Usporedba metoda autentifikacije u web aplikacijama

Zrno, Irena

SVEUČILIŠTE U SPLITU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET

ZAVRŠNI RAD

USPOREDBA METODA AUTENTIFIKACIJE U WEB APLIKACIJAMA

Irena Zrno

Split, rujan 2024.

Temeljna dokumentacijska kartica

Završni rad

Sveučilište u Splitu

Prirodoslovno-matematički fakultet

Odjel za Informatiku

Ruđera Boškovića 33, 21000 Split, Hrvatska

USPOREDBA METODA AUTENTIFIKACIJE U WEB APLIKACIJAMA

Irena Zrno

SAŽETAK

U radu se analiziraju različite metode autentifikacije, uključujući tradicionalne metode, autentifikaciju posjedovanjem i biometrijsku autentifikaciju. Svaka metoda ima svoje prednosti i izazove, posebno u kontekstu sigurnosti i korisničkog iskustva. Stoga, odabir optimalne metode autentifikacije zahtijeva balansiranje između sigurnosnih potreba i jednostavnosti korisničkog iskustva.

Ključne riječi: autentifikacija, sigurnost, upotrebljivost

Rad je pohranjen u knjižnici Prirodoslovno-matematičkog fakulteta, Sveučilišta u Splitu

Rad sadrži:	34 stranicu, 12 grafičkih prikaza i 21 literaturnih navoda. Izvornik je na hrvatskom jeziku.
Mentor:	**doc. dr. sc. Divna Krpan,** *docent Prirodoslovno-matematičkog fakulteta u Splitu, Sveučilišta u Splitu*
Neposredni voditelj:	**Dino Nejašmić, mag. educ. math. et inf.,** *predavač Prirodoslovno-matematičkog fakulteta u Splitu, Sveučilišta u Splitu*
Ocjenjivači:	**doc. dr. sc. Divna Krpan,** *docent Prirodoslovno-matematičkog fakulteta u Splitu, Sveučilišta u Splitu*
	doc. dr. sc. Monika Mladenović, *docent Prirodoslovno-matematičkog fakulteta u Splitu, Sveučilišta u Splitu*
	Dino Nejašmić, mag. educ. math. et inf., *predavač Prirodoslovno-matematičkog fakulteta u Splitu, Sveučilišta u Splitu*

Rad prihvaćen: **rujan, 2024**

Basic documentation card

Bachelor Thesis

University of Split

Faculty of Science

Department of Informatics

Ruđera Boškovića 33, 21000 Split, Croatia

COMPARISON OF AUTENTICATION METHODS IN WEB APPLICATIONS

Irena Zrno

ABSTRACT

The paper analyzes various authentication methods, including traditional methods, possession-based authentication, and biometric authentication. Each method has its own advantages and challenges, particularly in the context of security and user experience. Therefore, choosing the optimal authentication method requires balancing security needs with the simplicity of the user experience.

Key words: authentication, security, usabillity

Thesis deposited in library of Faculty of science, University of Split

Thesis consists of: 34 pages, 12 figures and 21 references.
Original language: Croatian.

Mentor: **Divna Krpan, Ph.D.**, *Assistant at the Faculty of Science and Mathematics, University of Split*

Supervisor: **Dino Nejašmić, mag. educ. math. et inf.,** *Lecturer at the Faculty of Science and Mathematics, University of Split*

Reviewers: **Divna Krpan, Ph.D.**, *Assistant at the Faculty of Science and Mathematics, University of Split*

Monika Mladenović, Ph.D., *Assistant Professor at the Faculty of Science and Mathematics, University of Split*

Dino Nejašmić, mag. educ. math. et inf., *Lecturer at the Faculty of Science and Mathematics, University of Split*

Thesis accepted: **September, 2024**

IZJAVA

kojom izjavljujem s punom materijalnom i moralnom odgovornošću da sam završni rad s naslovom USPOREDBA METODA AUTENTIFIKACIJE U WEB APLIKACIJAMA izradio/la samostalno pod voditeljstvom mag. educ. math. et inf., Dino Nejašmić. U radu sam primijenio/la metodologiju znanstvenoistraživačkog rada i koristio/la literaturu koja je navedena na kraju diplomskog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo/la u diplomskom radu na uobičajen, standardan način citirao/la sam i povezao/la s fusnotama s korištenim bibliografskim jedinicama. Rad je pisan u duhu hrvatskog jezika.

Student/ica

Irena Zrno

Sadržaj

1 Uvod

S obzirom na ubrzani razvoj tehnologije i digitalnih platformi, zaštita korisničkih podataka i osiguranje sigurnog pristupa postaju prioriteti u modernom informacijskom društvu. Autentifikacija, koja omogućuje provjeru identiteta korisnika, predstavlja ključnu komponentu u osiguranju tih resursa i u borbi protiv sve sofisticiranijih prijetnji. Tradicionalne metode autentifikacije, kao što su lozinke, PIN-ovi, te posjedovanje fizičkih kartica ili OTP tokena, i dalje su u upotrebi, ali sa sobom nose brojne izazove i rizike. U kontekstu sveprisutne digitalizacije, pojavljuje se potreba za naprednijim, sigurnijim i korisnički prihvatljivijim metodama autentifikacije.

U ovom radu, analiza različitih metoda autentifikacije, uključujući tradicionalne metode, autentifikaciju posjedovanjem i biometriju, pruža sveobuhvatan pregled trenutnih trendova i izazova u autentifikaciji. Istraživanje ovih metoda omogućava razumijevanje kako različiti pristupi mogu doprinijeti poboljšanju sigurnosti, zaštiti privatnosti i unapređenju korisničkog iskustva u sve kompleksnijem digitalnom okruženju.

2 Osnove autentifikacije

2.1 Definicija i značaj autentifikacije

Autentifikacija je, najjednostavnije rečeno, proces prepoznavanja identiteta korisnika. To je mehanizam povezivanja dolaznog zahtjeva sa skupom identifikacijskih vjerodajnica koje se uspoređuju s onima u bazi podataka s informacijama ovlaštenog korisnika na lokalnom operacijskom sustavu ili unutar poslužitelja za provjeru autentičnosti. [1]

Autentifikacija obuhvaća razne metode i tehnike koje se koriste kako bi se osiguralo da osoba ili entitet koji pristupa nekom sustavu ili usluzi zaista jest ona koja tvrdi da jest. Cilj ovog procesa je osigurati sigurnost i kontrolu pristupa informacijama ili resursima, kako bi se spriječio neovlašten pristup.

Primjeri autentifikacijskih metoda uključuju korisničko ime i lozinku, biometrijske podatke (npr. otisak prsta ili prepoznavanje lica), jednokratne lozinke (OTP) i certifikate. Uobičajeni primjer je unos korisničkog imena i lozinke prilikom prijave na web stranicu. Unos točnih podataka za prijavu omogućuje web stranici da zna tko ste i potvrđuje da ste to doista vi tko pristupa web stranici. Ovaj proces je ključan za osiguranje da samo prave osobe, usluge i aplikacije s pravim dozvolama mogu dobiti pristup organizacijskim resursima. [2]

Proces autentifikacije se može podijeliti na tri faze: identifikacija, autentifikacija i autorizacija. Identifikacija se odnosi na prepoznavanje korisnika na osnovu njegovog korisničkog imena. Nakon što je korisnik identificiran, provjerava se autentičnost identiteta korisnika. Ova faza može uključivati unos lozinke, upotrebu biometrijskih podataka ili nekih drugih vjerodajnica. Zatim, nakon autentifikacije, sustav provodi autorizaciju kako bi provjerio imaju li korisnici dozvolu za sustav kojem pokušavaju pristupiti.

Za organizacije je ključno implementirati mehanizme autentifikacije radi zaštite od prijetnji kao što su krađa identiteta ili neovlašteni pristup. U tom kontekstu, sustavi autentifikacije igraju ključnu ulogu u osiguravanju integriteta i sigurnosti informacija te u zaštiti povjerljivosti organizacijskih resursa. [3]

2.2 Povijest i razvoj metoda autentifikacije

Digitalna autentifikacija ima povijest dužu od šest desetljeća, tijekom kojih je značajno napredovala. U početku su se koristile jednostavne lozinke kao primarno sredstvo sigurnosti. Stoga su s vremenom u cilju povećanja sigurnosti razvijene naprednije metode provjere identiteta, poput tehnologije prepoznavanja lica.

Povijest autentifikacije počinje 1960-ih godina s uporabom lozinki. Tada su računala bila velika, skupa i spora, te su uglavnom bila dostupna samo sveučilištima i velikim poduzećima. Stoga su sveučilišta poput MIT-a razvila sustave poput CTSS-a (eng. Compatible Time-Sharing System), kako bi podijelila resurse jednog računala među više korisnika, odgovarajući na visoku potražnju za računalnim resursima. Godine 1961., student Fernando J. Corbató implementirao je prvi sustav lozinki koji je lozinke pohranjivao u običnom tekstu unutar sustava, što je učinilo lozinku lako dostupnom. Kasnih 1960-ih, programeri su shvatili da to nije sigurno, te su tražili način kako sigurno usporediti unesenu lozinku s pohranjenom bez izlaganja riziku. Ovaj problem je riješio kriptograf Robert Morris tako što je koristio funkciju izvedbe ključa koja bi omogućavala jednostavno računanje u jednom smjeru, ali bi bila teška za dešifriranje u suprotnom smjeru. Ovo je značajno povećalo sigurnost autentifikacije korisnika. [4]

Sredinom 1970-ih razvila se asimetrična kriptografija kako bi poboljšala autentifikaciju koja se temelji na dva ključa. Javni ključ služi za dokaz svog identiteta i siguran je za dijeljenje s ostalim korisnicima, dok se privatni ključ koristi za digitalno potpisivanje i provjeru identiteta. Digitalni certifikat kombinacija ta dva ključa – certifikat javnog ključa potpisan privatnim ključem, koji potvrđuje da pripada određenom korisniku.

