognitivne teškoće ili poteškoće s učenjem; odnosi se na potpunu ili samo djelomičnu nesposobnost nerazumijevanja uputa, koraka i iščitavanja znakova na mobilnom telefonu

Ispitanici su bili u interakciji s Android aplikacijom pokrenutom na pametnom telefonu OnePlus

---

[148] Usp. Blanco-Gonzalo R, Lunerti C, Sanchez-Reillo R, Guest R. Correction: Biometrics: Accessibility challenge or opportunity?. PLOS ONE 13(4). 2018. e0196372. https://doi.org/10.1371/journal.pone.0196372. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0194111 (2023-04-24)
[149] Isto.
[150] Isto.
[151] Isto.
[152] Isto.
[153] Isto.
[154] Isto..

3T.[155] Ovaj mobilni uređaj odabran je jer uključuje ugrađeni senzor otiska prsta te prednju kameru od 16 MP te se smatra kako uređaj zadovoljava standarde i zahtjeve utvrđene dosadašnjimradom.[156] Što se tiče fiktivnog bankomata, to je Sony Xperia Tablet Z, povezan s aplikacijom za pametni telefon putem Bluetootha.[157] Što se tiče provedbe eksperimenta, odvijao se u dvije sesije. Modela autentifikacije bilo je više - biometrijski (glas, lice i otisak prsta) te nebiometrijski (PIN i uzorak). Nakon što su svi ispitanici završili s ponuđenim načinima prijave, fiktivni bankomat na ekranu prikazao im je lažnu novčanicu od 20 €.[158] Osim toga, na ekranu je bila napisana rečenica koju su trebali pročitati. Rezultati su pokazali kako pridaju svoju sklonost modalitetima koji zahtijevaju manje interakcija s provjerom lica. Unatoč tome, na kraju evaluacije, 28% ispitanika idalje preferira korištenje PIN-a jer ga smatraju sigurnijim od biometrije. Također, eksperiment je potvrdio kao bi većina ispitanih koristila biometriju, ali ne za bankovne transakcije jer osjećaju strah te imaju manjak samopouzdanja i povjerenja u nove tehnologije. Osim toga, mnogi ispitanicinisu mogli dovršiti drugu provjeru PIN-a i uzorka jer su zaboravili svoje vjerodajnice, dok su nekiodustali u procesu autentifikacije lica i otiska prsta, navodeći pritom sigurnosne probleme. Shodno svemu tome, može se zaključiti kako je potrebno prilikom budućih eksperimenata obratiti pozornost na nervozne i tjeskobne korisnike koji pokušavaju obaviti autentifikaciju te da tajproces obave na što mirniji način.[159] Također, potrebno je poboljšati u provjeri glasa u trenutku čitanja rečenica jer dosta ispitanika ima vjerojatno problema s čitanjem s ekrana (npr. mala slova, poteškoće s pravilnim čitanjem zbog drhtanja ruku i sl.).[160] Na taj bi način bilo manje interakcije sa sustavom i korisnici bi puno bolje reagirali i riješili potrebne zadatke.

Održavanje

Budući da je biometrijska tehnologija postala sastavni dio mnogih sustava kontrole u tvrtkama, njezino održavanje smatra se dobrim baš onoliko koliko je dobra najslabija karika u sustavu.[161] Zahtjeva puno jer biometrijski sustav funkcionira zajedno s biometrijskom bazom podataka, internetskom mrežom, čitačem, kamerom i sa još drugim srodnim sustavima.[162] S obzirom da funkcioniraju zajedno, kvar bilo koje dijela biometrijskog sustava može ugroziti sigurnost

[155] Isto.
[156] Isto.
[157] Isto.
[158] Isto.
[159] Isto.
[160] Isto.
[161] Usp. The maintenance of biometric equipment is vital to its effective use - September 2012 - Hi-Tech Security Solutions. URL: http://www.securitysa.com/43423n (2023-02-17)
[162] Isto.

podataka i na taj način usporiti provođenje poslovnih procesa.[163] Kako bi se osiguralo dobro funkcioniranje biometrijskog softvera, prvo i osnovno što je potrebno je njegovo postavljanje, koje ovisi o točnoj registraciji korisnika - odnosno autentifikaciji. Uspješnom prijavom korisnik treba biti upisan u bazu podataka, no ako je prijava neuspješna, pristup se lažno prihvaća ili lažno odbija.[164] Osim toga, administrativni dio baze podataka također mora funkcionirati uredno, osobito ako neko od korisnika napusti tvrtku ili promijeni status.[165] U takvim slučajevima ažuriranje mora biti besprijekorno. Treba uzeti u obzir i broj mogućih registracija, jer uobičajene biometrijske baze podataka imaju ograničeni broj, tako da u prekoračenju broja registracija sustav sporije reagira, a u krajnjem slučaju može prouzrokovati kvarove i na mreži, čime opada operativna učinkovitost[166]. Također, važno je redovito provjeravati sve fizičke komponente. Primjerice, ako se biometrijski skener zaprlja ili ošteti izlaganjem određenim teškim uvjetima (npr. prašina, ekstremno visoka temperatura, kiša) može doći do pada cjelokupnog sustava.[167] Kako bi se ove situacije izbjegle, redovito održavanje svaka tri mjeseca ili češće (ovisno o korištenju) moglo bi eliminirati spomenute izazove i produžiti vijek trajanja biometrijskog softvera.[168] Za optimizaciju performansi biometrijskog sustava ključno je, dakako, imenovati pružatelja usluga koji ima odgovarajuće tehničke vještinama.[169] Idealan partner za održavanje treba biti tvrtka koja stvarno razumije i koja ima široko iskustvo u postavljanju i upravljanju biometrijskom tehnologijom i povezanim sustavima (kontrola pristupa, alarmi itd.) u različitim industrijama (korporacija, zdravstvo, javni prijevoz, javni sektor).[170] Tvrtka bi trebala imati kvalificirano osoblje koje će pokazati fleksibilnost i stručnost u pravo vrijeme.[171] U konačnici, važno je postići dobar odnos i po pravnom pitanju, odnosno uspostaviti ugovor o održavanju tehnologije ovakve vrste te obaviti cjelokupnu dijagnostiku kao što je procjena mreže, baza podataka i ostalih važnih čimbenika.[172]

[163] Isto.
[164] Isto.
[165] Isto.
[166] Isto.
[167] Isto.
[168] Isto.
[169] Isto.
[170] Isto.
[171] Isto.
[172] Isto.

Ograničenja

Web 3.0 vidljivo širi svoje granice i stalno se mijenja stoga organizacije trebaju proaktivno djelovati u cilju da zaštite svoju postojeću informacijsku infrastrukturu.[173] Zaštita infrastrukture nikada nije bila jednostavna, jer uvijek postoje određeni izazovi i ograničenja koji na neki način "koče" razvoj i primjenu biometrijskih sustava. Postojeća ograničenja mogu se sagledati s nekoliko stajališta - poslovnog, operativnog, sustavnog, tehničkog, pravnog i regulatornog te sa stajališta ljudskih resursa.[174] S poslovnog stajališta važno je napomenuti da biometrija sama po sebi nikad nije dovoljna. Ona mora ispunjavati određenu svrhu kako bi se osigurala povjerljivost, dostupnost i integritet postojećih podataka s kojima upravlja.[175] Izazov predstavlja dinamika organizacije te povezivanje i integraciju s drugim dijelovima sustava, a kao primjer mogu se navesti podjela dužnosti u tvrtki - nadzor, odobrenje, provjera transakcija ili pak procjena rizika.[176] Ograničenja s operativnog stajališta odnose se na proces autentifikacije i pohrane korisnika u biometrijski sustav, a sasvim je jasno da je privilegija pristupa jedan od najvažnijih problema, uz brzinu pristupa i vrijeme prekida rada sustava.[177] Stajalište ljudskih resursa predstavlja ogromno ograničenje u implementaciji jer se radi o izgradnji povjerenja u javnosti. I dalje vlada određena razina nesigurnosti i nepovjerenja među korisnicima upravo zbog pitanja kako očuvati privatnost i povjerjivost svojih podataka.[178] Ograničenja u pravnom i regulatornom smislu odnose se na nedostatak pravne jasnoće te na zabrinutost oko vlasništva.[179] Kako bi se nejasnoće smanjile, neminovno slijedi uspostava i provjera učinkovitosti biometrijskih podataka i procesa autentifikacije korisnika.[180] Osim toga, ograničenja u tehničkom pogledu može biti opseg biometrijskih karakteristika između potencijalnih korisnika. Nadalje, prirodno starenje i neočekivane promjene fiziološke karakteristike (npr. nezgoda ili operacija) mogu ograničiti upotrebu i učinkovitost autentifikacije.[181] Također, neki biometrijski sustavi zahtijevaju ponovni upis, što bi moglo povećati troškove i smanjiti privlačnost biometrijske sigurnost.[182] Izazovi sa stajališta sustava uključuju ne samo učinak tehnologije na poslovne procese, već i dizajn te performanse sustava zajedno sa modeliranjem i arhitekturom podataka.[183]

---

[173] Usp. Chandra, A., & Calderon, T.. Challenges and constraints to the diffusion of biometrics in information systems. Communications of the ACM, 48(12), 2005. Str. 101–106. doi:10.1145/1101779.1101784 (2023-04-24)

[174] Isto.
[175] Isto.
[176] Isto.
[177] Isto.
[178] Isto.
[179] Isto.
[180] Isto.
[181] Isto.
[182] Isto.
[183] Isto.

5. TRENDOVI RAZVOJA BIOMETRIJSKE TEHNOLOGIJE

5.1. Multimodalna autentifikacija korisnika

Kao prvi trend može se izdvojiti tzv. multimodalna provjera autentifikacije korisnika. Nazivaju se multimodalnima jer koriste dva ili više biometrijska modaliteta za identifikaciju pojedinca, a cilj im je poboljšati brzinu i kvalitetu prepoznavanja korisnika. Upravo zbog postojanosti autentifikacije ovakve vrste, gradi se dobra budućnost pametnih gradova.[184] Diljem svijeta pametni gradovi *(eng. Smart cities)* imaju implementiranu višeslojnu arhitekturu kako bi sepružile pametne i kvalitetne gradske usluge, a svaki od tih slojeva postavljen je za postizanje određenog cilja.[185] Prvi sloj je percepcijski koji upravlja interakcijom korisnika i prikupljanjem podataka na pametnim uređajima. Dugim riječima, u ovom sloju korisnik obavlja autentifikaciju. Drugi sloj odnosi se na implementaciju mrežnog protokola za povezivanje spomenutih uređaja, a posljednji, aplikacijski sloj, ima svrhu pružiti personalizirane usluge korisnicima. Ovaj posljednji sloj u pametnom gradu može sadržavati različite skupine aplikacija te se mogu kategorizirati na sljedeći način - aplikacije namijenjene zdravstvenim ustanovama, mobilnosti, komunalnoj infrastrukturi, gospodarstvu te Vladi. Uzimajući u obzir navedene primjere, važno je istaknuti najvažnije mogućnosti, odnosno prednosti multimodalne autentifikacije korisnika. S jedne strane, multimodalne autentifikacije imaju nižu stopu lažnog prihvaćanja *(eng. false acceptance rate)* i odbijanja *(eng. false rejection rate)*. To se događa jer ovakvi sustavi funkcioniraju s dvije vrste biometrije pa zato imaju i veću točnost od promatranja samo jedne biometrijske karakteristike. Osim toga, kao druga prednost može se izdvojiti veća razina sigurnosti, jer je hakerima tako teže lažirati dvije biometrijske karakteristike nego samo jednu.[186] Fleksibilnost je iduća značajka, a izdvaja se upravo zbog toga što se sustav lakše može boriti sa šumovima (bukom) u podacima. Primjerice, ako se korisnikov glas promijeni zbog bolesti ili je ozljeđena površina prsta koja se koristila kao otisak. Na taj način druga biometrijska karakteristika kompenzira, odnosno može "zamijeniti" prvu. S druge strane, multimodalne autentifikacije su vrlo skupe. Troškovi se mogu odnositi na sam sustav, njegovu izdržljivost, redovito održavanje te na prostor za pohranu biometrijske baze podataka.[187] Osim toga, na to utječe još i korisnikova okolina. Primjerice, na samu točnost prepoznavanja lica korisnika utječe osvjetljenje, poza, izraz lica te mogući šum u

[184] Usp. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm.. URL: https://www.nature.com/articles/s41598-021-04652-3 (2023-02-14)

[185] Usp. Arun Ross, Sudipta Banerjee, Anurag Chowdhury. Security in smart cities: A brief review of digital forensic schemes for biometric data, Pattern Recognition Letters,Volume 138, 2020, Pages 346-354. URL: https://doi.org/10.1016/j.patrec.2020.07.009. (2023-04-24)

[186] Usp. Multimodal Biometrics: A Better Security System? . URL: https://crestresearch.ac.uk/resources/multimodal-biometrics-a-better-security-system/ (2023-02-14)

[187] Isto.

podacima. Buka iz okoliša može itekako utjecati na bilo koju biometriju koja se tada mjeri. [188] Također, verifikacija se može pokazati kao nedostatak jer korisnici mogu zapeti u njezinim procesima. Neki multimodalni procesi verifikacije su duži, no u suštini funkcioniraju isto.[189] Poznavanje korištenja biometrijskih tehnologija za neke korisnike predstavlja određenu razinu straha ili nesigurnosti te iziskuje više znanja i strpljenja, tako da je to pitanje individualnog karaktera.