Pošto se tehnologija sve više razvijala, napadači su bili sve uspješniji u pogađanju korisničkih lozinki, te su tako statične lozinke postale nepouzdane. Stoga su se sredinom 1980-ih uvele dinamične lozinke tzv. jednokratne (One Time Password, OTP). Lozinke su se mijenjale na osnovu vremena ili lokacije. S vremenom su se razvila 2 protokola za dinamične lozinke: TOTP (gdje se jedinstvenost OTP-a generirala na osnovu trenutnog vremena) i HOTP (gdje se jedinstvenost OTP-a generirala na osnovu ključa prethodne lozinke).

U kasnim 1990-ima, asimetrična kriptografija, koja se počela razvijati 1970-ih, postala je javno dostupna preko infrastrukture javnog ključa PKI. Radi brzog napretka World Wide Weba,

kojeg više nisu koristila samo sveučilišta i vlada, brzo širenje interneta dovelo je do povećanja količine osjetljivih informacija te je bilo potrebno precizno odrediti pristup podacima radi značajnog poboljšanja sigurnosti.

Godine 1986., nekoliko američkih vladinih agencija razvile su SP4 protokol, kojeg su poslije preimenovali u sigurnosni protokol transportnog sloja (Transport Layer Security, TSL). Nekoliko godina kasnije razvili su i SSL protokol (Secure Sockets Layer), koji je sadržavao ključeve i autentifikacijski server. S vremenom je uloga PKI tehnologije postala sljedeća: kreiranje, pohrana i distribucija digitalnih certifikata. Ova uloga također uključuje:

- CA (Certificate Authority) – izdavanje i potpisivanje digitalnih certifikata,
- RA (Registration Authority) – provjeru identiteta korisnika koji podnose zahtjev za digitalni certifikat,
- Centralni imenik – pohrana ključeva,
- CMS (Certificate Management System) – operativne aktivnosti (pristup pohranjenim certifikatima i sl.) i
- Politika certifikata – izjava o zahtjevima za PKI.

Početkom 20. stoljeća dolazi do značajnog napretka u autentifikaciji uvođenjem dviju novih metoda : Multi-Factor Authentication (MFA) i Single Sign-On (SSO). MFA koristi više metoda za provjeru identiteta te je slična OTP-ima koji su se koristili u 80-ima. Za razliku od prijašnjih OTP-ova, više nije bilo potrebno imati posebni hardverski uređaj za generiranje lozinki, nego aplikaciju (npr. Google Authenticator, Duo i Auth) koje mogu same generirati OTP-ove. MFA kombnira tri glavna čibmenika za uspješnu autorizaciju, a to su: znanje (PIN ili lozinka), posjedovanje(mobilni uređaj, pametne kartice) i inherentnost (biometrija). Ostale MFA metode uključuju slanje SMS OTP-ova i čarobnih veza. Druga metoda, SSO, je nastala zbog neovlaštenog dijeljenja lozinki i korištenja istih na više stranica. SSO rješava te probleme uz pouzdanu treću stranu, tako što se korisnici mogu jednom prijaviti na SSO davatelja umjesto da svaka stanica provjerava svaki skup vjerodajnica. Međutim, SSO predstavlja rizike, posebice ovisnost o sigurnosti pružatelja SSO-a. Na primjer, ako je vaš Gmail račun ugrožen, to znači da je svaka web stranica/usluga za koju ste koristili Gmail za prijavu također u opasnosti.

Biometrijska autentifikacija je metoda za autentifikaciju koja koristi fizičke karakteristike kao što su otisci prstiju, prepoznavanje lica, glas i skeniranje šarenice oka za provjeru identiteta korisnika. Motorola ATRIX je bio prvi pametni mobitel koji je implementirao skener za otisak prsta 2011. godine. Tri godine kasnije, Apple je također uveo autentifikaciju otiskom prsta,

Touch ID, a kasnije je 2017. godine prešao na tehnologiju prepoznavanja lica, Face ID, koristeći 30.000 infracrvenih točaka za mapiranje lica korisnika. Danas je biometrijska provjera autentičnosti postala uobičajena, koristi se za otključavanje uređaja i provjeru digitalnih transakcija zbog sigurnosti i teškoće lažiranja. Međutim, problemi s privatnošću te potencijalne pravne i tehničke ranjivosti i dalje postoje.

Istodobno, kasnih 2010-ih došlo je do porasta bihevioralne autentifikacije, čiji je cilj poboljšati korisničko iskustvo. Za razliku od tradicionalne biometrije, ova metoda analizira obrasce interakcije korisnika s uređajima, kao što su brzina tipkanja, način korištenja miša ili kut pod kojim se drži uređaj. Najčešće se koristi u sektorima koji se bave osjetljivim informacijama, kao što je bankarstvo. [5]

Kako tehnologija napreduje, očekuje se da će se integracija biometrijske i bihevioralne autentifikacije proširiti te tako pružiti sigurnost i poboljšano korisničko iskustvo u raznim industrijskim sektorima.

3 Klasifikacija metoda autentifikacije

Klasifikacija autentifikacije se odnosi na sustavnu organizaciju različitih metoda i tehnika koje se koriste za provjeru identiteta korisnika pristupanjem digitalnim sustavima ili uslugama. Autentifikacija, ključni proces potvrđivanja identiteta korisnika ili sustava, pruža osnovni stupanj sigurnosti u suvremenim informacijskim sustavima. Različite metode autentifikacije omogućuju prilagodbu sigurnosnih rješenja koje se moraju prilagoditi specifičnim potrebama i zahtjevima pojedinaca i tvrtki. U ovom poglavlju ćemo analizirati različite metode autentifikacije prema njihovim vrstama, specifičnostima, prednostima, nedostacima i primjenama.

Metode autentifikacije se dijele prema načinu provjere identiteta korisnika:

- tradicionalne metode ili autentifikacije temeljene na znanju,
- autentifikacija posjedovanjem fizičkih objekata ili uređaja,
- biometrijska autentifikacija koja koristi fiziološke ili bihevioralne karakteristike,
- dvofaktorska i višefaktorska autentifikacija koje kombiniraju različite sigurnosne faktore.

Slika 1 Prikaz vrsta autentifikacije [6]

Metode autentifikacije su ključni elementi u zaštiti pristupa digitalnim sustavima i informacijama. Raznovrsnost tehnologija i pristupa autentifikaciji omogućuje njihovu klasifikaciju prema nekoliko osnovnih kriterija, kao što je prikazano u slici 1. Prva podjela temelji se na načinu provjere identiteta korisnika: "što znate", "što imate" i "što jeste". "Što

znate" obuhvaća autentifikacijske faktore poput lozinki ili osobnih identifikacijskih brojeva (PIN), koji se temelje isključivo na znanju korisnika. Suprotno tome, "što imate" uključuje autentifikaciju putem fizičkih objekata kao što su tokeni, pametne kartice ili mobilni uređaji. Naposljetku, "što jeste" koristi biometrijske karakteristike poput otisaka prstiju ili prepoznavanja lica za potvrdu identiteta korisnika. [7]

3.1 Tradicionalne metode autentifikacije

Prva klasa autentifikacije je temeljena na faktoru znanja "nečeg što znate" (knowledge-based authentication). Drugim riječima, temelji se na ideji da tajnu informaciju zna samo odgovarajući korisnik. Najčešći primjeri tajne informacije su lozinke, PIN-ovi i sigurnosna pitanja.

Lozinke su niz znakova (slova, brojeva i posebnih znakova) koji se koriste za provjeru identiteta korisnika i pristupu nekom sustavu, aplikaciji ili uređaju. Prilikom prijave u aplikaciju, sigurnosni sustav od vas traži da date svoje korisničko ime i lozinku. Lozinke spadaju u kategoriju "nešto što znate" jer predstavljaju informaciju koju korisnik posjeduje prije nego što se provede provjera autentičnosti. Iako se koriste često, lozinke imaju mnogo nedostataka. Napadači mogu doći do lozinke „brute force“ metodom. Osim toga, bitan je i ljudski faktor. Lozinke mogu biti jednostavne za pogađanje, ukradene, zaboravljene, korisnici ih mogu dijeliti s drugim korisnicima… Uz sve ove nedostatke, lozinke su najčešće korištena metoda autentifikacije. Poznate su svim korisnicima, što poboljšava korisničko iskustvo, jednostavne su za implementaciju, ne zahtijevaju dodatni hardver ili softver te ih korisnici uvijek mogu mijenjati. [1]

Uzorak za autentifikaciju korisnika na mobilnim telefonima također je primjer faktora znanja, budući da samo važeći korisnik zna autentifikacijski uzorak (poput lozinke ili PIN-a). Studije pokazuju da uzorci također nisu sigurni jer ostavljaju masnu mrlju na ekranu, što napadaču omogućuje da ih dohvati pomoću slika visoke rezolucije.

Drugi primjer faktora znanja je sigurnosno pitanje. Neki sustavi dopuštaju korisnicima postavljanje jednog ili više sigurnosnih pitanja, na koja su korisnici već ranije odgovorili prilikom kreiranja računa ili prijavi za uslugu na mreži. Obično se ova sigurnosna pitanja i odgovori koriste za oporavak lozinke—unošenje točnog odgovora potvrđuje korisnika i omogućuje mu ponovno postavljanje lozinke. Postoje dvije glavne vrste sigurnosnih pitanja:

1. Korisnički definirana pitanja: Korisnici odabiru pitanja s ponuđenog popisa i daju odgovore. Ova pitanja su jednostavna za implementaciju, ali su učinkovita samo ako korisnik odabere teško otkriven odgovor.
2. Sustavno definirana pitanja: Temelje se na informacijama koje pružatelj usluga već zna o korisniku (npr. adresa ili datum rođenja). Učinkovitost ovih pitanja ovisi o tome koliko sustav ima informacija o korisniku i koliko su te informacije teške za otkrivanje napadačima.

Iako je sigurnosna pitanja lako implementirati, vrlo ih je lako ukrasti, pogoditi ili zaključiti iz razgovora (tzv. društveni inženjering). [1]

Osobni identifikacijski broj (PIN) je još jedan primjer faktora autentifikacije koji se temelji na znanju. Sastoji se od niza znamenki koje korisnici sami odabiru kako bi potvrdili svoj identitet. Prilikom odabira PIN-a bitno je da je pamtljiv korisniku. Međutim, što je više slučajniji, to je PIN sigurniji. Potrebno je unijeti ispravan kod da bi se potvrdio identitet. Ako se PIN unese netočno previše puta, korisnik može biti zaključan iz sustava ili uređaja određeno vrijeme. PIN autentifikacija je također jednostavna za implementaciju jer ne zahtjeva posebnu tehnologiju ili algoritam (za razliku od biometrije) te je brža od ostalih metoda autentifikacije znanjem za unos, te zbog toga ima široku primjenu. Autentifikacija PIN-om se koristi u raznim aplikacijama, uključujući bankarstvo, mobilne uređaje i druge sustave gdje je brza i jednostavna autentifikacija bitna. [1]

3.2 Autentifikacija posjedovanjem

Druga klasa autentifikacije se temelji na faktoru posjedovanja odnosno „nečeg što imate“ (possession-based), npr. pametne kartice, USB tokeni, certifikati, OTP kodovi i sl. Autentifikacija posjedovanjem pruža dodatni sloj sigurnosti u odnosu na tradicionalne metode autentifikacije jer zahtijeva od korisnika dokaz posjedovanja fizičkog ili digitalnog predmeta.

Postoje dvije glavne vrste tokena:

1. hardverski tokeni – fizički predmeti koje korisnik posjeduje
2. softverski tokeni - oslanjaju se na softversku komponentu prisutnu na uređaju korisnika

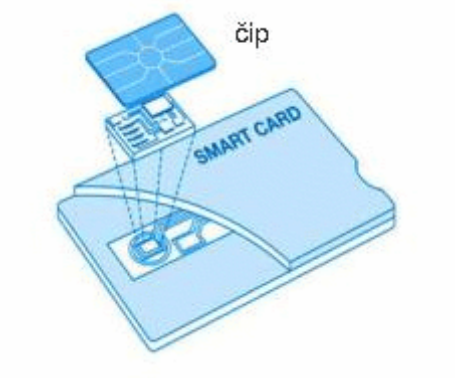
Postoji i dodatna podjela tokena na pasivne i aktivne. Pasivni tokeni su uređaji koji služe za spremanje statičke ili unaprijed definirane informacije te ne zahtijevaju aktivnu interakciju korisnika tijekom autentifikacije (npr. kartice s magnetnom trakom). S druge strane, aktivni

tokeni, zahtijevaju aktivnu interakciju korisnika te generiraju dinamičke kodove ili odgovore u stvarnom vremenu. Aktivni tokeni su sigurniji od pasivnih zbog težeg repliciranja dinamičkih kodova te se radi toga koriste u online bankarstvu.

Najpoznatija metoda faktora posjedovanja, koja se koristila kroz stoljeća, je ključ i brava. Korisnik posjeduje ključ, a brava je izrađena ako da samo nju taj ključ može otključati.

Pored metoda ključa i brave, koriste se i kartice. Kartica je specijalizirani uređaj za pohranu podataka. Podaci vezani za korisnika su zapisani na magnetskoj traci ili u čipu kartice, koje specijalizirani čitač može pročitati.

Pametne kartice, slika 2, su fizičke kartice koje u sebi sadrže čip koji pohranjuje informacije o korisniku poput digitalnih certifikata ili šifriranih ključeva. Za uspješnu autentifikaciju, korisnik mora umetnuti karticu u čitač pametnih kartica ili ih koristiti beskontaktno. Za razliku od običnih kartica, pametne kartice su sigurnije, ali i skuplje. Najpoznatiji primjer pametnih kartica su moderne bankovne kartice.



Slika 2 Izgled pametne kartice [8]

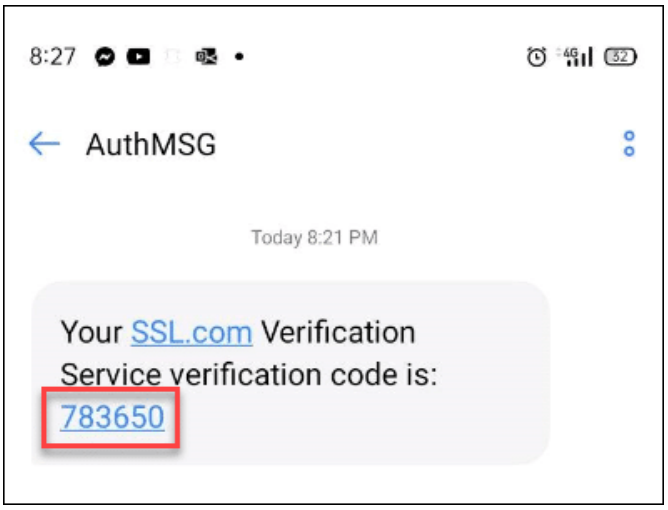
Uz kartice, faktoru posjedovanja pripadaju i tokeni za generiranje jednokratne lozinke, slika 3. Svrha ovih tokena je, kao što i ime kaže, generiranje jednokratne lozinke pomoću koje se vrši autentifikacija. Iako se autentifikacija provodi lozinkom, ova metoda ne pripada faktoru znanja, jer ovu vrstu lozinke korisnik ne može znati ili pamtiti, jer se ona mijenja pomoću kriptografskog algoritma. Tokeni generiraju jednokratne lozike (OTP) koristeći tajnu informaciju (nasumično veliki broj) i trenutno vrijeme. Sustav također zna tajnu i može generirati istu lozinku kako bi provjerio ima li podudaranja. Ovaj proces koristi algoritam nazvan Time-Based One-Time Password (TOTP).

Slika 3 Prikaz fizičkog tokena za generiranje jednokratne lozinke [9]

Postoje i RFID (eng. Radio-frequency identification) kartice koje koriste radio frekvenciju kako bi se razmijenile informacije između čitača i kartice. Osim RFID kartica, postoje i RFID privjesci, slika 4, koji su drugačiji u fizičkom obliku, ali funkcija im je ista. Navedeni uređaju su jeftini za izradu i laki za upotrebu, ali lako ih je klonirati.

Slika 4 Prikaz korištenja RFID privjeska [10]

Kod autentifikacije SMS tokenom, prikazan primjer na slici 5, sustav šalje tajne kodove putem tekstualne poruke, koju korisnik unosi kao jednokratnu zaporku za pristup svom računu. Ova je metoda korisna za zaposlenike kojima je potreban mobilni pristup, ali se može koristiti i na stolnim računalima. Laka je za implementaciju, no nedostatak ove metode je to da korisnik mora imati mobitel uz sebe te je ranjiva na „SIM swap“ ili „phishing“ napade.



Slika 5 Primjer SMS tokena [11]

Provjera autentifikacije tokena e-pošte je slična autentifikaciji SMS-a. Sustav šalje tajni kod na e-poštu korisnika, te tako pruža malo veću sigurnost od SMS tokena. Zahtijeva od korisnika prijavu na e-poštu, što čini pristup sporijim, ali eliminira potrebu za telefonom, jer korisnici mogu pristupiti s bilo kojeg uređaja koji može primati e-poštu.

Autentifikacija putem softverskog tokena zahtijeva od korisnika potvrdu identiteta pomoću aplikacije na mobitelu koja generira jednokratnu zaporku. Većina aplikacija osvježava PIN svake minute, što povećava sigurnost u odnosu na SMS tokene. Jedina mana ove metode autentifikacije je to što korisnik mora imati uređaj za instaliranje aplikacije.