5.2. Autentifikacija korisnika bez lozinke

Autentikacija bez lozinke predstavlja drugi trend, a odnosi se na metodu provjere korisnika kako bi se omogućio pristup aplikaciji ili drugom sustavu bez unosa lozinke ili odgovaranja na sigurnosna pitanja.[190] Umjesto toga, korisnik pruža neki drugi oblik dokaza kao što je otisak prsta ili pak kod putem tokena. Provjera bez lozinke često se koristi u kombinaciji s rješenjima za provjeru autentifikacije s više faktora *(eng. Multi-Factor Authentication)* i jedinstvenom prijavom kako bi se poboljšalo korisničko iskustvo, sigurnosti i smanjili troškovi i složenost izvođenja.[191] Današnji se korisnici oslanjaju na širok izbor aplikacija za obavljanje svojih poslova tako da su često prisiljeni pamtiti i pratiti niz lozinki koje se lako zaborave.[192] Preopterećeni time, mnogi korisnici koriste riskantne prečace kao što je korištenje iste lozinke za sve aplikacije ili upotreba slabih lozinki. Ugrožavajući pritom svoje vjerodajnice i korisnički račun, dovodi se u opasnost čitav informacijski sustav.[193] Da bi se to izbjeglo, autentifikacija bez lozinki predstavlja dobru ideju. Osim što smanjuje postotak kiberenetičkih napada, ona poboljšava korisničko iskustvo, pritom eliminirajući zamor pamćenja velikog broja lozinki.[194] Ovdje ne postoje lozinke koje je potrebno zapamtiti niti sigurnosna pitanja na koje je potrebno odgovoriti. Na ovaj način svaki korisnik može vrlo jednostavno pristupiti svojim aplikacijama koristeći druge metode autentifikacije kao što su tokeni, FIDO2 ključevi otisak prsta, prepoznavanje mrežnice, glasa ili lica.[195] Postoje brojni primjeri za to, a neki od njih su MiPass. Ovu biometrijsku tehnologiju razvila je tvrtka Mitek System, a omogućuje pristup korisnicima svojim računima i to pomoću snimanja selfija, izgovaranja određenih fraza i sl.[196] Također, MiPass ima mogućnost ugradnje u druge aplikacije te da njihov multimodalni biometrijski pristup poboljšava sigurnost u usporedbi

[188] Isto.
[189] Isto.
[190] Usp. What is Passwordless Authetification? . URL: https://www.cyberark.com/what-is/passwordless-authentication/ (2023-02-15)
[191] Isto.
[192] Isto.
[193] Isto.
[194] Isto.
[195] Isto.
[196] Isto.

sa jednomodalnim biometrijskim sustavima kao što je prepoznavanje lica.[197] Osim toga, algoritmi ove tehnologije razvijeni su i testirani na uravnoteženim skupovima podataka s ciljem smanjivanja bilo kakve pristranosti.[198] Na ovaj način se biometrijski podaci mogu kompromitirati ili dijeliti među korisnicima. Mitek je izvjestio kako primjena biometrije može pomoći bankama i njihovim klijentima, ali da svejedno postoji nesigurnost i manjak povjerenja koji proizvode loše korisničko iskustvo.[199] Također, Experian istraživanje izvjestilo je kako 82% britanskih potrošača može vjerovati bihevioralnoj biometriji u smislu sprječavanja prijevara, dok 55% potrošača smatra kako bi uporaba bihevioralne biometrije stvorila veće povjerenje u svakom poduzeću.[200] Sve to upućuje na činjenicu kako i dalje postoji jaz u povjerenju u tehnologiju te da je potrebno više educirati korisnike po pitanju naprednih tehnika korištenja biometrije i umjetne inteligencije.[201]

5.3. Jača integracija oblaka

Usponu biometrije svjedočit će također i tehnologije u oblaku, prema riječima Alcatraza i Geneteca, vodećih tvrtki koje svoje poslovanje temelje na umjetnoj inteligenciji. Razlog zašto ovetehnologije koriste biometriju jest taj da postojeća infrastruktura može podržati dovoljna radna opterećenja i učiniti postojeće uređaje kompatibilnima s oblakom pa samim time i omogućiti centralizirani pristup sustavima i njihovim podacima.[202] Također, Aware, svjetski poznata tvrtka koja proizvodi bioemetrijske tehnologije, navodi kako se predviđa da će globalno tržište biometrije kao usluge porasti za 16% godišnje u 2020-ima te da će do 2030. godine dosegnuti prihod od 10,4 milijarde dolara.[203] Korištenje biometrije s tehnologijama u oblaku omogućuje ne samo korištenje prilagodljivih resursa kao što su pohrana, mreže, poslužitelji, već i usluge te raznih aplikacija na zahtjev, bez napora i s bilo koje lokacije korisnika.[204] Mnoge tvrtke posljednjih godina nastoje migrirati i integrirati svoje sustave upravljanja upravo biometrijskom identifikacijom u oblak, a razlog su višestruke prednosti koje platforme u oblaku mogu pružiti.[205] Brojni su primjeri biometrije kao usluge *(eng. Biometrics as a Service = BaaS)*, a nude ju BioID,

---

[197] Isto.
[198] Isto.
[199] Usp. Consumer trust in banks is mixed. Behavioral biometrics can help, face less so | Biometric Updat. URL: https://www.biometricupdate.com/202210/consumer-trust-in-banks-is-mixed-behavioral-biometrics-can-help-face-less-so (2023-02-15)
[200] Isto.
[201] Isto.
[202] Usp. Biometrics trends for 2023: multimodal and MFA to grow alongside privacy regulations | Biometric Update. URL: https://www.biometricupdate.com/202212/biometrics-trends-for-2023-multimodal-and-mfa-to-grow-alongside-privacy-regulations (2023-02-15)
[203] Usp. Rise of Biometrics in the Cloud. URL: https://www.aware.com/blog-biometrics-in-the-cloud/ (2023-02-15)
[204] Usp. Cloud-Base Biometric, Its Advantages, And How It Works. URL: https://www.m2sys.com/blog/biometric-software/cloud-based-biometrics-solution-cloudabis/ (2023-02-15)

[205] Isto.

Animetrics, Aware i Iritech tvrtke. Ova tehnologija omogućuje organizacijama svih vrsta – od vlada do telekomunikacijskih kompanija da brzo implementiraju i počnu koristiti biometrijsku tehnologiju u svojim svakodnevnim poslovnim aktivnostima.[206] No, kako zapravo funkcionira biometrija u oblaku? Tvrtka Aware implementirala je biometrijsku platformu u oblaku koja ima sve funkcije potrebne za integraciju prepoznavanja lica, skeniranja otiska prsta i drugih procesa biometrijske identifikacije koje su nužne za identifikaciju zaposlenih.[207] BaaS rješenje ove tvrtke isporučuje se putem modela pretplate, odnosno softverske licence koja se temelji na poslužitelju, a dostupno je putem web preglednika.[208] Prva prednost biometrije u oblaku je ta što se organizaciji omogućuje pretraživanje i upis bez ikakvog stvaranja sustava iz nule, što znači da upravljanje podacima također ne mora obavljat organizacija, već jednostavno BaaS. Samim time, proces upisivanja zaposlenih odvija se na način da se pokrene internetski preglednik na računalu koji je povezan s biometrijskim softverom (npr. za za otisak prsta). Nakon tog upisa, potvrđuje seidentitet ljudi putem internetske veze s bazama podataka koje sadrže biometrijske podatke. Prema tome, ovi navedeni biometrijski procesi neovisni su o hardveru. Njihova sigurnost je u oblaku, ane na uređaju.[209] Važno je također, obratiti pozornost i na privatnost podataka, jer oni ovise o tvrtki koja ih prikuplja i operativnom okruženju.[210] Privatnost se svodi zapravo na način na koji sekoristi, na tvrtku te na propise i zakone koji se moraju pridržavati. Svi pružatelji usluga ovakvog tipa trebali bi biti u skladu s certifikatima kao što su ISO 27001 i 27701 te redovito obavljati revidiranje. Osim toga, važno je postići što bolju uključivost, odnosno doseći što više publike. Korištenjem biometrijskog softvera u oblaku kao što je iProov osigurava se da korisnici dobiju pristup uslugama online, čak i ako možda nemaju pristup računalu ili pametnom telefonu. Na taj način se gradi povjerenje, ali i sigurnost među korisnicima i biometrijske tehnologije.

5.4. Kvantna biometrija

Kvantna biometrija predstavlja integraciju biometrije s kvantnim računarstvom. Integracija se odvija zahvaljujući kvantnoj komunikaciji, odnosno prijenosu informacija olakšane kvantno mehaničkim sustavima. Kvantno računalstvo definira se kao područje računalne znanosti koje se usmjerava na razvoj tehnologija temeljenih na principima kvantne teorije i kao takvo koristi jedinstvena ponašanja kvantne fizike s ciljem rješavanja problema koji su previše složeni za

[206] Usp. What is Biometrics as a Service? Benefits and Use Cases - Aware. URL: https://www.aware.com/blog-biometrics-as-a-service-baas/ (2023-02-16)
[207] Isto.
[208] Isto.
[209] Usp. Cloud Biometric Authentication vs On Device Biometrics Explained | iProov. URL: https://www.iproov.com/blog/cloud-biometrics-vs-on-device-difference (2023-02-16)
[210] Isto.

klasično računalstvo.[211] Kvantna računala za razliku od klasičnih računaju s kubitima, čija vrijednost istovremeno može biti 0 i 1. Ovo se razlikuje od konvencionalnog računala, čija snaga raste izravno, odnosno proporcionalno broju tranzistora.[212] Drugim riječima, snaga kvantnih računala raste eksponencijalno pa su zato izvrstan primjer za rješavanje ekstremno zahtjevnih zadataka kao što su faktorizacije i simulacije u kemiji. Prema stručnoj publikaciji The Quantum Insider, postoji više od 600 tvrtki i više od 30 nacionalnih laboratorija i vladinih agencija diljem svijeta koji razvijaju tehnologije kvantnog računarstva.[213] Reprezentativni primjer biometrije ovakve vrste jest kvantni otisak prsta, a predstavlja novi pristup učinkovitom kodiranju i prijenosu informacija. Navedeni koncept koristan je u komunikaciji između mikroskopskih mreža ili primjerice između različitih lokacija na računalnom čipu.[214] Ovakav prijenos informacija proučavao je Li Qian, profesor na Odsjeku za elektrotehniku i računalno inženjerstvo na Sveučilištu Torontu. Navodeći kako je ovo zanimljiv tip kvantnog komuniciranja, profesor opisuje da kvantni otisak prsta funkcionira na sljedeći način: postoje dva korisnika - Alice i Bob, koji žele utvrditi jesu li njihove datoteke identične jedna drugoj. Moguće je da jedan od njih dvojejednostavno pošalje svoju datoteku drugome i provjeri, a to se postiže slanjem samo malene informacije - kvantnim otiskom prsta.[215] Postoji i treća strana, koja se često u literaturi zamišlja kao sudac po imenu Charlie i on bez izravnog pristupa datotekama može usporediti otiske prstiju Alice i Boba te na taj način utvrditi jesu li njihove datoteke identične ili ne.[216] Konvencionalni otisak prsta datoteke od samo jednog megabajta predstavlja veličinu digitalne fotografije te bi inače zahtijevao prijenos oko 300 bajtova. Za usporedbu, nova metoda kvantnog otiska zahtijevala bi samo oko tri bajta, drugim riječima - podataka u vrijednosti od tri slova.[217] Prema tome, ovaj novi, neobični pristup kodiranju informacija dramatično smanjuje ne samo vrijeme,već energiju i količinu potrebnih podataka u usporedbi s onima koje zahtijevaju klasične metode komuniciranja.[218] Osim ovih prednosti, postoje i određene implikacije na koje treba obratitipozornost. Potencijalni problem može nastati ako se koncept proširi na višu razinu, odnosno ako postoji više korisnika na mreži, no uzimajući u obzir kako je kvantna komunikacija relativno novapraksa, potreba su svakako daljnja istraživanja za rješavanje kompleksnijih zadataka.[219]

---

[211] Usp. What is Quantum Computing? | Definition from techTarget. URL: https://www.techtarget.com/whatis/definition/quantum-computing (2023-02-16)
[212] Usp. Quantum Computing Vs. Classical Computing In One Graphic - CB Insights Research. URL: https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/ (2023-02-16)
[213] Usp. What is Quantum Computing? Nav. Dj.
[214] Isto.
[215] Usp. Decoding the quantum fingerprint - The Varsity. URL: https://thevarsity.ca/2021/09/19/quantum-fingerprint-explained/ (2023-02-16)
[216] Isto.
[217] Isto.
[218] Isto.
[219] Isto.

5.5. Biometrija u metaverzumu

Još jedno područje koje dotiče biometrija jest metaverzum. Metaverzum se, jednostavno rečeno, odnosi na Web 3.0 - simulirano trodimenzionalno digitalno okruženje u kojemu korisnici mogu ostvariti impresivno iskustvo i time dobiti dojam da je to stvaran svijet.[220] Tehnički gledano, metaverzum povezuje više dijelova uključujući pritom virtualnu stvarnost, prišireni stvarnost, mješovitu stvarnost te blockchain. Sve veća upotreba metaverzuma postala je uobičajena osobito za vrijeme pandemije jer su tvrtke na takav način učinkovito promovirale svoje ponude i usluge.[221] No, kakva je uloga biometrije u tome metaverzumu? Biometrija može funkcionirati uz pomoć blockchaina, odnosno kriptovaluta. Kriptovaluta prema poznatoj tvrtci IBM, označava nepromjenjivu knjigu čiji je cilj olakšati proces bilježenja transakcija i praćenja imovine u poslovnoj mreži.[222] Imovina kao takva može biti materijalna (kuća, automobil) ili nematerijalna (intelektualno vlasništvo, autorska prava). Prema tome, sve što ima vrijednost može se pratiti i trgovati na blockchain mreži.[223] Razlog zašto je blockhain vrlo koristan je taj što sadrži transparentne informacije koje su pohranjene u tzv. nepromjenjivoj knjizi pa na taj način daje uvid u svaku transakciju olakšavajaući praćenje narudžbi, proces plaćanja, proizvodnje proizvodaitd.[224] No, kakvu ulogu ima biometrija u cjelokupnom metaverzumu? S obzirom da se interakcijau virtualnoj stvarnosti postiže uglavnom putem slušalica i naočala, često se interakcija može postići i preko dodatnih senzora na tijelu. Tako se prikupljaju podaci o korisniku koji prate njegovhod ili primjerice pokreti očiju. Biometrija u metaverzumu također nudi mogućnost skeniranja lica ili fotografije što u jednakoj mjeri stvara i prednost, kao odlična mogućnost identifikacije korisnika, ali i nedostatak, kao vid prijevare. Često korisnici na svojim pametnim telefonima znaju izvršiti 3D skeniranje svoga lica kako bi napravili personalizirani avatar ne razmišljajući o mogućim posljedicama. To govori kako korisnici i dalje nisu osviješteni o mogućim ranjivostima, sustava, koliko god se on činio moćnim. Uzimajući u obzir tu činjenicu, trebalo bi implementirati sučelja koja se kreću dalje od nekih vanjskih senzora.[225] Ako pak takva tehnologija napreduje do više razine, kao što su sučelja u interakciji s mozgom korisnika, onda bi se mogla stvoriti ponovnonova vrsta biometrije metaverzuma - biometrija s markerima koji su specifični za mozak, a isto

[220] Usp. The role of biometrics in the metaverse. URL: https://cointelegraph.com/metaverse-for-beginners/the-role-of-biometrics-in-the-metaverse (2023-02-16)
[221] Isto.
[222] Usp. What is Blockchain Technology? - IBM Blockchain | IBM. URL: https://www.ibm.com/topics/what-is-blockchain (2023-02-16)
[223] Isto.
[224] Isto.
[225] Usp. Ready for handling Metaverse biometric data? | Biometric Update. URL: https://www.biometricupdate.com/202107/ready-for-handling-metaverse-biometric-data (2023-02-16)

omogućuju provjeru i autentifikaciju korisnika. [226]

[235] Isto.

6. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

6.1. Stanje u svijetu

U Njemačkoj je provedeno istraživanje na temu uvođenja biometrijskih tehnologija, a provela ga je Istražiteljska grupa za biometriju i internetsku sigurnost sa Sveučilišta primijenjenih znanosti u Darmstadtu.[227] Korišteni instrument ovog istraživanja bio je anonimni anketni upitnik koji se sastojao od ukupno 56 pitanja, a sudjelovalo je 140 ispitanika diljem cijele Njemačke.[228] Većina ispitanika je bila između 20 i 29 godina životne dobi, bili su ili studenti ili zaposleni, a po spolu je bilo 90 muškaraca i 50 žena.[229] Sudionici su ispitani koje biometrije poznaju, a najčešći odgovori bili su biometrija otiska prsta, rožnice, lica i glasa. Također, na pitanje „Kako će se razvijati biometrijska tehnologija u budućnosti?“ otprilike 45% sudionika je odgovorilo pozitivno, dok je 30% sudionika „negativno“, a 25% ispitanika ima neutralan pogled na razvitak biometrijske tehnologije.[230] Osim toga, istraživanjem je dokazano da je većina ispitanika dovoljno upoznata s više biometrijskih karakteristika, ali čak 25% ispitanika nikako ne podržava biometriju.[231] Dobiveni rezultati govore da je potrebno podići svijest o korištenju biometrijskih tehnologija u Njemačkoj što bi moglo poboljšati prihvaćanje biometrije.

Za razliku od Njemačke, u Grčkoj se provodilo deskriptivno istraživanje 2022. godine čiji je cilj bio istražiti percepciju studenata na Sveučilištu u Egeju o biometriji i prihvaćanje njezinih tehnologija, pritom uzimajući u obzir njihove sociodemografske karakteristike. Prethodna istraživanja većinom su ispitivala samo različite fizičke i bihevioralne biometrijske karakteristike (primjerice otisak prsta, potpis ili pritisak tipke) te su se na taj način ograničila samo na tehnički dio, ne pružajući tako dovoljno analizu demografskih karakteristika.[232] Od ukupno 17.312 poslanih upitnika, 768 studenata je u potpunosti odgovoreno. Što se tiče spola, sudjelovalo je 279 muških studenata, 480 žena i 6 osoba koje se nisu htjele izjasniti.[233] Postotak ispitanika u dobi od 18 do 22 bio je 54%, od 23 do 30 iznosio je 23%, a postotak dobi od 31 do 45 bio je 17%.[234] Naposljetku, postotak ispitanih u dobi od 46 do 60 iznosio je 6%. Većina (28%) je potvrdila da jena prvoj godini studija, 20% na drugoj godini, 12% na trećoj, 18% na četvrtoj i 12% na petoj, dok je 10% studiralo dulje od pet godina.[235] S ciljem točnijeg ocrtavanja sociodemografskog profila

---

[227] Krupp, A. & Rathgeb, Christian & Busch, Christoph. Social Acceptance of Biometric Technologies in Germany: A Survey. BIOSIG 2013 - Proceedings of the 12th International Conference of the Biometrics Special Interest Group. 1-5. Str. 193.-200.
[228] Isto.
[229] Isto.
[230] Isto.
[231] Isto.
[232] Usp. Angeliki Kitsiou et al. The Role of Users' Demographic and Social Attributes for Accepting Biometric Systems: A Greek Case Study. Future Internet, MDPI, vol. 14(11), 2022. Str. 1-31.
[233] Isto.
[234] Isto.
[235] Isto.

sudionika, od njih se tražilo da navedu svoje zaposlenje status. Također, većina sudionika smatra da su biometrijske tehnologije jednostavne za naučiti i koristiti, kao što su primjerice otisci prstiju i prepoznavanje lica.[236] Međutim, ispitanici u dobi od 18 do 22 godine te od 46 do 60 godina istaknuli su kako osjećaju snažnu zabrinutost zbog mogućnosti kloniranja njihovih biometrijskih podataka.[237] Osim toga, bez obzira na dobnu skupinu, ispitanici su potvrdili da nakon što usluge prikupe njihove biometrijske podatke, njihova privatnost biva automatski narušena. Shodno tome, istraživanje je pružilo vrlo detaljnu analizu sociodemografskog profila korisnika u njegovom prihvaćanju i usvajanju biometrijske tehnologije i može poslužiti kao dobar izvor pomoći za sva buduća istraživanja, koja bi se više trebala usmjeriti na brige korisnika i njihove perspektive prihvaćanja.[238]

Još jedan dobar primjer istraživanja o usvojenosti i prihvaćanju biometrijskih tehnologija odnosi se na istraživanje u New Yorku, Sjedinjenim Američkim Državama. Istraživanje je provedeno 2017. godine te se oslanja u velikom dijelu na prijašnje istraživanje o biometrijskim tehnologijama koje je provelo Pace Univerisity.[239] Cilj ovog istraživanja bio je testirati hipotezu da je stupanj prihvaćanja biometrijske tehnologije veći za korisnike koji su mlađi i obrazovaniji. Također, drugi cilj je bio dati prijedloge kako premostiti postojeće prepreke glede usvajanje tehnologije.[240] Sudjelovalo je ukupno 410 ispitanika te se primjenjivala metodologija kvantitativnog istraživanja, zajedno sa statističkom i numeričkom analizom prikupljenih podataka putem anonimne online ankete. Anketni upitnik je sadržavao ukupno 18 pitanja, raspoređenih prema sljedećima elementima: demografija, prethodno korištenje i upoznatost s biometrijom općenito, lakoća korištenja, uvjerenje i sigurnost, korištenje korisničkog računa i lozinki, trošak kao čimbenik korištenja te briga o privatnosti.[241] Što se tiče spola, 50% ispitanih se identificiralo kao muškarac, a 49% kao žena, dok se 1% ispitanih nije htio izjasniti. Važno je napomenuti da je bila ravnomjerna raspodjela dobi, dakle od 18 do 55 i više godina, pri čemu svaka kategorija čini približno 20%.[242] Razmatrajući rezultate, ukupno 87% ispitanika izjavilo je da je dosad koristilo jednu aplikaciju koja uključuje biometrijske karakteristike autentifikacije ili pak tehnologiju koja može zamijeniti korištenje višestrukih lozinki, korisničkih imena i PIN-ova[243]. Također, rezultati su pokazali da 22% ispitanika smatra trošak kao značajnu prepreku u korištenju jedne

[236] Isto.
[237] Isto.
[238] Isto.
[239] Usp. Fletcher, James et al. A Study of Biometric Security Technology Acceptance and Primary Authentication. URL: http://csis.pace.edu/~ctappert/srd2017/2017PDF/d8.pdf (2023-04-24)
[240] Isto.
[241] Isto.
[242] Isto.
[243] Isto.

biometrijske tehnologije, a tomu potvrđuje i činjenica da je samo 3% ispitanih voljno iz vlastitog džepa spremno platiti 25 dolara ili više. U pogledu sigurnosti, 48% ispitanih je izjavilo da barem djelomično smatra da su biometrijska sigurnosna skeniranja nametljiva ili da narušavaju privatnost korisnika.[244] Ukupno 74% se smatra ranim korisnicima biometrijskih tehnologija, dok je ukupno 60% sudionika izjavilo kako trenutno koristi biometrijsku sigurnosnu značajku. Prema tome, navedeni podaci podupiru spomenutu hipotezu da više obrazovani ispitanici s višim prihodima bolje prihvaćaju korištenje biometrijskih tehnologija pa samim time razvijaju više povjerenja i sigurnosti.

Istraživanje u Indiji provedeno je 2022. godine od strane Instituta za menadžment, zajedno u suradnji sa State Bank institutom u Hyderabadu. Ono što se proučavalo su preferencije korisnika o korištenju bankomata, odnosno načinu autentifikacije - kartično ili beskartično. Sudionici su bili klijenti jedne od najvećih banaka u Indiji, a odabrani instrument istraživanja bio je anonimni anketni upitnik. Upitnik se sastojao od nekoliko grupa pitanja, čiji je cilj bio saznati stavove o percipiranoj korisnosti, lakoći, sigurnosti i povjerenju korisnika banke. Sudjelovalo je ukupno 521 osoba, od njih 32% žena, a 68% muškaraca.[245] Što se tiče dobi ispitanika, 10% bilo je mlađih od 20 godina, 33% od 20 do 40 godina te 49% u dobi od 40 do 60 godina.[246] Čak 82% ispitanih izjavilo je kako više kod korištenja bankomata preferira beskontaktan način autentifikacije, dok je 18% potvrdilo suprotno, odnosno da više voli koristiti kartični način autentifikacije (putem PIN-a)[247]. Na temelju ovih rezultata, jasno je kako zapravo usvajanje bezkartičnog načina autentifikacije utječe na razvoj stavova korisnika o korištenju bankomata u Indiji.

Tehnologija koja obavlja autentifikaciju korisnika putem njegovih vena na dlanu istražena je od strane australskog Deakins Sveučilišta (Deakins University) 2022. godine. Cilj istraživanja bio je istražiti koji su to glavni čimbenici koji utječu na korištenje biometrije vene dlana, oslanjajući se na konstrukte (varijable) Davisovog modela o prihvaćanju tehnologije - percipirana korisnost, namjera ponašanja, stavovi tijekom korištenja, osobna inovativnost, lakoća korištenja, povjerenje, rizik te percipirana ugodnost.[248] U namjeri da se ispitivanje uspješno provede, sudjelovalo je ukupno 100 ispitanika, dok je dobna skupina ispitanika zahvaćala sudionike od 18 do 60 godina.[249] Ispitanici su morali koristiti aparat za kavu koji je imao ugrađen biometrijski

[244] Isto.
[245] Usp. Nambiar, B.K., Bolar, K. Factors influencing customer preference of cardless technology over the card for cash withdrawals: an extended technology acceptance model. *J Financ Serv Mark* **28**, 2022. Str. 58–73. https://doi.org/10.1057/s41264-022-00139-y(2023-04-24)
[246] Isto.
[247] Isto.
[248] Usp. Technology Acceptance Model: A Case Study Of Palm Vein Authentification Technology. URL: https://ieeexplore.ieee.org/abstract/document/9945960 (2023-04-24)

[249] Isto.

sustav za prepoznavanje vena na dlanu te se pomoću njega registrirati.[250] Nakon autentifikacije, svi ispitanici ispunili su anketni upitnik, koji je sadržavao 16 pitanja. Svi podaci modelirani su korištenjem tzv. modeliranja strukturnih jednadžbi *(eng. SEM - Structural Equation Modelling*) s ciljem potvrđivanja odnosa između različitih konstrukata u spomenutom Davisom modelu.[251] Za dublje promatranje navedenih podataka, korišten je IBM-ov softver za statistiku SPSS Statistics te tehnika potvrdne faktorske analize, dok je pouzdanost određenih pokazatelja iz ankete izmjerena pomoću Cronbachove alfa vrijednosti.[252] Istraživanje je otkrilo da bi sve tehnologije koje nude mogućnost autentifikacije vena na dlanu trebale omogućiti jednostavno rukovanje istom te da ona bude korisna svima. Također, pronađeni su statistički dokazi koji pokazuju da percipirana korisnost, percipirani rizik i percipirani užitak predviđa namjeru korisnika da korist navedenu autentifikaciju Palm Vein. No, bez obzira na to, potrebno je još istraživanja kako bi se detaljnije proučili oni izravni i neizravni utjecaji spomenutih varijabli.[253]

Istraživanje u Španjolskoj donosi nešto drugačiju perspektivu. Provodilo se na sveučilištu u Madridu (Madrid Open University), među dvjema grupama studenata - dakle među 100 studenata koji su bili raspoređeni u dvije grupe po 50. Fokus istraživanja je zapravo percepcija studenata o korištenju platforme Smowl koja je integrirana u informacijski sustav Moodle.[254] Smowl se odnosi na biometrijsko rješenje koje koristi određeni algoritam koji može potvrditi i analizirati identitet pojedinca ovisno o njegovim fiziološkim značajkama.[255] Prva grupa studenata je dosad koristila Smowl, dok druga grupa nije tako da je ona testirala Prilikom prve prijave u Moodle, studentima se pojavljuje pitanje na ekranu, odnosno dopuštenje o korištenju web kamere kako bi se mogla uspostaviti autentifikacija.[256] Nakon pritiska na gumb "Dopusti", aplikacija Smowl tada prikazuje što je uhvaćeno web kamerom i pritom prikazuje crvenom bojom da je kamera uspješno aktivirana i predviđena za snimanje tri fotografije.[257] Instrument istraživanja bio je test, oblikovan kao Likertova ljestvica u rasponu mogućih odgovora od "Potpuno se ne slažem"
(1) do "U potpunosti se slažem" (7). Cilj testa bio je izmjeriti stavove te saznati percepciju studenata u vezi korištenja Smowla u online učenju i nastavi.[258] Pitanja su se odnosila na prikladnost platforme u akademsko okruženje, njegovu implementaciju te davanje generalnog

[250] Isto.
[251] Isto.
[252] Isto.
[253] Isto.
[254] Usp. Guillen-Gamez, Francisco D., et al. Analysis of the perception of students about biometric identification. *International Journal of Web-Based Learning and Teaching Technologies*, vol. 10, no. 3, 2015. URL: https://www.researchgate.net/publication/276271985_Analysis_of_the_Perception_of_Students_about_Biometric_Identification (2023-04-24)
[255] Isto.
[256] Isto.
[257] Isto.
[258] Isto.

mišljenja o korištenju[259]. Rezultati su pokazali kako oni ispitanici koji su testirali softver prvi puta zapravo vrlo cijene implementaciju ove tehnologije te da ovo istraživanje može pomoći u utvrđivanju hoće li ovakva tehnologija moći zamijeniti ispite uživo te hoće li studenti moći svoje rezultati ostvariti puno bolje ili ne.[260]

Proučavanje prihvaćenosti tehnologije odvijalo se i u Skandinaviji, odnosno u Finskoj te u južnoameričkoj državi Brazil. Iako su kulturno vrlo različite zemlje, stupanj prihvaćanja tehnologije zaista je interesantan i u određenim aspektima poprilično jednak. Istraživanja su proučavana i iz perspektive Hofstedeovih kulturnih dimenzija. Dimenzije je razvio Geert Hofstede 60-ih godina 20. stoljeća te se odnose na okvir (model) koji se koristi s ciljem razumijevanja kulturnih razlika među određenim zemljama.[261] Postoji 6 ključnih dimenzija - distanca moći, izbjegavanje neizvjesnosti, individualizam-kolektivizam, muškost-ženstvenost, kratkoročna-dugoročna orijentacija te indulgencija.[262] Na temelju ovih dimenzija, bolje se razumijevaju bonton i komunikacija među kulturama u raznim područjima pa tako i po pitanju korištenja tehnologije. Instrument ovog istraživanja bio je online anketni upitnik, a uzorak su bili studenti dvaju sveučilišta u Finskoj i Brazilu.[263] Točnije rečeno, prikupljali su se slučajni uzorci iz studentske populacije, kako bi se minimizirala pristranost. Anketni upitnik kreiran je pomoću softvera Webropol, kojeg je ukupno 815 studenata otvorilo, 563 studenata ga je nastavilo odgovarati te ih je 312 ispunilo u potpunosti.[264] Prema tome, ukupno odgovora s finskog sveučilišta bilo je 150, dok je s brazilskog bilo 152.[265] Nakon pitanja o demografiji, koristeći se Likertovom skalom, preostala pitanja su zahtijevala od ispitanika da se izjasne kako percipiraju lakoću i korisnost biometrijske tehnologije, njezinu sigurnost te moguću invazivnost.[266] Rezultati su pokazali kako finski studenti prije ispunjavanja anketnog upitnika nisu bili upoznati s pojmom biometrije uopće, tako da su tek nakon ispunjavanja shvatili što biometrijske tehnologije zapravo uključuju i kakve sve metode autentifikacije postoje.[267] S druge pak strane, brazilski studenti imali su doticaja s korištenjem biometrije te ju smatrala korisnijom metodom autentifikacije ukoliko je osigurana veća razina sigurnosti.[268]

---

[259] Isto.
[260] Isto.
[261] Usp. Hofstede's Cultural Dimensions Theory & Examples. URL: https://www.simplypsychology.org/hofstedes-cultural-dimensions-theory.html (2023-04-30)
[262] Isto.
[263] Ljiljander, Akseli. ATTITUDES TOWARDS BIOMETRIC AUTHENTICATION TECHNOLOGIES BETWEEN CULTURES: ACCEPTANCE IN FINLAND AND BRAZIL. URL: https://jyx.jyu.fi/bitstream/handle/123456789/66405/1/URN%3ANBN%3Afi%3Ajyu-201911154909.pdf (2023-04-30)
[264] Isto.
[265] Isto.
[266] Isto.
[267] Isto.
[268] Isto.