Ova podjela pokriva ključne vrste faktora posjedovanja i jasno ih razvrstava u dvije glavne kategorije, olakšavajući razumijevanje i primjenu različitih metoda autentifikacije. [8]

3.3 Biometrijska autentifikacija

Biometrijska metoda autentifikacije zahtjeva od korisnika da potvrdi svoj identitet svojim fiziološkim karakteristikama ili karakteristikama ponašanja, odnosno temelji se na faktoru inherencije ili pripadnosti tj. „nečeg što jeste“. Fiziološke karakteristike su otisak prsta, prepoznavanje lica, skeniranje šarenice oka, dok su bihevioralne prepoznavanje glasa, hoda,

skeniranje pritiska tipke i skeniranje potpisa. Postoje tri primarna zadatka biometrijskog prepoznavanja: upis, verifikacija i identifikacija. Pri upisu se pohranjuje predložak izdvojen iz ulaznog uzorka zajedno sa referencom korisničkog identiteta (npr. ime, ID) u bazu podataka koja se naziva galerija. Prilikom verifikacije (autentifikacije), uspoređuje se dobiveni uzorak s pohranjenim predloškom da bi se potvrdila referenca identiteta. Zatim se taj identitet koristi za pretragu galerije, a sustav uspoređuje svaki predložak da bi utvrdio valjanost same reference. Ovo je postupak podudaranja 1:1. Tijekom identifikacije se dobiveni uzorak uspoređuje sa svim predlošcima u galeriji da bi se otkrio identitet korisnika. Ovo je postupak podudaranja 1:N. [12]

Prva od prednosti biometrijske autentifikacije je ta što, za razliku od metoda znanja ili posjedovanja, korisnik ne mora pamtiti lozinke ili nositi fizički uređaj i tako ne mora brinuti o zaboravu ili gubitku podataka. Biometrijski podaci su jedinstveni za svaku osobu, što otežava krivotvorenje ili krađu podataka. Uz to, korištenje ove metode je jednostavno i brzo, u većini slučajeva brže nego unošenje PIN-a ili lozinke. Međutim, veliki problem je privatnost podataka, jer njihovo prikupljanje i čuvanje može dovesti do zloupotrebe istih. Ako su biometrijski podaci ugroženi, ne mogu se promijeniti kao lozinke, što predstavlja dodatni sigurnosni rizik. Također, biometrijski sustavi su podložni pogreškama. Pogreška lažnog odbijanja, pogreška tipa 1, se događa kada sustav lažno odbije poznatog korisnika, dok se pogreška lažnog prihvaćanja, pogreška tipa 2, događa kada sustav lažno identificira nepoznatog korisnika kao poznatog korisnika. [1]

Najčešće korištena biometrijska metoda je analiza otisaka prstiju, slika 6. Kroz povijest, ljudi su znali da otisci prstiju imaju jedinstvene karakteristike, te ih koristili za potpisivanje umjetničkih djela ili pravnih ugovora. Otisci prstiju su jedinstveni zbog svojih različitih uzoraka grebena (uzdignute linije na površini kože) i udolina (udubljenja između grebena). Na tržištu postoje različite vrste čitača otisaka prstiju, međutim svi se temelje na mjerenju fizičke razlike između grebena i udolina. Čitači se dijele na čvrste i optičke. Čvrsti čitači koriste različite fizičke čitače za očitavanje uzorka, dok optički koriste svjetlosne čitače. Preko integriranog kondenzatora koji se prazni nakon kontakta s prstom, kapacitivni čitač proizvodi malo električnog naboja. Korištenjem prizme za osvjetljavanje prsta i mjerenjem načina na koji grebeni i udoline reflektiraju svjetlost, optički snima digitalnu sliku otiska prsta. Zatim se ove informacije pretvaraju u sliku. Nakon skeniranja, otisci se uspoređuju metodama podudaranja uzoraka. Potom se jedinstveni podaci i specifične karakteristike otiska prsta spremaju kao šifrirani biometrijski ključ u obliku binarnog koda. Zbog svoje jednostavne upotrebe, sigurnosti i pouzdanosti, metoda otiska prsta se koristi u mnogim područjima, uključujući banke,

računalne sustave, vojsku, zdravstvene ustanove… Međutim, postoje i neki nedostaci ove metode, kao što je privatnost i sigurnost podataka, tehnički problemi i neprikladnosti u nekim okolnostima (npr. kada korisnici imaju ozbiljno oštećenje prsta). [13]

Slika 6 Primjer biometrijske autentifikacije - otisak prsta [14]

3.4 Dvofaktorska i višefaktorska autentifikacija

Kako se s vremenom tehnologija sve više razvijala, tako je rasla i potreba za sigurnošću u digitalnom svijetu. Stoga se razvila višefaktorska autentifikacija kao odgovor za tu potrebu. Svaka metoda autentifikacije ima slabosti, dok metode iz istog autentifikacijskog faktora imaju slične slabosti (npr. ključ i kartica se mogu ukrasti). Autentifikacija je jednofaktorska kada je dovoljno samo jednom da se korisnik autentificira uspješno, npr. unos lozinke. No, kada se koristi i više metoda iz istog autentifikacijskog faktora, kao što su lozinka i sigurnosno pitanje, to je i dalje jednofaktorska autentifikacija.

Autentifikacija je višefaktorska kada je potrebno više metoda iz različitih autentifikacijskih faktora za uspješnu autentifikaciju korisnika. Najzastupljeniji primjer je upotreba bankovne kartice i PIN-a za podizanje gotovine ili kartično plaćanje. U ovom primjeru se koriste metode iz dva različita faktora, faktora posjedovanja i faktora znanja, pa se ovakva višefaktorska autentifikacija naziva dvofaktorskom autentifikacijom.

Zadnjih godina, višefaktorska autenitifikacija je postala dostupna i za mnoge usluge na internetu, e-mail i društvene mreže. Od korisnika se uz lozinku traži i tajni kod poslan putem SMS-a ili jednokratna zaporka generirana pomoću aplikacije na mobitelu.

Višefaktorska autentifikacija pruža još prednosti, osim što poboljšava sigurnost. Jedna od njih je da smanjuje rizik kompromitiranih lozinki. Nadalje, daje fleksibilnost, gdje korisnici mogu prilagoditi različite metode autentifikacije vlastitim potrebama. Ako napadač dobije pristup lozinci korisnika, ne može se prijaviti bez drugog faktora autentifikacije, te se time smanjuje rizik od krađe identiteta i štiti od „phishing“ napada. Uz to, omogućava bolju kontrolu pristupa određenim resursima na osnovu uloge korisnika, lokacije i vremena pristupa.

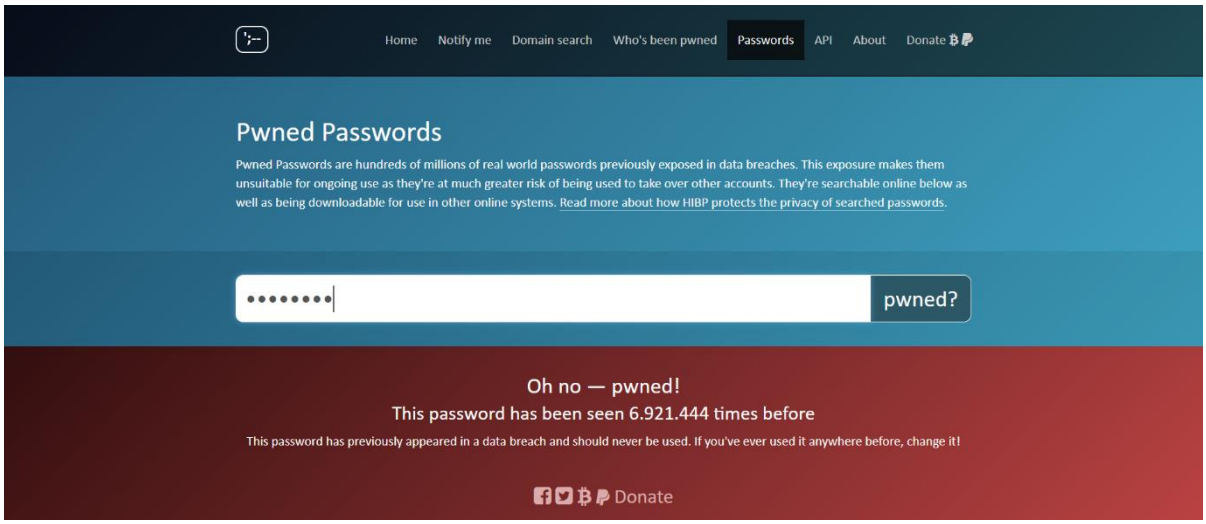
S druge strane, višefaktorska autentifikacija može dati korisniku lažan osjećaj sigurnosti. Iako je sigurnija od jednofaktorske, napadači uvijek mogu pronaći načine kako da dođu do željenih informacija, bilo „phishing“ napadom, društvenim inženjerstvom… Uz to, zahtjeva više vremena za autentifikaciju, jer korisnici moraju proći kroz još jedan ili više dodatnih koraka za autentifikaciju. Implementacija i održavanje mogu biti skupo, pogotovo za manje organizacije i tvrtke. Nadalje, oslanjanje na vanjske strane dovodi do problema nemogućnosti kontrole vanjskih usluga u slučaju kvara. [15]

4 Sigurnost i upotrebljivost(korisničko iskustvo)

Iako su sustavi za autentifikaciju korisnika sveprisutni i moraju zadovoljiti visoke standarde sigurnosti i upotrebljivosti, podložni su raznim napadima. Trenutna istraživanja ne nude dovoljno detaljan pregled napada i odgovarajućih protumjera, od tradicionalnih metoda lozinki do biometrijskih metoda. Korisnici od sustava za autentifikaciju očekuju i jednostavnost korištenja i visoku sigurnost. Sigurnost u sustavima autentifikacije odnosi se na zaštitu korisničkih podataka i osiguranje da samo ovlašteni korisnici mogu pristupiti resursima, dok upotrebljivost podrazumijeva jednostavnost i intuitivnost korištenja sustava. Međutim, upotrebljivost se često žrtvuje radi veće sigurnosti. Stoga je potrebno postići ravnotežu između upotrebljivosti i sigurnosti.

4.1 Sigurnost

Lozinke i PIN-ovi su najčešće korištene metode autentifikacije, ali i najranjivije. Korisnici uglavnom biraju jednostavne lozinke koje su lako pamtljive, npr. „12345678“ ili „password“. Na slici 6 vidimo kako je lozinka „12345678“ viđena preko 6 milijuna puta u javno objavljenim skupovima kompromitiranih podataka. Većina sustava prihvaća lozinke od osam znakova. Postoje tri faktora koja određuju snagu lozinke: duljina, kardinalnost i entropija. Kardinalnost od 94 znači korištenje skupa od 94 znakova (velika i mala slova, brojevi te posebni znakovi). Entropija je izračunata snaga lozinke u bitovima. Npr. lozinka duljine osam znakova s kardinalnošću 94 ima entropiju od 52,4 bita. Obično računalo takvu lozinku može probiti za 20 minuta, a superračunalo za 0,07 sekundi, što je čini slabom. Dulje lozinke nude veću sigurnost jer povećavaju broj mogućih kombinacija koje napadači moraju isprobati. Preporučuje se korištenje lozinki duljih od 12 znakova kako bi se smanjo rizik od „brute force“ napada. „Brute force“ napad je metoda kojom napadač pokušava svaku moguću kombinaciju znakova dok ne pronađe ispravnu lozinku. Uz „brute force“ napad, tu je i „phishing“ napad gdje korisnici unose podatke na lažnim web stranicama. Još jedan od sigurnosnih rizika je korištenje iste lozinke na više računa. Ako je jedna od tih lozinki kompromitirana, svi povezani računi postaju ranjivi.



Slika 7 provjera pojavljivanja lozinke u javno objavljenim skupovima kompromitiranih podataka na servisu Have I been pawned [16]

Kao i kod lozinki, sigurnosni problemi kod PIN-ova su „brute force“ i „phishing“ napadi. PIN-ovi su kraći od lozinki, stoga postoji manji broj kombinacija dok se ne pronađe ispravni PIN. Također, mnogi korisnici biraju lako pamtljive PIN-ove, kao što su „1234“ ili „1111“, koje je lako pogoditi. Uz to, PIN-ovi se često unose na uređajima s fizičkim tipkovnicama ili ekranima osjetljivim na dodir, što dovodi do rizika da netko u blizini vidi unos brojeva. [17] [18]

Autentifikacija posjedovanjem uključuje fizički element i pruža dodatni sloj sigurnosti za razliku od tradicionalnih metoda, ali nije imuna na prijetnje.

RFID kartice i privjesci koriste radio-frekvencijsku identifikaciju, stoga su lako ranjivi na presretanje signala. Napadači mogu s udaljenosti do jednog metra presresti podatke s kartice ili privjeska i stvoriti njihove klonove te si tako omogućiti neovlašteni pristup.

Kartice s magnetskom trakom lako su ranjive na kopiranje podataka, jer nemaju enkripciju. Napadači mogu koristiti uređaje za očitavanje trake i izraditi duplikate, što ih čini podložnima prevarama. S druge strane, pametne kartice, koje u sebi sadrže čip s pohranjenim informacijama, pružaju višu razinu sigurnosti u odnosu na kartice s magnetskom trakom. Međutim, i one imaju svoje sigurnosne rizike. Ako napadač fizički dođe u posjed kartice, može pokušati dešifrirati podatke pohranjene na čipu. Osim toga, ako kartica koristi zastarjele

protokole ili kriptografske algoritme, može biti ranjiva na različite vrste napada, uključujući napade presretanja i dešifriranja podataka.

OTP tokeni, bilo fizički ili softverski, dodaju dinamičku sigurnost u autentifikaciju jer generiraju jednokratne lozinke. Međutim, ti tokeni nisu imuni na prijetnje. Fizički tokeni mogu biti izgubljeni ili ukradeni, dok softverski tokeni mogu postati žrtve „phishing“ napada, gdje napadači prevare korisnike da im otkriju lozinke.

Autentifikacija putem SMS-a, iako široko korištena, ima svoju ranjivost u obliku „SIM swap“ napada. Napadači koriste socijalni inženjering ili podmićivanje zaposlenika mobilnih operatera kako bi preuzeli kontrolu nad telefonskim brojem žrtve. Kada to uspiju, mogu presretati SMS poruke, uključujući one koje sadrže kodove za autentifikaciju. „Phishing“ napadi dodatno povećavaju rizik, budući da korisnici mogu biti zavarani da predaju svoje kodove napadačima. Slično tome, autentifikacija putem e-pošte nosi rizik kompromitacije računa. Ako napadač dobije pristup korisničkoj e-pošti, može presresti sve tajne kodove, što ozbiljno ugrožava sigurnost računa.

Softverski tokeni generiraju lozinke putem mobilnih aplikacija, u kojima se PIN-ovi često osvježavaju, pružajući veću sigurnost od autentifikacije SMS-om. Međutim, gubitkom ili krađom uređaja na kojem je instalirana aplikacija, napadač može dobiti pristup aplikaciji i generiranim kodovima.

Biometrijska autentifikacija nudi visoku sigurnost, no također nije imuna na prijetnje. Biometrijski podaci su jedinstveni i nepromjenjivi za svaku osobu. Ako dođe do njihovog ugrožavanja, za razliku od lozinki, ti podaci se ne mogu promijeniti. Gubitak ili krađa biometrijskih podataka može imati trajne posljedice, jer ih je nemoguće ponovno generirati ili izmijeniti.

„Spoofing“ napadi predstavljaju ozbiljnu prijetnju biometrijskim sustavima, omogućujući napadačima da prevarom dobiju neovlašten pristup korištenjem replika biometrijskih podataka. Fiziološke karakteristike poput otisaka prstiju, lica ili potpisa relativno je lako imitirati. Otisci prstiju ostavljeni na kvakama, osobne fotografije objavljene na društvenim mrežama i slike snimljene kamerama u javnim prostorima se mogu lako iskoristiti. Često koriste maske lica ili gumene modele otisaka prstiju kako bi prevarili sustave autentifikacije. Napadači izrađuju lažne otiske prstiju od materijala poput silikona ili gela na temelju tragova koje korisnici ostavljaju

na površinama, te korištenjem visokokvalitetnih fotografija ili video zapisa za prevaru sustava za prepoznavanje lica. Napredni sustavi prepoznavanja lica koriste tehnologije poput 3D mapiranja ili infracrvenih senzora kako bi se zaštitili od takvih prijetnji, no sustavi koji se oslanjaju na 2D slike ostaju ranjivi, posebno u javnim prostorima s nižom razinom sigurnosti.

Prepoznavanje lica postalo je široko rasprostranjeno na mobilnim uređajima, s točnošću koja može doseći više od 98% zahvaljujući dubokim neuronskim mrežama dok prepoznavanje otisaka prstiju nudi visoku točnost do 99,2%. Iako je prepoznavanje šarenice sigurnije i može postići točnost do 97%, njegova primjena je ograničena zbog specifičnih zahtjeva za opremom. Međutim, biometrijski sustavi, nisu bez tehničkih ograničenja i mogu generirati pogreške koje utječu na njihovu sigurnost i pouzdanost. Pogreška lažnog odbijanja, kada sustav ne prepozna legitimnog korisnika, i pogreška lažnog prihvaćanja, kada sustav prepozna neovlaštenu osobu kao legitimnu, mogu dovesti do nenamjernog uskraćivanja pristupa ili omogućavanja neovlaštenog pristupa. Ove pogreške mogu biti uzrokovane različitim tehničkim nepravilnostima, poput oštećenja kože koje ometa pravilno skeniranje otisaka prstiju ili nepravilnog osvjetljenja koje smanjuje točnost prepoznavanja lica. [19]

4.2 Upotrebljivost

Kada se procjenjuju različite metode autentifikacije, upotrebljivost i korisničko iskustvo igraju ključnu ulogu u njihovom prihvaćanju i efektivnosti. Iako je sigurnost najvažniji aspekt svake metode autentifikacije, ako je korisnicima teško ili neprijatno koristiti određenu metodu, postoji rizik da će je izbjegavati ili tražiti načine da je zaobiđu, što može dovesti do ugrožavanja sigurnosti sistema. Upotrebljivost (usability) metoda autentifikacije igra ključnu ulogu u njihovoj efektivnosti, jer čak i najnaprednija metoda može biti neefikasna ako korisnici ne mogu lako da je koriste. Ovdje su prikazane metode autentifikacije sa fokusom na njihove prednosti i nedostatke u pogledu upotrebljivosti. [20]

Međutim, tradicionalne metode autentifikacije posjeduju i nedostatke. Primarno, korisnici su dužni pamtiti lozinke ili PIN-ove, što može predstavljati problem, posebno kada se radi o složenim lozinkama. Zaboravljanje lozinke često dovodi do frustrirajućeg procesa oporavka računa, što negativno doprinosi korisničkom iskustvu. Konačno, ove metode nisu prikladne za

osiguranje visoke razine sigurnosti, jer lozinke, koje su same po sebi složene također uveliko narušavaju upotrebljivost sustava.

Korisnici su već upoznati s tradicionalnim metodama provjere autentičnosti koje su u širokoj upotrebi kod većine sustava i intuitivne za korištenje bez dodatne edukacije. Ove metode nude veliku jednostavnost korištenja te omogućuju brzi unos lozinki ili PIN-ova. Također, tradicionalne metode ne zahtijevaju dodatni hardver ili softver, što omogućuje njihovu upotrebu na širokom spektru uređaja i platformi bez dodatnih komplikacija ili troškova.

Međutim, kada se tradicionalne metode autentifikacije sagledaju kroz prizmu upotrebljivosti, javljaju se i određeni problemi. Prvi među njima je potreba za pamćenjem lozinki, osobito složenih lozinki koje su potrebne za održavanje odgovarajuće razine sigurnosti. Ovaj zahtjev može biti izazovan za mnoge korisnike, dovodeći do situacija u kojima koriste jednostavne i predvidljive lozinke, što kompromitira sigurnost. Alternativno, korisnici mogu biti prisiljeni zapisivati lozinke ili koristiti iste lozinke na više mjesta, što dodatno povećava sigurnosne rizike.