6.2. Stanje u Republici Hrvatskoj

U Republici Hrvatskoj postoji malo istraživanja o biometriji te su provedena uglavnom sa stajališta kriminalistike i nacionalne sigurnosti, a opisuju primjerice uvođenje raznih biometrijskih tehnologija poput putnih isprava.[269] Do sada nije provedeno istraživanje koje bi istražilo isključivo percepciju studenata o biometriji i tehnologijama takve vrste, međutim postoji samo jedno istraživanje koje je imalo za cilj istražiti kontrolu pristupu, metode autentifikacije i percepciju biometrijske tehnologije u društvu, tj. mladih u dobi od 18 do 30 godina.[270] Metodom online anketnog upitnika prikupljeno je 203 odgovora, koji su pokazali znatno visoku razinu poznavanja biometrije u mladeži.[271] Prema podacima, čak preko 86% ispitanih se dosada susrelo s raznim biometrijskim tehnologijama, a od najpoznatijih metoda autentifikacije ispitanici koriste otisak prsta,šarenicu oka, lice i glas.[272] Također, promatrajući dobivene podatke, najviše povjerenja pruža otisak prsta jer se najlakše prihvaća među ljudima.[273] Bez obzira na tu dostatnu razinu povjerenja, među mladima svejedno vlada određena razina opreza i skeptičnosti prema biometrijskoj tehnologiji, koja bi se svakako trebala pratiti, a društvo što više informirati i educirati o mogućim rizicima.[274]

[269] Usp. Nađ, Stjepan. Metode autentikacije korisnika : prednosti i izazovi biometrijske tehnologije. Master's thesis, University of Zagreb, Faculty of Economics and Business, 2022. https://urn.nsk.hr/urn:nbn:hr:148:937102 (2023-04-24)
[270] Isto.
[271] Isto.
[272] Isto.
[273] Isto.
[274] Isto.

7. PERCEPCIJA I STAVOVI STUDENATA PREMA BIOMETRIJSKOJ TEHNOLOGIJI

7.1. Cilj i istraživačka pitanja

Cilj ovoga istraživanja bio je ispitati percepciju i stavove studenata Filozofskog fakulteta u Osijeku, Ekonomskog fakulteta u Osijeku, Fakulteta elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, Filozofskog fakulteta u Zagrebu te Filozofskog fakulteta Sveučilišta u Mostaru o korištenju biometrijskih tehnologija. Istraživačka pitanja bila su sljedeća:

1) Jesu li studenti upoznati s pojmom biometrija i jesu li je dosad koristili?
2) Razlikuju li studenti osnovne vrste biometrijskih karakteristika?
3) Kako studenti percipiraju lakoću korištenja i razvoj biometrijske tehnologije u budućnosti?
4) Što smatraju najvećim izazovom biometrijske tehnologije?
5) Smatraju li studenti biometriju invazivnom te imaju li studenti povjerenja u biometrijsku tehnologiju?

7.2. Metodologija

Istraživanje se provodilo u siječnju 2023. godine te su u njemu bili uključeni studenti sljedećih fakulteta - Filozofski fakultet Osijek, Ekonomski fakultet Osijek, Fakultet elektrotehnike,računarstva i informacijskih tehnologija, Filozofski fakultet Zagreb, Filozofski fakultet Zadar te Filozofski fakultet Sveučilišta u Mostaru. Za potrebe istraživanja u Google Forms-u kreiran je upitnik koji je preko društvenih mreža poslan studentima navedenih fakulteta.

Instrument ovog istraživanja bio je online upitnik, sastavljen od 25 pitanja, koji su bili jednostrukog i višestrukog tipa odgovora. U prvoj skupini pitanja ispitanici su odgovorili na pitanje spola, dobi, fakulteta kojeg trenutno pohađaju i trenutne godine studiranja. Druga skupina pitanja je veća te se njome pokušalo saznati jesu li studenti upoznati s pojmom biometrije, koje su vrste biometrijskih karakteristika koristili dosada i u koje svrhe. Također, željelo se saznati razlikuju li studenti određene vrste biometrijskih metoda, što smatraju idealnom biometrijskom karakteristikom, je li biometrija nužna i olakšava li svakodnevni život te kako percipiraju razvoj biometrijskih tehnologija u budućnosti. Posljednjom, trećom skupinom pitanja, nastojalo se odgovoriti posjeduju li studenti uređaj koji ima mogućnost koristiti bilo koji tip biometrijske karakteristike (primjerice otisak prsta), kako usvajaju nove tehnologije, koliko trenutno zaporki koriste i kakve su one (iste/različite za sve korisničke račune ili mješovite). Također, u trećoj skupini pitanja, ispitanici su trebali navesti bi li

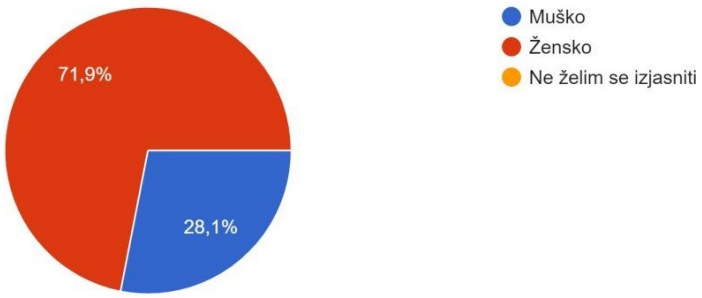
koristili određenu biometrijsku karakteristiku u zamjenu za primjerice PIN ili lozinku te koje su prednosti, nedostaci i izazovi korištenja biometrijske tehnologije. U konačnici, posljednja četiri pitanja trebala su pomoći ustanoviti smatraju li studenti biometrijsku tehnologiju invazivnom, kako percipiraju lakoću njezina korištenja, u koja područja bi ovu tehnologiju trebalo još implementirati te naposljetku, saznati imaju li studenti uopće povjerenja u tehnologiju takve vrste.

7.3. Rezultati

Demografski podaci

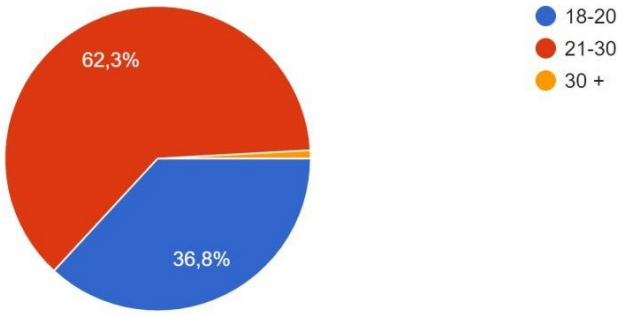
U istraživanju je sudjelovalo ukupno 114 ispitanika, no uzimajući u obzir da jedan ispitanik nije odgovorio na pitanje fakulteta na kojem studira, može se reći kako zapravo postoji 113 valjanih odgovora.

Što se tiče spola, anketni upitnik ispunile su ukupno 82 ženske osobe, što označava 71,9%, dok je muških osoba ispunilo ukupno 32, odnosno 28,1%. Podaci su vidljivi na Grafičkom prikazu 1.



Grafički prikaz 1. Zastupljenost studenata prema spolu

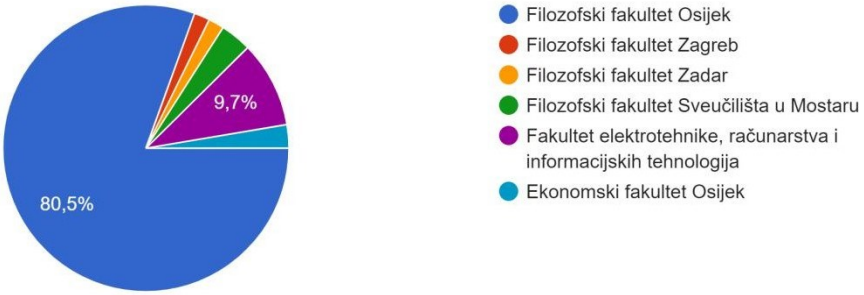
Ispitanici su bili podijeljeni u tri skupine - prva je označavala dob 18-20 godina, druga skupina 21- 30 godina i treća skupina ispitanike starije od 30 godina. Studenata u dobi od 18-20 godina bilo je ukupno 42 (36,8%), dok je studenata u dobi od 21-30 godina bilo više, odnosno 71 student (62,3%). Naposljetku, samo jedan student imao je više od 30 godina (0,09%). Podaci u vidljivi na Grafičkom prikazu 2.



Grafički prikaz 2. Dob ispitanika

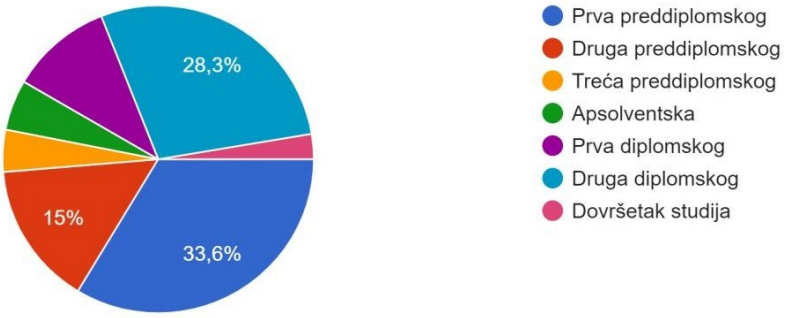
S Filozofskog fakulteta online anketni upitnik ispunilo je ukupno 95 studenata (83,33%), s Ekonomskog fakulteta 3 (2,6%), dok je s Fakulteta elektrotehnike, računarstva i informacijskih tehnologija ispunilo ukupno 11 studenata (9,6%). S Filozofskog fakulteta u Zagrebu ispunilo je ukupno 2 studenta (1,8%), sa Filozofskog fakulteta u Zadru isto 2 studenta (1,8%) te sa Filozofskog fakulteta u Mostaru 4 studenta (2,6%). Podaci su prikazani na Grafičkom prikazu 3.

.



Grafički prikaz 3. Odaziv studenata s obzirom na fakultete koje pohađaju

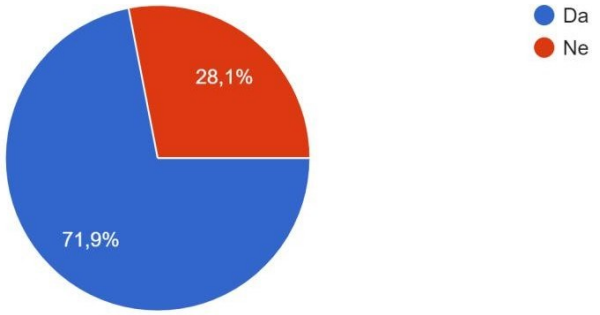
Što se tiče razine studiranja, svi podaci prikazani su na Grafičkom prikazu 4. Studenata s preddiplomskog studija bilo je ukupno 38 (33,6%), s druge godine preddiplomskog studija bilo je 17 (15%), a s treće godine preddiplomskog bilo je ukupno 5 studenata (4,4%). Ukupno 6 ispitanika (5,3%) su studenti apsolventi, dok je s dovršetka studija sudjelovalo ukupno 3 studenta (2,7%). S prve godine diplomskog studija sudjelovalo je ukupno 12 (10,6%) studenata, dok je s druge godine sudjelovalo ukupno 32 (28,3%).



Grafički prikaz 4. Razina studija studenata

Znanje o biometriji

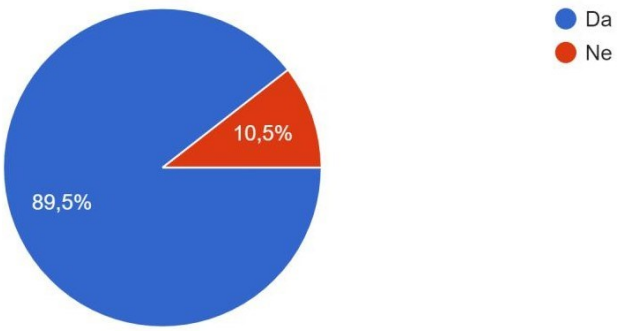
Na pitanje "*Znate li da je biometrija automatska identifikacija osobe bazirana na njezinoj fizičkoj i/ili ponašajnoj karakteristici?"* ukupno 82 (71,9%) ispitanih odgovorilo je "DA", dok je ukupno 32 (28,1%) studenata odgovorilo "NE", što upućuje kako im je pojam biometrije potpuno stran. Podaci su vidljivi na Grafičkom prikazu 5.



Grafički prikaz 5. Znanje studenata o pojmu biometrija

Korištenje biometrije

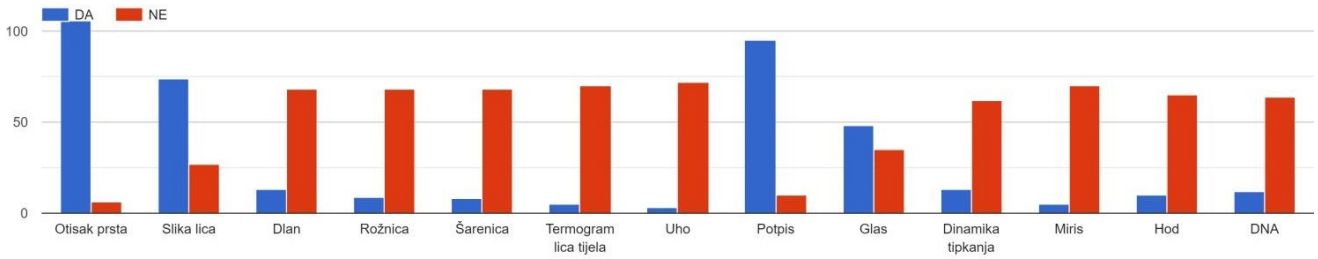
Na pitanje *"Jeste li dosada koristili biometriju?"* ukupno 102 studenata (89,5%) odgovorilo je da je dosada koristilo biometriju, dok je 12 studenata (10,5%) odgovorilo kako biometriju nije uopće koristilo. Podaci su vidljivi na Grafičkom prikazu 6.