Zaboravljanje lozinke ili PIN-a predstavlja još jedan značajan problem s aspekta upotrebljivosti. Proces oporavka računa često je zamoran i može izazvati frustraciju kod korisnika, narušavajući njihovo ukupno iskustvo sa sustavom. To je posebno problematično u poslovnim okruženjima, gdje gubitak pristupa računu može dovesti do smanjenja produktivnosti ili propuštanja važnih rokova.

Također, potreba za redovitom promjenom lozinki, što je često preporučena sigurnosna praksa, dodatno opterećuje korisnike. Često mijenjanje lozinki može biti zamorno i može dovesti do smanjenja učinkovitosti, jer korisnici moraju pamtiti nove, često složene lozinke, što dodatno povećava rizik od pogrešaka i frustracije.

Metoda posjedovanja u autentifikaciji korisnika predstavlja jednu od najjednostavnijih i najefikasnijih strategija za verifikaciju identiteta, temeljenu na fizičkom posjedovanju uređaja poput pametnih telefona, pametnih kartica ili USB tokena. Ova metoda omogućava brzo i intuitivno prijavljivanje, jer se oslanja na uređaje koje korisnici već rutinski koriste. Nakon inicijalne konfiguracije, proces autentifikacije je često gotovo trenutan i može se odvijati automatski, smanjujući potrebu za aktivnim angažmanom korisnika i time povećavajući efikasnost i praktičnost svakodnevnih operacija. U suštini, metoda posjedovanja značajno

pojednostavljuje korisničko iskustvo, omogućavajući korisnicima da se brzo prijave u sisteme bez potrebe za pamćenjem lozinki ili drugih složenih sigurnosnih podataka.

Međutim, usprkos navedenim prednostima, ova metoda nije bez svojih inherentnih ograničenja. Konstantna potreba za fizičkim prisustvom uređaja može biti nepraktična, naročito u situacijama kada korisnik zaboravi uređaj, izgubi ga, ili ga jednostavno nema pri ruci. Ovaj problem postaje još ozbiljniji u kontekstu gubitka ili krađe uređaja, što ne samo da onemogućava autentifikaciju, već također predstavlja značajan sigurnosni rizik. U slučaju da neovlaštena osoba dođe u posjed uređaja, može doći do kompromitacije sigurnosti sistema, što može rezultirati ozbiljnim posljedicama po integritet korisničkih podataka. Nadalje, tehnički problemi, poput niske baterije, kvarova uređaja ili problema s povezivanjem, mogu dodatno ugroziti pouzdanost ove metode. Takvi problemi mogu dovesti do privremenog ili potpunog onemogućavanja autentifikacije, čime se smanjuje dostupnost i pouzdanost sistema, što može frustrirati korisnike i dovesti do negativnog iskustva. Stoga, iako metoda posjedovanja nudi značajne pogodnosti, neophodno je pažljivo razmotriti i upravljati potencijalnim rizicima kako bi se osigurala njena efektivna implementacija u različitim sigurnosnim okruženjima.

Biometrijske metode autentifikacije predstavljaju jedan od najinovativnijih pristupa sigurnosti, nudeći brojne prednosti koje ih čine sve popularnijim izborom u današnjem tehnološkom okruženju. Prva i možda najvažnija prednost ovih metoda je njihova iznimna jednostavnost korištenja. Razlog tomu je što biometrijske tehnologije eliminiraju potrebu za pamćenjem lozinki ili nošenjem dodatnim uređaja, što je uobičaji izvor frustracije i nesigurnosti kod tradicionalnih metoda autentifikacije. Biometrijski proces identifikacije je brz i jednostavan, koristeći jedinstvene fizičke karakteristike ili karakteristike ponašanja korisnika kao što su otisak prsta, prepoznavanja lica ili analiza glasa. Ova prirodnost korištenja, koja se oslanja na intrinzične karakteristike korisnika, čini biometrijske metode posebno intuitivnima i lakima za svakodnevno korištenje, čime se značajno poboljšava korisničko iskustvo. Osim toga, biometrijski podaci imaju svojstvo nepromjenjivosti, što znači da se ne mogu zaboraviti, izgubiti ili ukrasti poput lozinki ili fizičkih sigurnosnih uređaja. Ova funkcija pomaže u povećanju sigurnosti i pouzdanosti sustava jer izbjegava mnoge probleme povezane s tradicionalnim metodama provjere autentičnosti, poput rizika od krađe identiteta ili neovlaštenog pristupa.

No, unatoč ovim značajnim prednostima, biometrijske metode nisu bez nedostataka, koji često zabrinjavaju korisnike i sigurnosne stručnjake. Veliki problem u biometrijskoj autentifikaciji je privatnost. Prikupljanje, obrada i pohranjivanje biometrijskih podataka podliježu strogim regulatornim okvirima, ali također stvaraju određenu dozu nesigurnosti među korisnicima, posebice u pogledu potencijalne zlouporabe ili curenja podataka. Ova briga postaje još izraženija u pogledu nepromjenjivosti biometrijskih podataka; za razliku od lozinki, biometrijski podaci ne mogu se jednostavno promijeniti ako su ugroženi.

Dodatno, tehnička složenost biometrijskih sustava može dovesti do određenih problema u njihovoj implementaciji i korištenju. Doista, biometrijski sustavi autentifikacije nisu uvijek savršeni i mogu se pojaviti pogreške u prepoznavanju, kako lažno pozitivnih tako i lažno negativnih. Ovi problemi mogu frustrirati korisnike, uzrokovati neuspjeh autentifikacije i smanjiti povjerenje u sustav. Promjene u fizičkom izgledu korisnika, kao što su starenje, ozljede ili jednostavne promjene izgleda, kao i nepovoljni uvjeti poput lošeg osvjetljenja, mogu dodatno otežati prepoznavanje i ispravnu identifikaciju. U konačnici, iako biometrijske metode autentifikacije nude impresivne prednosti u smislu sigurnosti i jednostavnosti upotrebe, njihov uspjeh uvelike ovisi o sposobnosti sustava da riješi i ublaži gore navedene nedostatke, posebno u pogledu privatnosti, tehničke pouzdanosti i podložnosti promjenama. [21]

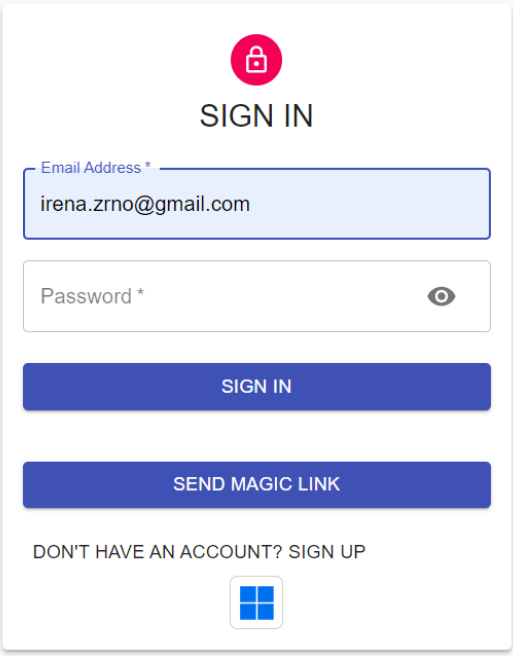
5 Implementacija

U praktičnom dijelu ovog rada implementirana je autentifikacija bez lozinki. Autentifikacija bez lozinki je metoda gdje korisnici ne moraju unositi lozinku ili odgovarati na sigurnosna pitanja kako bi pristupili nekom sustavu ili servisu. Umjesto toga, korisnici mogu pristupiti tim servisima ili sustavima biometrijskim podacima ili OTP kodovima. Smanjuje rizike povezane s lozinkama, poboljšava korisničko iskustvo i može značajno smanjiti opterećenje za IT podršku.

Prvi dio implementacije ove metode je prijava na aplikaciju putem čarobnih veza. Čarobne veze su metoda autentifikacije bez lozinke koje koriste jedinstvene i vremenski ograničene URL-ove za identifikaciju korisnika prilikom prijave. Uglavnom se šalju putem e-pošte, SMS-a ili aplikacija za razmjenu poruka. Korisnici se autentificiraju jednostavnim klikom na vezu. Ova metoda poboljšava korisničko iskustvo i sigurnost te smanjuje broj zahtjeva za promjenu lozinki.

```
    const handleSendMagicLink = async (e) => {
        e.preventDefault();
        try {
            await axios.post('http://localhost:5000/user/send-
magic-link', { email: formData.email });
            alert('Magic link sent! Check your email.');
        } catch (error) {
            console.error('Error sending magic link:', error);
            alert('Failed to send magic link.');
        }
    };
```

Kod 1 Prikaz funkcije za slanje čarobne veze



Slika 8 Prikaz korisničkog sučelja gdje je dugme preko kojeg šaljemo čarobnu vezu