Grafički prikaz 6. Korištenje biometrije općenito

Korištenje različitih biometrijskih karakteristika

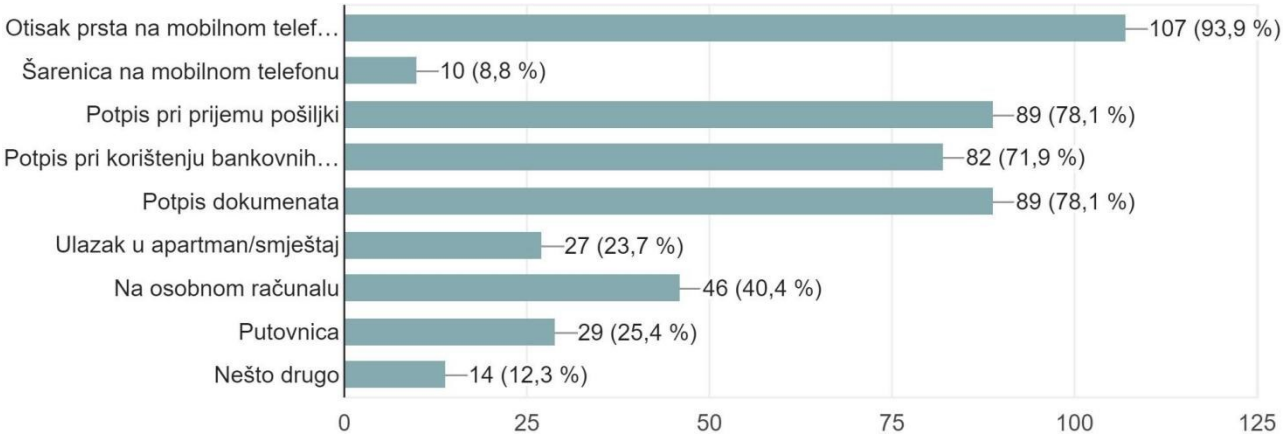
Anketni upitnik zatim je tražio od studenata da se izjasnu koje su vrste biometrijskih karakteristika dosad koristili. Bilo je ponuđeno ukupno 13 biometrijskih karakteristika, a rezultati su vidljivi na Grafičkom prikazu 7. Najveći postotak korištenja ima biometrijska karakteristika otisak prsta kojeg je koristilo ukupno 106 studenata (93%), dok potpis zauzima drugo mjesto i koristilo ga je dosad ukupno 95 studenata (83,3%). Sliku lica koristilo je ukupno 74 ispitanih (65%), dlan 13 studenata (11,4%), rožnicu 9 ispitanih (8%), šarenicu 8 studenata (7%), a termogram lica tijela čak 5 ispitanih (4,3%). Biometrijsku karakteristiku uho dosad je koristilo 3 studenta (2,6%), glas 48 ispitanih (42,1%), dinamiku tipkanja 13 studenata (11,4%), dok je miris koristilo ukupno 5 ispitanih (4,4%). Ukupno 10 studenata (8,7%) složilo se kako je dosad koristilo hod kao biometrijsku karakteristiku, dok je DNA koristilo 12 ispitanih (10,5%).



Grafički prikaz 7. Korištenje različitih biometrijskih karakteristika

Svrha korištenja biometrijskih tehnologija

Na pitanje *"U koju svrhu ste dosada koristili biometrijsku tehnologiju u svakodnevnom životu?"* ispitanici su mogli označiti više odgovora te su podaci prikazani ispod na Grafičkom prikazu 8.

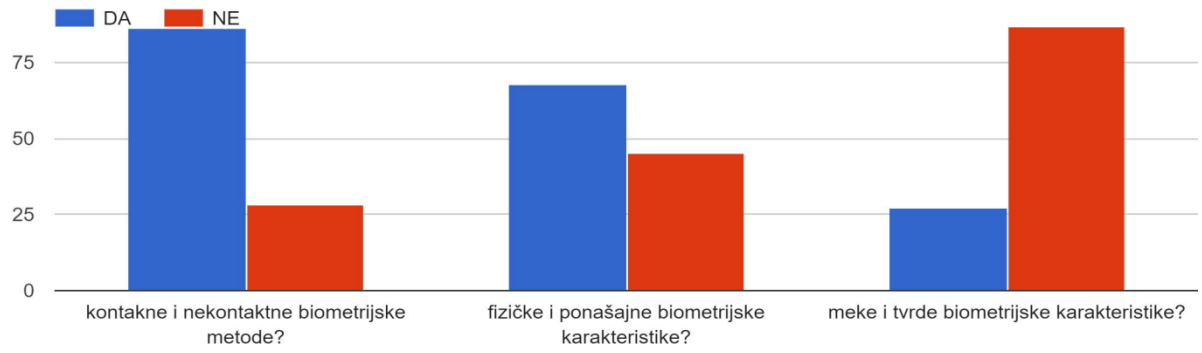


Grafički prikaz 8. Razlog korištenja biometrijskih tehnologija

Otisak prsta ponovno koristi najveći broj ispitanih, dakle ukupno 107 studenata (93,9%), a koristi se prilikom otključavanja i zaključavanja mobilnog telefona. Šarenica se kao biometrijska karakteristika također koristi prilikom autentifikacije 10 studenata na mobilnom telefonu te ukupni postotak iznosi 8,8%. Nadalje, u svakodnevici 89 studenata koristio je svoj potpis pri prijamu pošiljki te taj postotak iznosi ukupno 78,1%. Osim toga, svoj potpis je 82 studenta koristilo kod bankovnih usluga tako da taj postotak iznosi 71,9%. Također, potpis od strane 89 studenata koristio se i u druge svrhe kao što je potpisivanje službenih dokumenata, što označava postotak od 78,1%. Ulazak u apartman/smještaj bila je svrha 27 studenata, odnosno 23,7% njih, dok je svrha korištenja na osobnom računalu bila od strane 46 studenta (40,4%). Naposljetku, u svrhu putovnice u svakodnevnom životu koristilo je ukupno 29 studenata (25,4%). U neke druge svrhe biometrijsku tehnologiju koristilo je ukupno 14 ispitanih, odnosno 12,3%.

Poznavanje razlika biometrijskih karakteristika i metoda

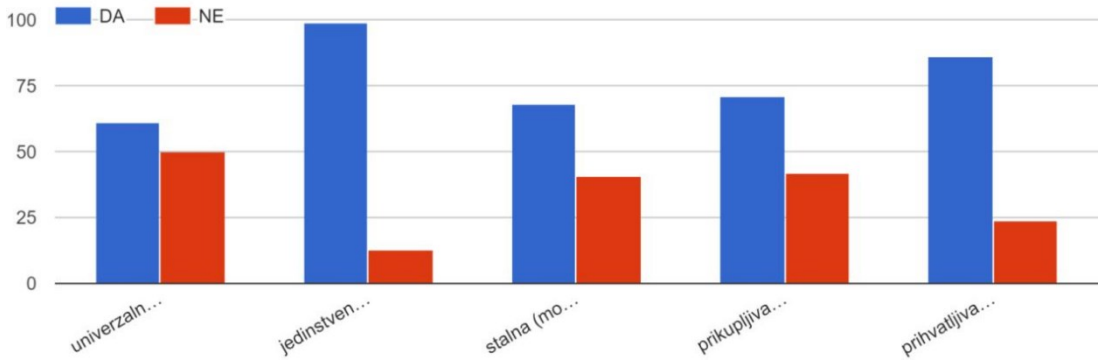
Na pitanje *"Razlikujete li kontaktne i nekontaktne biometrijske metode?"* 86 studenata (75,4%) odgovorilo je da razlikuje, dok se 28 studenata (24,5%) izjasnilo da ne razlikuje. Također, na pitanje *"Razlikujete li fizičke i ponašajne karakteristike?"* odgovorilo je ukupno 68 ispitanih (59,6%) da razlikuje, dok je preostalih 45 studenata (39,5%) odgovorilo da ne razlikuje navedenu podjelu. U konačnici, na pitanje *"Razlikujete li meke i tvrde biometrijske karakteristike?"* 27 ispitanih (23,7%) odgovorilo je da razlikuje, dok je 87 preostalih studenata (76,3%) odgovorilo kako ne mogu razlikovati. Grafički prikaz 9 predstavlja te podatke.



Grafički prikaz 9. Saznanje o različitim biometrijskim metodama i karakteristikama

Kakva treba biti idealna biometrijska karakteristika?

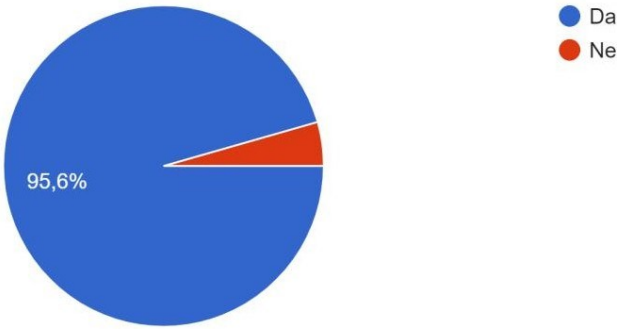
Nadalje, od studenata se tražilo da se izjasne koje značajke treba imati jedna biometrijska karakteristika pojedinca. Mogli su odabrati više odgovora, a među ponuđenima su bili da biometrijska karakteristika treba biti univerzalna (svaka osoba mora posjedovati svoju karakteristiku), jedinstvena (dvije osobe ne smiju imati jednaku karakteristiku), stalna (mora biti stalna tijekom vremena), prikupljiva (mora se moći prikupljati i mjeriti) i prihvatljiva (mora biti opće prihvaćena). Ukupno 61 student (53,5%) složio se kako biometrijska karakteristika pojedinca mora biti univerzalna, dok je 50 ispitanih (43,8%) odgovorilo kako ne mora biti. Povrh toga, da biometrijska karakteristika mora biti jedinstvena, složilo se 99 studenata (86,8%), dok se 13 studenata (11,4%) izjasnilo kako ona ne mora biti. Također, 68 studenata (59,6%) složilo se da svaka biometrijska karakteristika mora biti stalna u vremenu, a 41 student (36%) odgovorio kako ne mora biti stalna. Osim toga, 71 student (62,3%) složio se kako se ona mora moći prikupljati i mjeriti, dok je 42 ispitanih (36,8%) odgovorilo suprotno. Da biometrijska karakteristika mora biti opće prihvaćena složilo se 86 ispitanih (75,4%), a ukupno 24 studenata (21%) tvrdilo je kako ne mora biti.Svi podaci vidljivi su na Grafičkom prikazu 10.



Grafički prikaz 10. Najvažnije značajke biometrijske karakteristike

Biometrija u svakodnevnom životu

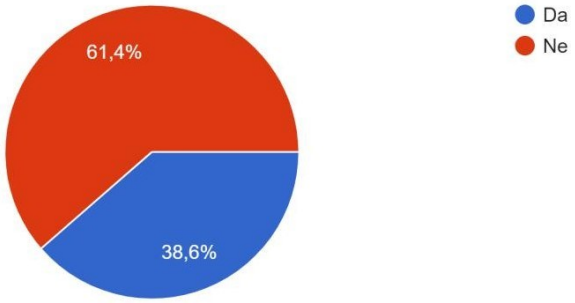
Na pitanje *"Prema Vašem mišljenju, olakšava li biometrija svakodnevni život?"* ukupno 108 studenata (95,6%) složilo se kako ona olakšava, dok je 5 studenata (4,4%) odgovorilo suprotno. Podaci su vidljivi na Grafičkom prikazu 11.



Grafički prikaz 11. Stav studenata o tome olakšava li biometrija svakodnevicu

Nužnost biometrije danas

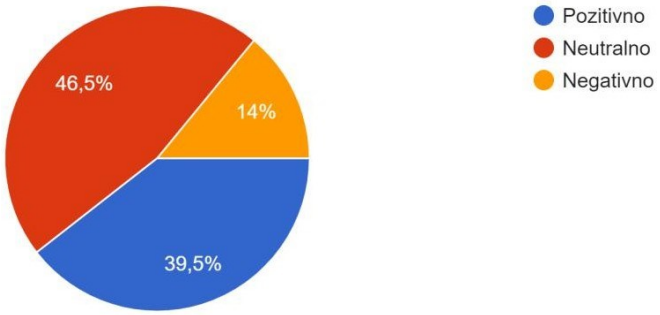
Anketni upitnik zahtijevao je od studenata da se izjasnu je li biometriju danas nužna u svakodnevnom životu. Ukupno 44 studenata (38,6%) složilo se kako je nužna, dok je 70 studenata (61,4%) odgovorilo kako nije stvarno nužna. Podaci su prikazani na Grafičkom prikazu 12.



Grafički prikaz 12. Stav studenata o nužnosti biometrije

Percepcija biometrijske tehnologije u budućnosti

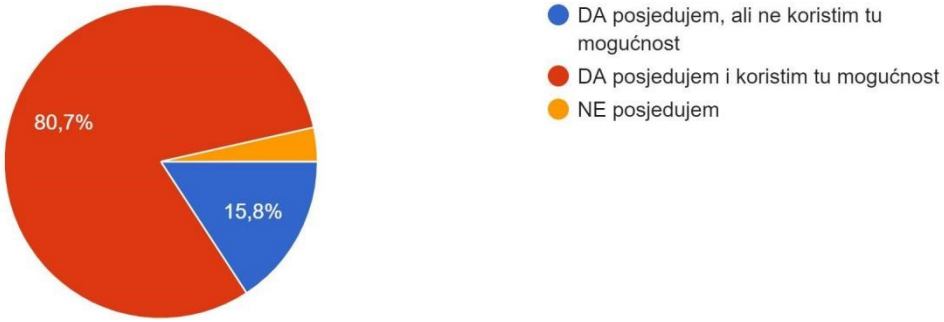
Iduće važno pitanje odnosilo se na stavove o biometriji u budućnosti, odnosno tražilo se da studenti odgovore doživljavaju li njezin razvoj pozitivno, neutralno ili negativno. Ukupno 46,5% ispitanih studenata odgovorilo je da im je percepcija neutralna, dok je pozitivnih percepcija bilo ukupno 39,5%, a negativnih 14%. Podaci su vidljivi ispod na Grafičkom prikazu 13.



Grafički prikaz 13. Studentska percepcija biometrijske tehnologije u budućnosti

Posjedovanje uređaja koji nude mogućnost korištenja otiska prsta

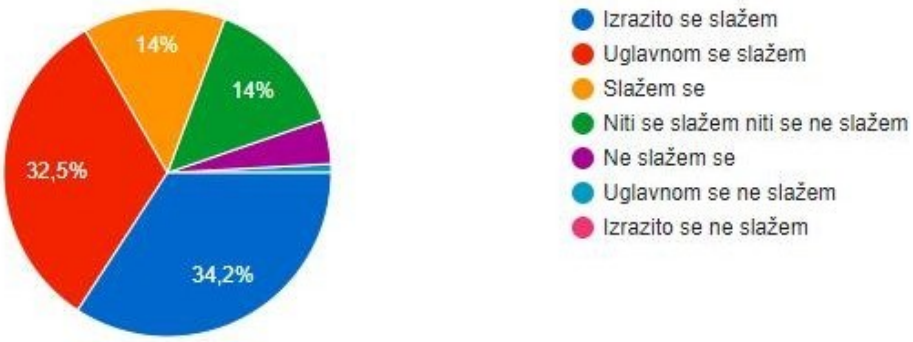
Studenti su također ispitani posjeduju li uređaje koji imaju mogućnost korištenja biometrijske karakteristike kao što je otisak prsta. 92 ispitanih (80,7%) odgovorilo je da posjeduje i da koristi tu mogućnost, 18 studenata (15,8%) da posjeduje, ali ne koristi te 4 ispitanih (3,5%) kako uopće nema tu mogućnost. Podaci su prikazani grafički na Grafičkom prikazu 14.



Grafički prikaz 14. Posjedovanje uređaja s biometrijskom karakteristikom

Percepcija o usvajanju tehnologija

Iduće pitanje odnosilo se na njihovu procjenu o usvajanju tehnologija, a tražilo se da procjene jesu li osoba koja vrlo rano može usvojiti nove tehnologije općenito. Ukupno 39 studenata (34,2%) složilo se s tvrdnjom "Izrazito se slažem", 37 ispitanih (32,5%) je odgovorilo "Uglavnom se slažem", dok je odgovor "Slažem se" i "Niti se slažem niti se ne slažem" dalo jednak broj studenata, odnosno 16 studenata (14%). 5 studenata (4,4,%) odgovorilo je kako se ne slaže s tom tvrdnjom, dok je samo 1 student (0,9%) odgovorio da se uglavnom ne slaže s tom tvrdnjom. Podatke je moguće usporediti na Grafičkom prikazu 15.

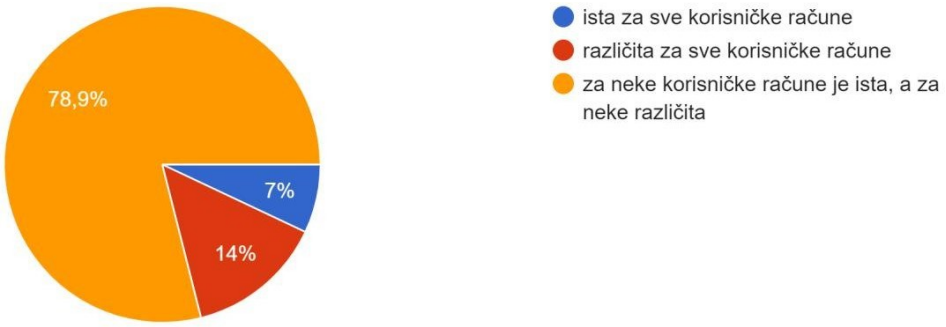


Grafički prikaz 15. Stav o ranom usvajanju tehnologije

Vrste zaporki

Također, anketni upitnik nastojao je otkriti kakve zaporke koriste ispitanici - jesu li one uvijek iste ili različite za sve korisničke račune ili su podjednako zastupljene, tj. koriste li studenti podjednako različite i one iste zaporke. Podaci su vidljivi na grafikonu 15. Ukupno 90 studenata (78,9%)

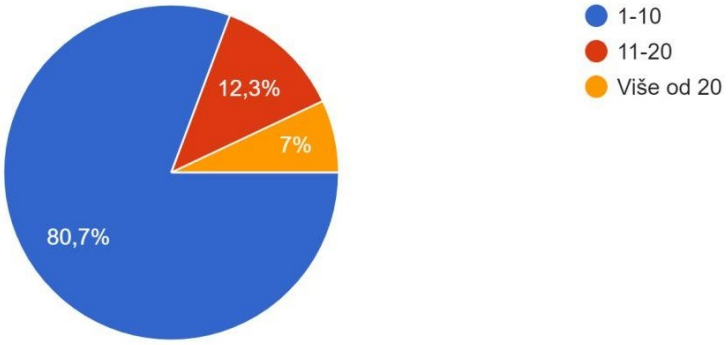
odgovorilo je kako za neke korisničke račune koristi iste, a za neke različite zaporke, dok je 16 ispitanih (14%) potvrdilo kako koriste uvijek različite zaporke. Iste zaporke koristi ukupno 8 studenata, odnosno 7% ispitanih. Podaci su vidljivi na Grafičkom prikazu 16.



Grafički prikaz 16. Korištenje zaporki

Broj korištenih zaporki

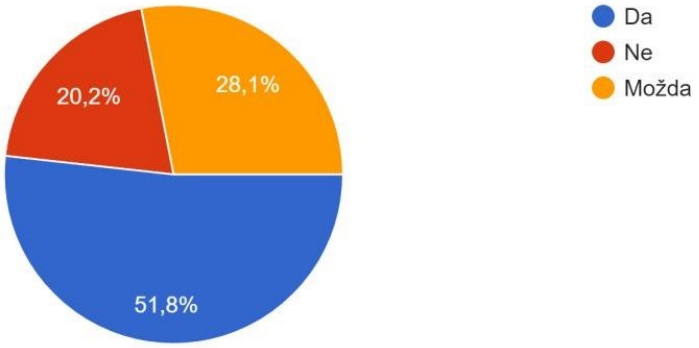
Ispitanici su također bili zamoljeni da odgovore na pitanje koliko zaporki trenutno koriste. 92 ispitanih studenata (80,7%) odgovorilo je kako koristi 1-10 zaporki, 14 ispitanika (12,3%) izjasnilose kako koristi 11-20 zaporki, dok je najmanji broj ispitanih (8 studenata) odgovorio kako koristiviše 20 zaporki, točnije 7% ispitanih. Podaci su prikazani ispod na Grafičkom prikazu 17.



Grafički prikaz 17. Broj korištenih zaporki

Biometrijska karakteristika kao alternativa

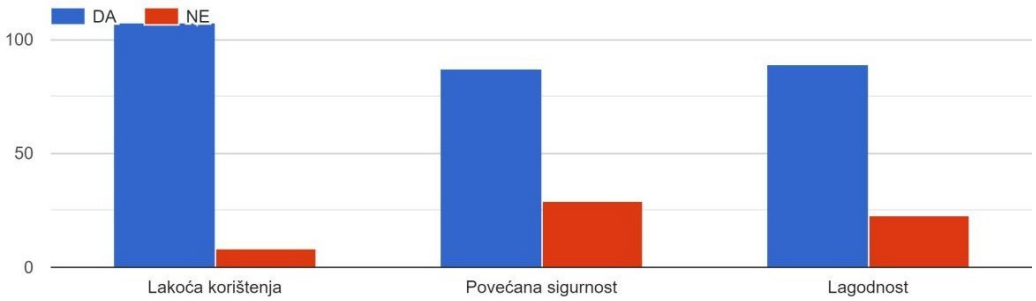
Osim zaporki, sudionici su morali odgovoriti na pitanje bi li umjesto uobičajenog PIN-a koristili biometrijsku karakteristiku i 59 studenata je odgovorila da bi, dakle 51,8% njih. Odgovor "Možda" dao je dalo je 32 studenata, odnosno 28,1%, dok je 20,2% studenata (ukupno 23) izjavilo kako ne bi uopće zamjenjivali. Grafički je prikazano na Grafičkom prikazu 18.



Grafički prikaz 18. Korištenje biometrijske karakteristike kao alternative

Prednosti biometrijskih tehnologija

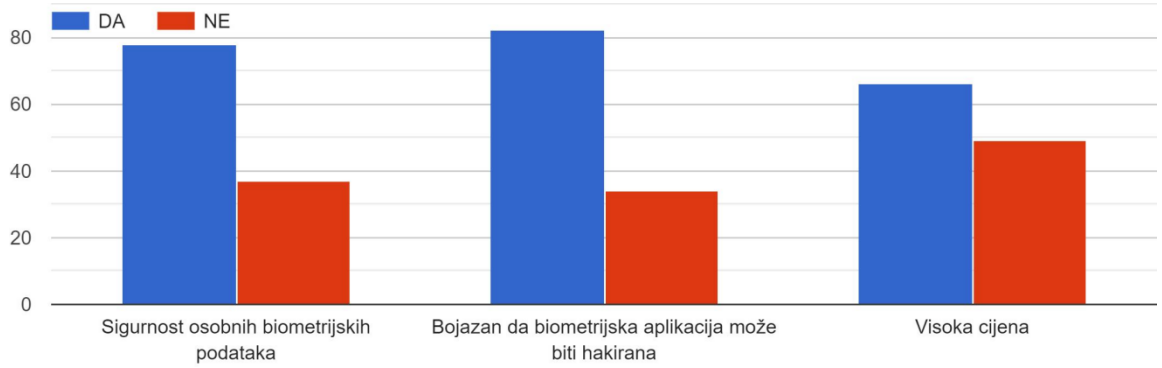
Anketni upitnik zahtijevao je od studenata da označe koje prednosti u odnosu na korištenje različitih korisničkih računa/zaporki i/ili PIN-ova studenti smatraju da ima biometrijska tehnologija. Od ponuđenih je bilo lakoća korištenja, povećana sigurnost i lagodnost. Ukupno 107 studenata (94%) smatra lakoću korištenja kao prednost, dok je 8 studenata (7%) odgovorilo kako to nije za njih prednost. Također, 87 studenata (76,3%) smatra kako je prednost biometrijske tehnologije povećana sigurnost, za razliku od 29 studenata (25,4%), koji misle suprotno. Naposljetku, lagodnost kao prednost korištenja vidi 89 studenata (78%), dok 29 ispitanih (25,4%) tvrdi kako ipak nije prednost. Rezultati su vidljivii usporedivi na Grafičkom prikazu 19.



Grafički prikaz 19. Prednosti biometrijskih tehnologija

Nedostaci biometrijskih tehnologija

Nadalje, anketni upitnik zahtijevao je od studenata da označe koje nedostatke u odnosu na korištenje različitih korisničkih računa/zaporki i/ili PIN-ova studenti smatraju da ima biometrijska tehnologija. Od ponuđenih nedostataka bilo je navedeno: sigurnost osobnih biometrijskih podataka, bojazan da biometrijska aplikacija može biti hakirana te visoka cijena. Ukupno 78 ispitanih (68%) smatra nedostatkom sigurnost osobnih biometrijskih podataka, dok 37 studenata (32%) tvrdi suprotno. Nadalje, bojazan se ističe kao nedostatak od strane 82 studenta (71%), dok se od strane 34 studenata (29%) to ne smatra nedostatkom. U konačnici, visoka cijena je za 66 studenta (58%) nedostatak, dok 49 ispitanih (42%) tvrdi suprotno. Podaci su prikazani ispod na Grafičkom prikazu 20.



Grafički prikaz 20. Nedostaci biometrijskih tehnologija

Izazovi biometrijskih tehnologija

Osim prednosti i nedostataka koje su morali navesti studenti, bilo je potrebno označiti koji izazov biometrijskih tehnologija smatraju najvećim. Bilo je nabrojano 7 izazova: neuspjela autentifikacija, biometrijski sustav autentificira pogrešnog korisnika, biometrijski sustav ne uspije autentificirati pravog korisnika, spoofing, deepfake, nemogućnost ponovnog stvaranja biometrijskog uzorka te etički problemi. 27 studenata (23,7%) izjasnilo kako je za njih spoofing najveći izazov. Nakon toga slijedi autentifikacija pogrešnog korisnika (18,4%), s kojom se složio 21 student. Nemogućnost ponovnog stvaranja biometrijskog uzorka i neuspješna autentifikacija pravog korisnika dijele isti postotak od 13,2% i s time se složilo 15 studenata. Etički problemi (10,5%) su za 12 studenata najveći izazov, dok je neuspjela autentifikacija (8,8%) za 10 studenata. Rezultati su vidljivi ispod na Grafičkom prikazu 21.

Grafički prikaz 21. Izazovi biometrijskih tehnologija

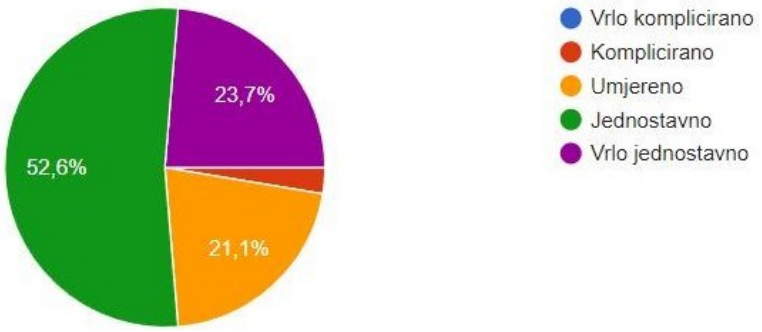
Invazivnost biometrijskih tehnologija

Pitanje invazivnosti je također jedno od bitnih pitanja na koje se željelo odgovorit čiji su podaci prikazani ispod na grafikonu 22. 66 studenata (57,9%) misli da biometrijska tehnologija nije invazivna, no 25 studenata (21,9%) ipak misli da je biometrijska tehnologija invazivna jer ne žele dijeliti svoje osobne karakteristike. 12 studenata (10,5%) potvrdilo je kako je biometrijska tehnologija invazivna i da zbog nje osjećaju strah i/ili anksioznost. Nadalje, 5 studenata (4,4%) izjasnilo se kako ovu vrste tehnologije smatraju invazivnom jer je nezdrava, a 4 studenta (3,5%) izjavila su kako je tehnologija invazivna iz kulturoloških i/ili religijskih razloga. Naposljetku,najmanji postotak (1,8%) odnosi se na mišljenje da je biometrijska tehnologija invazivna zbog averzije prema fizičkom kontaktu s uređajem i s ovom su se tvrdnjom složila 2 studenta. Podaci su prikazani na Grafičkom prikazu 22.