Kada korisnik pritisne dugme „*Send Magic Link*“, slika 8, poziva se funkcija „*handleSendMagicLink*“, prikazana na slici 8, koja šalje POST zahtjev ka API-u na backend-u sa korisničkom email adresom. Ako je zahtjev uspješan, korisniku se prikazuje obavještenje da je čarobna veza poslana, a ako nije, onda se prikazuje greška.

```
export const sendMagicLink = async (req, res) => {
    const { email } = req.body;

    try {
        const existingUser = await User.findOne({ email });
        if (!existingUser) {
            return res.status(404).json({ message: 'User not
found.' });
        }

        const token = jwt.sign({ email: existingUser.email, id:
existingUser._id }, secretKey, { expiresIn: '15m' });
        const magicLink = `http://localhost:3000/auth/magic-
login/${token}`;

        console.log(`Magic link for ${email}: ${magicLink}`);
        await sendMagicLinkEmail(email, magicLink);
```

```
        res.status(200).json({ message: 'Magic link sent
successfully.' });
    } catch (error) {
        console.error('Error sending magic link:', error);
        res.status(500).json({ error: 'Failed to send magic
link.' });
    }
};
```

Kod 2 Prikaz obrađivanja zahtjeva na serveru i kreiranja JWT tokena

Zatim funkcija „*sendMagicLink*“ na serveru prima zahtjev i provjerava je li taj korisnik postoji u bazi podataka. Ako postoji, generira se JWT token (koji sadrži korisnički email i ID). Na kraju, ta funkcija kreira URL (čarobnu vezu) koji sadrži ovaj token i šalje ga na korisnikov email putem „*Nodemailer*“ servisa.

```
const sendMagicLinkEmail = async (email, magicLink) => {
    try {
        let info = await transporter.sendMail({
            from: `"PhotoGram Support" <${emailSender}>`,
            to: email,
            subject: 'Magic Link for login',
            html: `<p>Click the following link to sign in: <a
href="${magicLink}">${magicLink}</a></p>`
        });

        console.log('Magic link sent:', info.messageId);
        return info.messageId;
    } catch (error) {
        console.error('Error sending magic link:', error);
        throw error;
    }
};
```

Kod 3 Funkcija koja šalje čarobnu vezu na korisnikov email

```
const MagicLogin = () => {
    const dispatch = useDispatch();
    const { token } = useParams();

    useEffect(() => {
        const handleAuthentication = async () => {
            try {
```

```
                const response = await
authenticateWithMagicLink(token);

                if (response && response.authToken) {
                    const profileData = {
                        result: response.user,
                        token: response.authToken
                    };
                    localStorage.setItem('profile',
JSON.stringify(profileData));
                    dispatch({ type: 'AUTH', data: profileData
});
                    window.location.href = '/posts';
                } else {
                    throw new Error('Authentication failed. No
authToken found.');
                }
            } catch (error) {
                console.error('Error during authentication:',
error);

            }
        };
        handleAuthentication();
    }, [dispatch, token]);

    return (
        <div>

            <p>Authenticating...</p>
        </div>
    );
};

export default MagicLogin;
```

Kod 4 Prikaz „*MagicLogin*“ komponente

Kada korisnik klikne na čarobnu vezu koji je primio putem e-pošte, otvara se aplikacija na ruti /auth/magic-login/:token. Ovaj URL sadrži JWT token u parametrima, koji se iz URL-a preuzima u komponenti „*MagicLogin*“, kod 4, pomoću *useParams*() iz React Router-a.

```
const authenticateWithMagicLink = async (token) => {
    try {
        const response = await
axios.get(`http://localhost:5000/user/authenticateWithMagicLink
/${token}`);
        return response.data;
    } catch (error) {
        console.error('Error authenticating with magic link:',
error);
        throw error;
    }
};

export default authenticateWithMagicLink;
```

Kod 5 Prikaz funkcije *autenticateWithMagicLink*

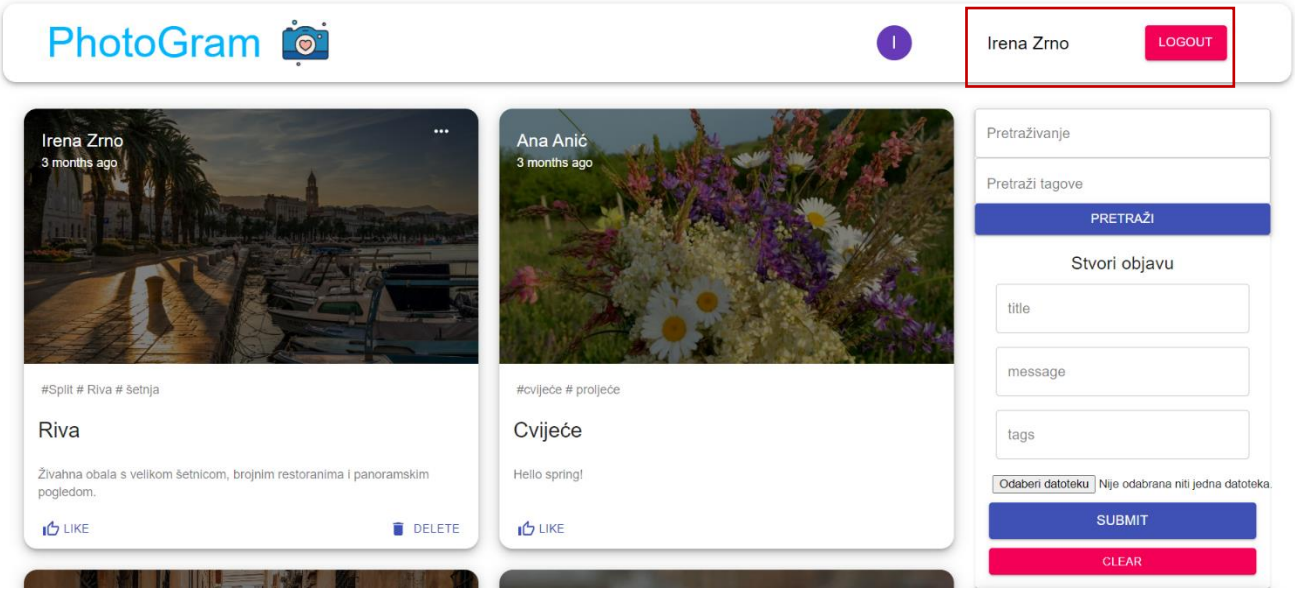
Funkcija „*handleAuthentication*“ koja se nalazi u komponenti „*MagicLink*“, sadrži u sebi funkciju koja se zove „*authenticateWithMagicLink*“ koja šalje GET zahtjev prema backend-u radi validacije tokena.

```
export const authenticateWithMagicLink = async (req, res) => {
    const { token } = req.params;

    try {
        const decodedToken = jwt.verify(token, secretKey);
        const existingUser = await User.findOne({ email:
decodedToken.email });

        if (!existingUser) {
            return res.status(404).json({ message: 'User not
found.' });
        }
        const authToken = jwt.sign({ email: existingUser.email,
id: existingUser._id }, secretKey, { expiresIn: '1h' });

        res.status(200).json({ authToken, user: existingUser,
message: 'User authenticated successfully.' });
    } catch (error) {
        console.error('Error verifying magic link:', error);
        res.status(401).json({ message: 'Invalid or expired
magic link.' });
```

```
        }
    };
```

Kod 6 Funkcija na backend-u koja validira token

Nakon što zahtjev dođe na backend, funkcija „`authenticateWithMagicLink`“, kod 6, validira token. Ako je token validan, pronalazi korisnika u bazi na osnovu emaila iz tokena i generira novi token koji traje 1 sat.



Slika 9 Prikaz aplikacije nakon prijave putem čarobne veze

Ako je autentifikacija uspješna, podaci o korisniku (uključujući novi token) se vraćaju na frontend. Ovi podaci se zatim čuvaju u localStorage-u i ažuriraju se u Redux stanju pozivom *dispatch({ type: 'AUTH', data: profileData* }). Nakon toga, korisnik se preusmjerava na glavnu stranicu aplikacije (npr. /*posts*) – što se može vidjeti na slici 9.

Drugi dio implementacije praktičnog dijela je prijava korisnika pomoću otiska prsta preko OwnID aplikacije. OwnID omogućuje sve prednosti FIDO autentifikacije na način koji je jednostavan za implementaciju i prikladan za korisnike web stranica. Cilj FIDO autentifikacije je smanjiti upotrebu lozinki i unaprijediti sigurnosne standarde na stolnim računalima i mobilnim uređajima. FIDO je osmišljen kako bi zaštitio sigurnost i privatnost korisnika, pri čemu privatni ključevi i biometrijski podaci, ako se koriste, nikada ne napuštaju uređaj. Umjesto složenih lozinki, korisnici mogu koristiti otisak prsta ili jednokratni PIN za autentifikaciju.