Grafički prikaz 22. Invazivnost biometrijske tehnologije

Percepcija lakoće korištenja biometrijskih tehnologija

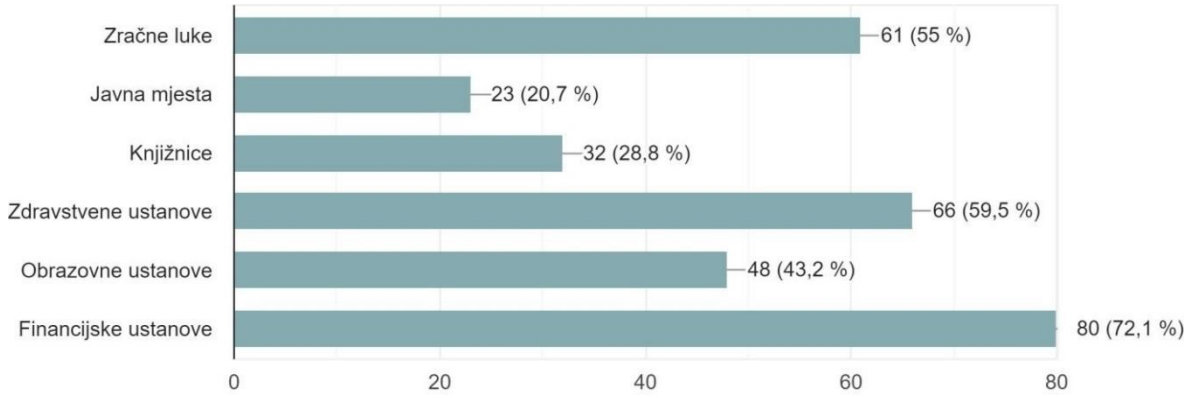
Studenti su također zamoljeni da odgovore kako percipiraju lakoću korištenja biometrijske tehnologije. 60 studenata (52,6%) odgovorilo je kako korištenje percipira jednostavno, dok 27 (23,7%) studenata ipak misli da vrlo jednostavno mogu koristiti ovakvu vrstu tehnologije. Nadalje, 24 (21,1%) ispitanih potvrdilo je kako je njihova percepcija korištenja umjerena, dok se 3 (2,6%) studenata izjasnilo kako im je korištenje zapravo kompliciranо. Podaci su vidljivi ispod na Grafičkom prikazu 23.



Grafiči prikaz 23. Percepcija lakoće korištenja biometrijske tehnologije

Implementacija biometrijskih tehnologija

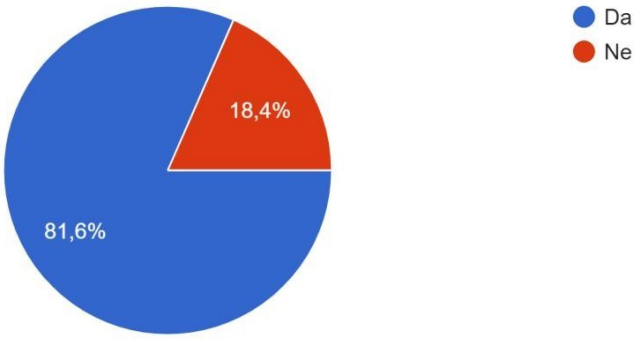
Na pitanje *"Po Vašem mišljenju u kojim sektorima ljudske djelatnosti bi trebalo implementirati biometrijsku tehnologiju?"* ukupno 80 ispitanih (2,1%) smatra kako bi implementacija bila potrebna u financijskim, dok 66 studenata (59,5%) tvrdi kako je potrebna u zdravstvenim ustanovama. Također, 61 student (55%) složio se kako je biometrijsku tehnologiju potrebno uvesti u zračne luke, a 48 ispitanih (43,2%) izjavilo je kako bi bilo dobro implementirati i u obrazovne ustanove. Knjižnice bi također trebale ostvariti implementaciju, što potvrđuje 30 studenata (28,8%), ali i javna mjesta, potvrđeno od strane 23 studenta (20,7%). Podatke je moguće usporediti ispod na Grafičkom prikazu 24.



Grafički prikaz 24. Implementacija biometrijske tehnologije

Povjerenje u biometrijske tehnologije

Posljednjim pitanjem *"Imate li povjerenja u biometriju?"* htjelo se saznati koliko sigurnom studenti smatraju biometriju. 93 studenata (81,6%) smatra kako ima povjerenje, dok ostatak, 21 student (18,4%) smatra kako nema povjerenja. Podaci su vidljivi na Grafičkom prikazu 25.



Grafički prikaz 25. Povjerenje u biometrijske tehnologije

7.4. Rasprava

Proučavajući navedene odgovore koji su ispitanici dali putem online upitnika u siječnju 2023. godine, može se reći kako su rezultati zapravo očekivani i slični rezultatima stranih istraživanja. Mladež je ta koja najlakše može popratiti tehnološke promjene i prilagoditi im se znatno brzo, a tomu potvrđuje i činjenica kako je 79,1% studenata već upoznato s pojmom biometrije te činjenica da je dosad biometriju koristilo 89,5% ispitanih. Dobro percipirana lakoća korištenja također

dokazuje odlično usvajanje tehnologije koje se najčešće koriste u svrhe autentifikacije na mobilnom telefonu, potpisu pri prijemu pošiljki te na potpisu dokumenata i potpisu kod korištenja određenih usluga u banci. Poznavanje razlika biometrijskih metoda također nije iznenađujuća, kao i mišljenje da idealna biometrijska karakteristika stvarno treba biti drugačija za svakog korisnika, jer prema mišljenju 95,6% studenata, ona zbilja olakšava život u današnjem društvu. Međutim, ono što je bilo pomalo iznenađujuće je to što je ukupno 25 studenata (22%) izjavilo kako zbog korištenja biometrijske tehnologije osjeća anksioznost te zbog toga smatra ovakvu vrstu tehnologije invazivnom. Ipak, 81,6% ispitanih je izjavilo kako osjeća dovoljnu razinu povjerenja i sigurnosti. Što se tiče implikacija ovog istraživanja, postoje pozitivna i negativna. S jedne strane je to teorijski doprinos, jer pruža generalnu sliku o percpeciji studenata, a s druge su to problemi oko korištenja tehnologije ovakve vrste zbog kojih ispitanici osjećaju anksioznost. Prvo graničenje ovog istraživanja jest neujednačeni uzorak. Postotak studenata primjerice na Filozofskom fakultetu u Osijeku (83,33%) je drastično neujednačen s odazivom studenata na Filozofskom fakultetu u Mostaru (2,6%). Osim toga, za sva reprezentativnija istraživanja potrebno je bolje organizirati anketni upitnik, odnosno dodati pitanja kako bi se produbila percepcija. U konačnici, ograničenje je i vrijeme provedbe istraživanja. Vrijeme bi u svakom slučaju trebalo biti duže. Produljenje vremena provedbe istraživanja omogućilo bi prikupljanje više podataka i dublju analizu rezultata. Ovo istraživanje može poslužiti kao osnova za daljnje istraživanje i razvoj politika kako bi se bolje razumjelo i upravljalo prihvaćanjem biometrijske tehnologije u društvu.

8. ZAKLJUČAK

Povijest same biometrije seže u doba drevnog Egipta, a danas se može definirati kao disciplina koja koristi biološke karakteristike (fiziološke i bihevioralne) pojedinca sa svrhom obavljanja određene funkcije. Ovaj se proces odvija pomoću biometrijskih sustava koji su integrirani u različitim tehnologijama koje primjerice omogućuju otključavanje zaslona mobilnog telefona pomoću otiska prsta, DNK, glasa, potpisa, uha, mrežnice i šarenice oka ili pak pomoću lica korisnika. Korisnici zahvaljujući raznovrsnim mogućnostima autentifikacije imaju olakšano korištenje svakodnevnih aktivnosti. Utjecajem umjetne inteligencije, trendovi biometrijskih tehnologija variraju (pozitivno) iz godine u godinu, a među najpoznatijima izdvajaju se multimodalna autentifikacija korisnika, autentifikacija korisnika bez lozinke, biometrija u oblaku, snažna, kvantna biometrija te biometrija u novom prostoru - metaverzumu. Ove mogućnosti ponekad imaju svoja ograničenja pa stvaraju izazove korisnicima, a oni se odnose na neovlašteno korištenje, neuspjelu autentifikaciju, etičke probleme i sl. Prema tome, prihvaćenost tehnologije, kao i percepcija lakoće njezina korištenja različita je u određenim kulturama u svijetu, a to potvrđuju istraživanja provedena u Finskoj i Brazilu. S druge pak strane, istraživanje provedeno u Republici Hrvatskoj 2022. godine proučavalo je samo kontrolu pristupa i određene metode autentikacije među mladima od 18 do 30 godina, gdje je online anketnim upitnikom prikupljeno 203 odgovora. Potvrđeno je kako je više od 86% ispitanih koristilo različite biometrijske tehnologije, dok se kao vodeća biometrijska karakeristika izdvaja otisak prsta. Kako bi se iscrpno dobila komparacija, odnosno istražila razina svijesti o korištenju i važnosti biometrijske tehnologije u studentskoj populaciji, provedeno je istraživanje u siječnju 2023. godine. Kao uzorak istraživanja bili su studenti Filozofskog fakulteta u Osijeku, Fakulteta elektrotehnike i računarstva u Osijeku, Ekonomskog fakulteta u Osijeku, Filozofskog fakulteta u Zagrebu, Filozofskog fakulteta u Zadru te Filozofskog fakulteta Sveučilišta u Mostaru. Od ukupno 114 ispitanih, 71.9% ispitanika je bilo ženskog spola, dok je preostali dio ispitanih bio muškog spola,28.1%. Najviše ispitanih bilo je u dobi od 20 do 30 godina (62.3%) te su to bili studenti preddiplomskog studija (33.6%). Također, rezultati su pokazali kako više od 75 ispitanih ne poznaje zapravo razliku između kontaktnih i nekontaktnih biometrijskih metoda, kao i razliku između mekih i tvrdih biometrijskih karakteristika. Činjenica da je ukupno 95.6% ispitanih izjavilo kako biometrija olakšava svakodnevni život zaista daje doznanja da je uistinu tako, kao i činjenica da 80.7% studenata posjeduje i koristi mogućnost korištenja otiska prsta. Dakako, pritom valja napomenuti da ispitanici koriste uglavnom različite zaporke kod svojih korisnikih računa (78.9%) te da koriste uglavnom do 10 zaporki (80.7%). Osim toga, korištenje biometrijske karakteristike se od strane 51.8% ispitanih smatra kao dobra alternativa. Od prednosti koje izdvajaju studenti najveću ima

lakoća korištenja, dok se kao najveći nedostatak izdvaja strah, odnosno bojazan od hakiranja.Premda postoji strah od hakiranja, ispitanici su izjavili kako ovu vrstu tehnologije ne smatra invazivnom (57.9%) te da je njezina lakoća korištenja jednostavna (52.6%).

9. LITERATURA

1. Abaza, Ayman et al. Ear recognition: A Complete System. URL: http://www.wvhtf.org/wpcontent/uploads/2015/08/EarSystem3_1.pdf (2023-02-24)
2. Angeliki Kitsiou et al. The Role of Users' Demographic and Social Attributes for Accepting Biometric Systems: A Greek Case Study. Future Internet, MDPI, vol. 14(11), 2022. Str. 1-31.
3. Anthropometry - Definition, History and Applications | Biology Dictionary. URL: https://biologydictionary.net/anthropometry/ (2022-12-30)
4. Arun Ross, Sudipta Banerjee, Anurag Chowdhury. Security in smart cities: A brief review of digital forensic schemes for biometric data, Pattern Recognition Letters,Volume 138, 2020, Pages 346-354. URL: https://doi.org/10.1016/j.patrec.2020.07.009. (2023-04-24)
5. Biometric System Architecture - GeeksForGeeks. URL: https://www.geeksforgeeks.org/biometric-system-architecture/ (2023-01-30)
6. Biometrics Authentication vs Verification - Javatpoint. URL: https://www.javatpoint.com/biometrics-authentication-vs-verification (2023-01-04)
7. Biometrics trends for 2023: multimodal and MFA to grow alongside privacy regulations | Biometric Update. URL: https://www.biometricupdate.com/202212/biometrics-trends-for-2023-multimodal-and-mfa-to-grow-alongside-privacy-regulations (2023-02-15)
8. Biometrics. Enciklopedia Britannica. URL: https://www.britannica.com/science/biometrics (2023-01-04)
9. Biometrija. URL: https://www.cis.hr/www.edicija/Biometrija.html (2022-12-17)
10. Blanco-Gonzalo R, Lunerti C, Sanchez-Reillo R, Guest R. Correction: Biometrics: Accessibility challenge or opportunity?. PLOS ONE 13(4). 2018. e0196372. https://doi.org/10.1371/journal.pone.0196372. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0194111 (2023-04-24)
11. Chandra, A., & Calderon, T.. Challenges and constraints to the diffusion of biometrics in information systems. Communications of the ACM, 48(12), 2005. Str. 101–106. doi:10.1145/1101779.1101784 (2023-04-24)
12. Cloud Biometric Authentication vs On Device Biometrics Explained | iProov. URL: https://www.iproov.com/blog/cloud-biometrics-vs-on-device-difference (2023-02-16)
13. Cloud-Base Biometric, Its Advantages, And How It Works. URL: https://www.m2sys.com/blog/biometric-software/cloud-based-biometrics-solution-cloudabis/ (2023-02-15)

14. Consumer trust in banks is mixed. Behavioral biometrics can help, face less so | Biometric Updat. URL: https://www.biometricupdate.com/202210/consumer-trust-in-banks-is-mixed-behavioral-biometrics-can-help-face-less-so (2023-02-15)
15. Could you Unlock Your Phone with Your Body Odor? | by Brinnae Bent, PhD | Medium. URL: https://runsdata.medium.com/could-you-unlock-your-phone-with-your-body-odor-830ae1860481 (2023-02-16)
16. CULTURES: ACCEPTANCE IN FINLAND AND BRAZIL. URL: https://jyx.jyu.fi/bitstream/handle/123456789/66405/1/URN%3ANBN%3Afi%3Ajyu-201911154909.pdf (2023-04-30)
17. Current state of the art and enduring issues in anthropometric data collection. URL: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532016000300003 (2023-02-06)
18. Decoding the quantum fingerprint - The Varsity. URL: https://thevarsity.ca/2021/09/19/quantum-fingerprint-explained/ (2023-02-16)
19. Difference between Centralized Database and Distributed Database - GeeksforGeeks. URL: https://www.geeksforgeeks.org/difference-between-centralized-database-and-distributed-database/ (2023-01-04)
20. Domain 5: Identity and access management (controlling access and managing identity). URL: https://www.sciencedirect.com/science/article/pii/B978012811248900005X (2023-0430)
21. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm.. URL: https://www.nature.com/articles/s41598-021-04652-3 (2023-02-14)
22. Everything about FAR and FRR | Recogtech. URL: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience (2023-02-24)
23. Explainer: Keystroke recognition | Biometric Update. URL: https://www.biometricupdate.com/201612/explainer-keystroke-recognition (2023-04-30)
24. Exploring viability of signature recognition biometrics | Infosec Resources. URL: https://resources.infosecinstitute.com/topic/signature-recognition-biometrics/ (2023-04-28)
25. Fingerprints and Flywallet developing wearable biometric payment & access products for Europe. URL: https://www.fingerprints.com/2023/02/24/fingerprints-and-flywallet-developing-wearable-biometric-payment-access-products-for-europe-2302240800/?utm_source=iseepr&utm_medium=NEWS&utm_campaign=Flywallet (2023-

02-24)

26. Fletcher, James et al. A Study of Biometric Security Technology Acceptance and Primary Authentication. URL: http://csis.pace.edu/~ctappert/srd2017/2017PDF/d8.pdf (2023-04-24)
27. Gait Recognition: How It Works, The System & The Algorithm — RecFaces. URL: https://recfaces.com/articles/what-is-gait-recognition (2023-04-30)
28. Guillen-Gamez, Francisco D., et al. Analysis of the perception of students about biometric identification. *International Journal of Web-Based Learning and Teaching Technologies*, vol. 10, no. 3, 2015. URL: https://www.researchgate.net/publication/276271985_Analysis_of_the_Perception_of_Students_about_Biometric_Identification (2023-04-24)
29. Hanmandlu, M et al. Online Biometric Authentication Using Facial Thermograms. IEE, 2012. Washington. URL: 10.1109/AIPR.2012.6528223 (2023-04-28)
30. HELIX SDK - Ear Recognition Software for the Enterprise. URL: http://www.descartesbiometrics.com/helix-sdk/ (2023-02-24)
31. History of Biometrics | Biometric Update. URL: https://www.biometricupdate.com/201802/history-of-biometrics-2 (2022-12-18)
32. Hofstede's Cultural Dimensions Theory & Examples. URL: https://www.simplypsychology.org/hofstedes-cultural-dimensions-theory.html (2023-04-30)
33. IBIA | Biometric Technologies | DNA . URL: https://www.ibia.org/biometrics-and-identity/biometric-technologies/dna (2023-04-28)
34. Identity Fraud Report 2022. URL: https://onfido.com/wp-content/uploads/2022/10/identity-fraud-report-2022.pdf (2023-02-17)
35. Iloanusi,O et al. Automating DNA Biometric Recognition for Real-Time Person Identification. URL: http://nanotechunn.com/new/wp-content/uploads/2018/09/Nanocon314-29-Ilonusi-Automating-DNA-Biometric-Recognition-for-Real.pdf (2023-04-28)
36. Iris Recognition | Electronic Frontier Foundation. URL: https://www.eff.org/pages/iris-recognition (2023-02-25)
37. Iris Recognition Technology - How it Works. URL: https://www.innovatrics.com/iris-recognition-technology/ (2023-02-24)
38. Jain, Ross, Nandakumar. Introduction to Biometrics. Str. 4.-9.
39. Krupp, A. & Rathgeb, Christian & Busch, Christoph. Social Acceptance of Biometric Technologies in Germany: A Survey. BIOSIG 2013 - Proceedings of the 12th International Conference of the Biometrics Special Interest Group. 1-5. Str. 193-200.

40. Ljiljander, Akseli. ATTITUDES TOWARDS BIOMETRIC AUTHENTICATION TECHNOLOGIES BETWEENCULTURES: ACCEPTANCE IN FINLAND AND BRAZIL. URL: https://jyx.jyu.fi/bitstream/handle/123456789/66405/1/URN%3ANBN%3Afi%3Ajyu-201911154909.pdf (2023-04-30)
41. Matsui, Y. et al. Global Deployment of Finger Vein Authentication. URL: https://www.hitachi.com/rev/pdf/2012/r2012_01_108.pdf (2023-04-28)
42. Multimodal Biometrics: A Better Security System? . URL: https://crestresearch.ac.uk/resources/multimodal-biometrics-a-better-security-system/ (2023-02-14)
43. Nađ, Stjepan. Metode autentikacije korisnika : prednosti i izazovi biometrijske tehnologije. Master's thesis, University of Zagreb, Faculty of Economics and Business, 2022. https://urn.nsk.hr/urn:nbn:hr:148:937102 (2023-04-24)
44. Nambiar, B.K., Bolar, K. Factors influencing customer preference of cardless technology over the card for cash withdrawals: an extended technology acceptance model. *J Financ Serv Mark* 28, 2022. Str. 58–73. https://doi.org/10.1057/s41264-022-00139-y (2023-04-24)
45. Quantum Computing Vs. Classical Computing In One Graphic - CB Insights Research.URL: https://www.cbinsights.com/research/quantum-computing-classical-computing- comparison-infographic/ (2023-02-16)
46. Ready for handling Metaverse biometric data? | Biometric Update. URL: https://www.biometricupdate.com/202107/ready-for-handling-metaverse-biometric-data (2023-02-16)
47. Research on Technology of Finger Vein Pattern Recognition Based on FPGA. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1453/1/012037/pdf (2023-04-28)
48. Retinal Recognition: the Ultimate Biometric. URL: https://www.rootstrap.com/blog/retinal-recognition-the-ultimate-biometric (2023-02-24)
49. Rise of Biometrics in the Cloud. URL: https://www.aware.com/blog-biometrics-in-the-cloud/ (2023-02-15)
50. Saranya, M et al. An Approach towards Ear Feature Extraction for Human Identification. IEE, 2016. Chennai. URL: 10.1109/ICEEOT.2016.7755636 (2023-04-24)
51. Signature verification in Real Time. URL: https://www.xyzmo.com/e-signature-products/signature-verification (2023-04-28)
52. sustav. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. http://www.enciklopedija.hr/Natuknica.aspx?ID=58904 (2023-01-30)
53. Technology Acceptance Model: A Case Study Of Palm Vein Authentification Technology.

URL: https://ieeexplore.ieee.org/abstract/document/9945960 (2023-04-24)
54. The maintenance of biometric equipment is vital to its effective use - September 2012 - Hi-Tech Security Solutions. URL: http://www.securitysa.com/43423n (2023-02-17)
55. The role of biometrics in the metaverse. URL: https://cointelegraph.com/metaverse-for-beginners/the-role-of-biometrics-in-the-metaverse (2023-02-16)
56. Two Main Types of Biometrics: Physical vs. Behavioral Biometrics | RecFaces. URL: https://recfaces.com/articles/types-of-biometrics#26 (2023-04-28)
57. Understanding Biometric Performance Evaluation. URL: https://precisebiometrics.com/wp-

content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf (2023-02-24)

58. Usability and Acceptability of Biometric Security Systems. URL: file:///C:/Users/Donata/Downloads/Usability_and_Acceptability_of_Biometric_Security_.pdf (2023-02-17)
59. Vein Recognition. URL: https://findbiometrics.com/solutions/vein-recognition/ (2023-04-28)
60. What is a decentralized database? | VentureBeat. URL: https://venturebeat.com/business/what-is-a-decentralized-database/ (2023-01-04)
61. What is bihevioral bioemtrics? | Definition from TechTarget. URL: https://www.techtarget.com/whatis/definition/behavioral-biometrics (2023-04-28)
62. What is Biometrics as a Service? Benefits and Use Cases - Aware. URL: https://www.aware.com/blog-biometrics-as-a-service-baas/ (2023-02-16)
63. What is Biometrics? How is it used in security?. URL: https://www.kaspersky.com/resource-center/definitions/biometrics (2023-01-04)
64. What is Blockchain Technology? - IBM Blockchain | IBM. URL: https://www.ibm.com/topics/what-is-blockchain (2023-02-16)
65. What is Facial Recognition? - Face Recognition Software and Face Analysis Explained - AWSURL: https://aws.amazon.com/what-is/facial-recognition/ (2023-02-24)
66. What is Passwordless Authetification? . URL: https://www.cyberark.com/what-is/passwordless-authentication/ (2023-02-15)
67. What is Quantum Computing? | Definition from techTarget. URL: https://www.techtarget.com/whatis/definition/quantum-computing (2023-02-16)
68. What is Usability? | IxDF. URL: https://www.interaction-design.org/literature/topics/usability (2023-02-17)
69. What is Voice Recognition Technology an Its Benefits - Zesium . URL: https://zesium.com/what-is-voice-recognition-technology-and-its-benefits/ (2023-04-29)
70. What's Your Type? Keystroke Dynamics as Behavioral Biometrics. URL: https://www.aratek.co/news/keystroke-dynamics-as-behavioral-biometrics (2023-04-30)

71. Wu, Wei et al. Review of palm vein recognition. URL: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2019.0034 (2023-04-28)

10. PRILOZI

UPITNIK O PERCEPCIJI STUDENATA PREMA BIOMETRIJSKOJ TEHNOLOGIJI

Poštovani,
pred Vama se nalazi online upitnik koji se provodi za potrebe istraživanja u sklopu diplomskog rada studentice Filozofskog fakulteta u Osijeku Donate Szombathelyi, diplomski studijinformacijskih tehnologija i nakladništva. Upitnik je u potpunosti anoniman, a popunjavanje upitnika traje desetak minuta.
Unaprijed se zahvaljujemo na sudjelovanju!

1. Spol

- muško
- žensko
- ne želim se izjasniti

2. Dob

- 18-20
- 21-30
- 30+

3. Na kojem fakultetu studirate?

- Filozofski fakultet Osijek
- Filozofski fakultet Zagreb
- Filozofski fakultet Zadar
- Filozofski fakultet Sveučilišta u Mostaru
- Fakultet elektrotehnike, računarstva i informacijskih tehnologija
- Ekonomski fakultet Osijek

4. Koja ste godina studija?

- prva preddiplomskog
- druga preddiplomskog
- treća preddiplomskog

- apsolventska
- prva diplomskog
- druga diplomskog
- dovršetak studija

5. Znate li da je biometrija automatska identifikacija osobe bazirana na njezinoj fizičkoj i/ili ponašajnoj karakteristici? DA NE

6. Jeste li dosada koristili biometriju? DA NE

7. Koju biometrijsku karakteristiku ste dosada koristili (možete odabrati više odgovora)?

- Otisak prsta DA NE
- Slika lica DA NE
- Dlan DA NE
- Rožnica DA NE
- Šarenica DA NE
- Termogram lica tijela DA NE
- Uho DA NE
- Potpis DA NE
- Glas DA NE
- Dinamika tipkanja DA NE
- Miris DA NE
- Hod DA NE
- DNA DA NE

8. U koju svrhu ste dosada koristili biometrijsku tehnologiju u svakodnevnom životu(možete odabrati više odgovora)?

- Otisak prsta na mobilnom telefonu
- Šarenica na mobilnom telefonu
- Potpis pri prijemu pošiljki
- Potpis pri korištenju bankovnih usluga
- Potpis dokumenata
- Ulazak u apartman/smještaj

- Na osobnom računalu
- Putovnica
- Nešto drugo

9. Razlikujete li:

- kontakne i nekontaktne biometrijske metode? DA NE
- fizičke i ponašajne biometrijske karakteristike? DA NE
- meke i tvrde biometrijske karakteristike? DA NE

10. Smatrate li da idealna biometrijska karakteristika treba biti:

- univerzalna (svaka osoba mora posjedovati tu karakteristiku) DA NE
- jedinstvena (dvije osobe ne smiju imati jednaku karakteristiku) DA NE
- stalna (mora biti stalna tijekom vremena) DA NE
- prikupljiva (mora se moći prikupljati i mjeriti) DA NE
- prihvatljiva (mora biti opće prihvaćena) DA NE

11. Po Vašem mišljenju olakšava li biometrija svakodnevni život? DA NE

12. Po Vašem mišljenju je li biometrija nužna u svakodnevnom životu? DA NE

13. Kako percipirate razvoj biometrijske tehnologije u budućnosti?

Pozitivno Negativno Neutralno

14. Posjeduje li pametni telefon, tablet ili neki drugi uređaj koji ima mogućnost korištenja biometrijske karakteristike otisak prsta?

- DA posjedujem, ali ne koristim tu mogućnost
- DA posjedujem i koristim tu mogućnost
- NE posjedujem

15. Smatrate li da ste osoba koja rano usvaja nove tehnologije općenito?

- Izrazito se slažem
- Uglavnom se slažem

- Slažem se
- Niti se slažem niti se ne slažem
- Ne slažem se
- Uglavnom se ne slažem
- Izrazito se ne slažem

16. Kada koristite zaporku je li ona:

- ista za sve korisničke račune
- različita za sve korisničke račune
- za neke korisničke račune je ista, a za neke različita

17. Koliko korisničkih računa/zaporki trenutno koristite?

- 1-10
- 11-20
- Više od 20

18. Biste li razmotrili korištenje biometrijske tehnologije u zamjenu za korištenje različitih korisničkih računa/zaporki i/ili PIN-ova?

- DA
- NE
- MOŽDA

19. Smatrate li da biometrijska tehnologija ima sljedeće prednosti u odnosu na korištenje različitih korisničkih računa/zaporki i/ili PIN-ova?

- Lakoća korištenja DA NE
- Povećana sigurnost DA NE
- Lagodnost DA NE

20. Smatrate li da biometrijska tehnologija ima sljedeće nedostatke u odnosu na korištenje različitih korisničkih računa/zaporki i/ili PIN-ova?

- Sigurnost osobnih biometrijskih podataka DA NE
- Bojazan da biometrijska aplikacija može biti hakirana DA NE
- Visoka cijena DA NE

21. Po Vašem mišljenju koji su najopasniji izazovi biometrijske tehnologije?

- neuspjela autentifikacija
- biometrijski sustav autentificira pogrešnog korisnika (engl. *false acceptance rate*)
- biometrijski sustav ne uspije autentificirati pravog korisnika (engl. *false rejection rate*)
- spoofying (npr. haker upotrebljava sliku korisnika jer korisnik nije fizički prisutan)
- deepfake (npr. haker lažira glas korisnika)
- nemogućnost ponovnog stvaranja biometrijskog uzorka ako je isti postao ugrožen (npr. otisak prsta)
- etički problemi

22. Smatrate li da je biometrijska tehnologija invazivna?

- smatram da je biometrijska tehnologija invazivna jer ne želim dijeliti svoje osobne karakteristike
- smatram da je biometrijska tehnologija invazivna zbog kulturoloških i/ili religijskih razloga
- smatram da je biometrijska tehnologija invazivna jer imam averziju prema fizičkom kontaktu s uređajem
- smatram da je biometrijska tehnologija invazivna jer je nezdrava
- smatram da je biometrijska tehnologija invazivna jer osjećam strah i/ili anksioznost
- ne smatram da je biometrijska tehnologija invazivna

23. Kako percipirate lakoću korištenja biometrijskom tehnologijom?

- Vrlo komplicirano
- Komplicirano
- Umjereno
- Jednostavno
- Vrlo jednostavno

24. Po Vašem mišljenu u kojim sektorima ljudske djelatnosti bi trebalo implementirati biometrijsku tehnologiju?

- Zračne luke
- Javna mjesta
- Knjižnice

- Zdravstvene ustanove
- Obrazovne ustanove
- Financijske ustanove

25. Imate li povjerenja u biometrijsku tehnologiju? DA NE

Ako želite, ostavite svoj komentar vezano uz biometrijsku tehnologiju!

NAJLJEPŠE SE ZAHVALJUJEMO NA SUDJELOVANJU!