Prvo je potrebno napraviti račun na web stranici https://console.ownid.com i odabrati vrstu aplikacije. Zatim, u bazi podataka je potrebno kreirati polje pod nazivom „*ownIdData*“ za

svakog korisnika. Ovo polje će se nalaziti u tablici koja pohranjuje korisničke podatke. Nakon toga, potrebno je implementirati tri krajnje točke koje će OwnID poslužitelji koristiti za autentifikaciju korisnika:

1. /*setOwnIDDataByLoginId*: Ova krajnja točka omogućuje pohranjivanje podataka u polje ownIdData za odgovarajućeg korisnika u bazi podataka (kod 7).
2. /*getOwnIDDataByLoginId*: Ova krajnja točka vraća niz podataka iz polja *ownIdData* za korisnika specificiranog u zahtjevu (kod 8).
3. /*getSessionByLoginId*: Ova krajnja točka vraća korisničku sesiju, JWT token, omogućujući autentifikaciju korisnika putem OwnID poslužitelja (kod 9).

```
export const setOwnIDDataByLoginId = async (req, res) => {
    const email = req.body.loginId;
    const ownIdData = req.body.ownIdData;
    try {
        const user = await User.findOne({ email });
        if (!user) {
            return res.status(404).json({ errorCode: 404 });
        }
        user.ownIdData = ownIdData;
        await user.save();
        return res.sendStatus(204);
    } catch (error) {
        console.error('Error setting OwnID data:', error);
        res.status(500).json({ message: 'Failed to set OwnID
data.' });
    }
};
```

Kod 7 Prikaz *setOwnIDDataByLoginId* koda

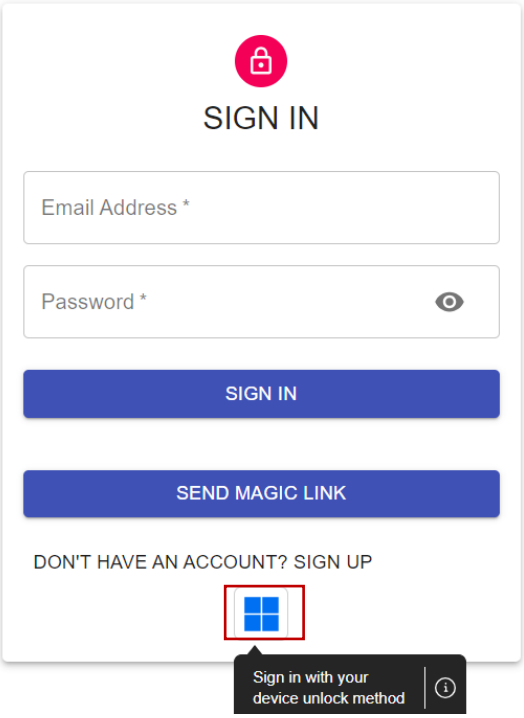
```
export const getOwnIDDataByLoginId = async (req, res) => {
    const email = req.body.loginId;
    try {
        const user = await User.findOne({ email });
        if (!user) {
            return res.status(404).json({ errorCode: 404 });
        }
        return res.json({ ownIdData: user.ownIdData });
    } catch (error) {
```

```
        console.error('Error getting OwnID data:', error);
        res.status(500).json({ message: 'Failed to get OwnID
data.' });
    }
};
```

Kod 8 Prikaz *getOwnIDDataByLoginId* koda

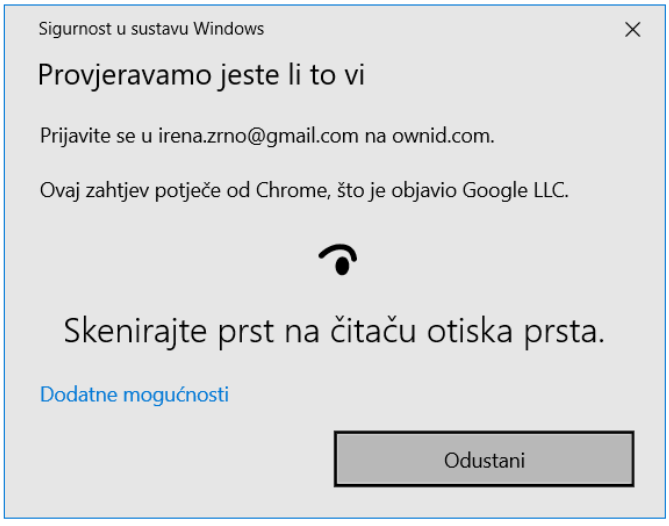
```
export const getSessionByLoginId = async (req, res) => {
    const email = req.body.loginId;
    try {
        const user = await User.findOne({ email });
        if (!user) {
            return res.status(404).json({ errorCode: 404 });
        }
        const token = jwt.sign(
            { email: user.email, name: user.name },
            'test',
            { expiresIn: '1h' }
        );

        return res.json({ token });
    } catch (error) {
        console.error('Error getting session:', error);
        res.status(500).json({ message: 'Failed to get
session.' });
    }
};
```

Kod 9 Prikaz *getSessionByLoginId* koda



Slika 11 Prikaz gumba za biometrijsku autentifikaciju

Pritiskom gumba za biometrijsku autentifikaciju (slika 11), otvara se novi prozor na gdje se korisnik autentificira, slika 12. Ako se uspješno autentificira, onda ga vraća na početnu stranicu aplikacije i prijavljuje ga, kao na slici 9.



Slika 12 Prikaz prozora za biometrijsku autentifikaciju

6 Zaključak

Analizom različitih metoda autentifikacije u okviru ovog rada, uključujući autentifikaciju putem lozinki i PIN-ova, autentifikaciju posjedovanjem, te biometrijsku autentifikaciju, dolazi se do ključnih uvida u trenutno stanje i izazove u zaštiti korisničkih podataka. Svaka od metoda nosi svoje specifične prednosti i nedostatke koji su relevantni za različite scenarije upotrebe i razine sigurnosti.

Autentifikacija putem lozinki i PIN-ova, iako široko prihvaćena i lako implementirana, suočava se s brojnim sigurnosnim rizicima, uključujući mogućnost krađe lozinki, zaborava i napada poput „phishinga“. Ove metode, iako pristupačne, često zahtijevaju dodatne mehanizme zaštite kako bi se osigurala njihova efikasnost i sigurnost.

S druge strane, autentifikacija posjedovanjem, uključujući RFID kartice i OTP tokena, donosi dodatni sloj sigurnosti koji otežava neovlašteni pristup. Ipak, ove metode nisu bez mana, s obzirom na potencijalne probleme poput presretanja signala i potrebe za fizičkom prisutnošću korisnika. Ove karakteristike zahtijevaju inovativne pristupe i poboljšanja kako bi se maksimizirala njihova sigurnost i praktičnost.

Biometrijska autentifikacija, koja se oslanja na jedinstvene fizičke karakteristike korisnika, predstavlja značajan korak naprijed u unapređenju sigurnosti i korisničkog iskustva. Ova metoda nudi visoku preciznost i teško ju je replicirati ili zloupotrijebiti. Međutim, izazovi kao što su mogućnost "spoofing" napada i varijacije u biometrijskim podacima korisnika ukazuju na potrebu za dodatnim istraživanjima i razvojem kako bi se osigurala maksimalna efikasnost i pouzdanost.

Zaključno, izbor odgovarajuće metode autentifikacije zavisi od specifičnih zahtjeva i rizika povezanih s određenim sustavima i aplikacijama. Kombinacija više metoda, često označena kao višefaktorska autentifikacija, može pružiti optimalnu ravnotežu između sigurnosti i korisničkog iskustva. Budući razvoj tehnologije i stalna evolucija prijetnji zahtijevaju stalno usklađivanje i unapređenje autentifikacijskih praksi kako bi se osigurala adekvatna zaštita u dinamičnom digitalnom okruženju. Ovaj rad naglašava važnost integracije inovativnih pristupa i stalne evaluacije postojećih metoda kako bi se osigurala sigurnost i pouzdanost u autentifikaciji korisnika.

LITERATURA

1. Farik, Mohammed & Lal, Nilesh & Prasad, Shalendra. (2016). A Review Of Authentication Methods. International Journal of Scientific & Technology Research. 5. 246-249. , 26. lipnja 2024.
2. Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, Sarminah Samad, Authentication systems: A literature review and classification, Telematics and Informatics, Volume 35, Issue 5, 2018, Pages 1491-1511, ISSN 0736-5853, 26.lipnja 2024.
3. S interneta, https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview, 26. lipnja 2024.
4. S interneta, https://cybersecurity.asee.io/blog/history-of-authentication/, 27.lipnja 2024.
5. S interneta, https://workos.com/blog/a-developers-history-of-authentication, 27. lipnja 2024.
6. S interneta, https://ventex.hr/hr/novosti/Zasto-koristiti-visefaktorsku-autentifikaciju/ , 30. kolovoza 2024.
7. Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 2013, 7 (5),pp.95-107. ffhal-00912435, 27. lipnja 2024.
8. S interneta, https://security.foi.hr/wiki/index.php/Pametne_kartice.html, 30.kolovoza 2024.
9. S interneta, https://commons.wikimedia.org/wiki/File:RSA_SecurID_Token_Old.jpg, 30. kolovoza 2024.
10. S interneta, https://kosuta.com.hr/modern_Products-133356, 30. kolovoza 2024.
11. S interneta, https://www.ssl.com/guide/how-to-enable-otp-sms-two-factor-authentication-for-esigner-cloud-code-or-document-signing/, 30.kolovoza 2024.

12. Smith-Creasey, M. (2024). Continuous Biometric Authentication Systems: An Overview. Njemačka: Springer International Publishing, 29.lipnja 2024.
13. Erlich, Zippy. “Identification and Authentication: Technology and Implementation Issues.” Communications of the Association for Information Systems (2006), 12. srpnja 2024.
14. S interneta, https://www.techjuice.pk/bank-biometric-verification-last-date/, 30. kolovoza 2024.
15. S interneta, https://www.microsoft.com/en-us/security/business/security101/what-is-two-factor-authentication-2fa?msockid=19e21d2b98326cbf0ecc0cc399836d96, 30. kolovoza 2024.
16. S interneta, https://haveibeenpwned.com/Passwords, 30. kolovoza 2024.
17. S interneta, https://www.logintc.com/types-of-authentication/password-authentication/, 29.kolovoza 2024.
18. S interneta, https://www.descope.com/learn/post/password-authentication, 29.kolovoza 2024.
19. S interneta, https://www.researchgate.net/publication/220745779_Security_and_usability_the_case_of_the_user_authentication_methods, 30. kolovoza 2024.
20. S interneta, https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en, 30.kolovoza 2024.
21. Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications, 188, Article 103080, 31.kolovoza 2024.