Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/14BE13Mihajlovic

UPOTREBLJIVOST SIGURNOSNIH MEHANIZAMA VEB APLIKACIJA

USABILITY OF WEB APPLICATION SECURITY MECHANISMS

Dragana Mihajlović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – RAČUNARSTVO I AUTOMATIKA

Kratak sadržaj – *U ovom radu su prikazani osnovni principi online plaćanja i balans između upotrebljivosti i sigurnosti. Predstavljeni su načini autentifikacije za koje korisnici smatraju da su najjednostavniji i najsigurniji te su predstavljeni zahtjevi koji se moraju ispoštovati za poslovanje na Internetu. U ekperimantalnom dijelu analizirane su dvije aplikacije za obavljanje transakcija te vrijeme potrebno za njihovo izvršavanje. Opisane su prednosti i mane aplikacija kao i poboljšanja koja su potrebna da se implementiraju za bolju sigurnost i upotrebljivost.*

Ključne reči: *korisnički interfejs, bezbednost, upotrebljivost, ranjivost, KLM-GOMS.*

Abstract – *This paper explains the basic concepts of online payment and the balance between usability and security. The methods of authentication that users consider to be the simplest but also the most secure are presented as well as the requirements that must be met for doing business on the Internet. In the experimental part, two applications for performing transactions and the time required for their execution were analyzed. The advantages and disadvantages of applications as well as the improvements needed to be implemented for better security and usability are described.*

Keywords: *user interface, security, usability, vulnerability, KLM-GOMS.*

1. UVOD

Savremeni način života donosi brz tempo te prelazak na digitalno plaćanje naglo raste posebno uzimajući u obzir činjenicu o rastu prekogranične kupovine koja otvara više mogućnosti samim trgovcima ali i potencijalnim kupcima. Razvojem Interneta, evolucija sistema elektronskog plaćanja je još više napredovala.

Pored e-trgovine sve više aktuelna je i m-trgovina koja predstavlja sprovođenje aktivnosti koje su i finansijske i promotivne prirode uz pomoć mobilnih telefona ali uključuju i upotrebu drugih bežičnih uređaja.

Fleksibilan i upotrebljiv interfejs je potrebno postići uz poštovanje svih propisanih i zahtjevanih standarda koje je potrebno ispoštovati u cilju postizanja sigurnosti transakcija i ličnih podataka klijenata.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dragan Ivetić, red. prof.

2. NAČINI PLAĆANJA NA INTERNETU

Da bi poslodavci uspjeli na današnjem globalnom tržištu i da bi se izborili protiv stranih konkurenata, moraju svojim kupcima ponuditi atraktivne uslove prodaje podržane odgovarajućim načinima plaćanja. Neki od korišćenih načina plaćanja na Internetu su [1]: elektronske platne kartice, elektronski čekovi, elektronski keš, elektronski novčanici, *P2P* plaćanja, plaćanje vaučerima, mikroplaćanja, mobilna plaćanja, sistemi zasnovani na zlatu i kriptovalute. Za svaku metodu (npr. kreditne kartice) postoji više opcija (*Visa*, *Mastercard* i *American Express*, i druge). Generalno, postoji više od 200 alternativnih načina plaćanja širom svijeta.

2.1. Elektronske platne kartice

Plaćanje kreditnim karticama postaje sve popularnije. Razlog za ovo jeste što se kartice mogu koristiti na bilo kojoj lokaciji uz ispunjavanje određenih uslova. Za plaćanja na Internetu mogu se koristiti svi tipovi platnih kartica. Bez obzira na tip kartice, proces realizacije plaćanja je sličan. Ključnu ulogu u sistemu plaćanja ima *payment gateway* koji predstavlja ekvivalent terminalu na fizičkom mjestu prodaje (*POS*). *Payment gateway* omogućava autorizaciju platnih kartica i siguran transfer informacija između mjesta plaćanja preko Interneta (veb-sajt, mobilna aplikacija i sl.) i procesora plaćanja odgovarajuće banke. *Payment gateway* enkripcijom štiti osjetljive informacije s kreditnih kartica. Najbitnija karakteristika platnih kartica jeste *real time* autorizacija transakcije. Podaci su organizovani na način da je korisniku omogućen lak i jednostavan uvid u podatke koji su potrebni prilikom *online* plaćanja. Segmetni koji se izdvajaju olakšavaju korisniku prikaz podataka koji su mu od interesa u trenutku u kojem su mi potrebni.

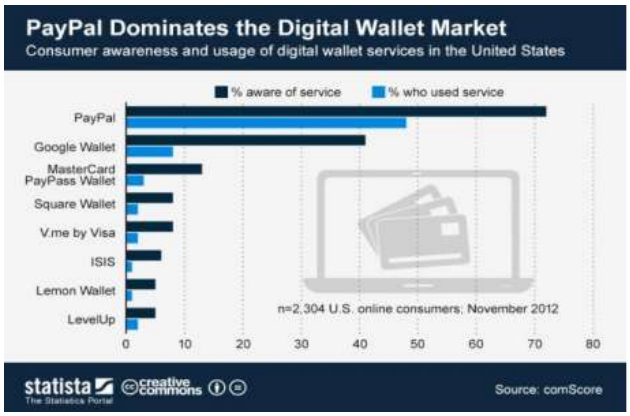
2.2. Elektronski novčanici

Elektronski novčanici (*E-wallet*) su aplikacije koje predstavljaju unapređenje standardnih načina plaćanja, kao što su kartice ili transfer preko banke. Zasnivaju se na nalozima korisnika koji su otvoreni kod provajdera elektronskog novčanika. Nakon uplate depozita, korisnik može da kupuje na veb-sajtovima, tako što se uloguje na svoj elektronski novčanik. Digitalni novčanik posjeduje softversku komponentu i komponentu podataka. Softver obezbeđuje sigurnost i enkripciju vezanu za lične podatke i aktuelne transakcije. Komponenta podataka sadrži podatke kao što su adresa dostave, adresa računa, metode plaćanja (broj kreditne kartice, datum isteka, sigurnosni brojevi) i druge informacije. Najznačajniji provajderi elektronskog novčanika su Google i PayPal. Elektronski novčanici omogućavaju i slanje i primanje novca od drugih osoba na jednostavan način ali prednost koja se

ističe jeste dostupnost *e-wallet*-a 24/7 za razliku od banaka koje imaju svoje radno vrijeme. Tradicionalni novčanici su podložni fizičkoj krađi koja je jako česta za razliku od *e-wallet*-a. Takođe, e-novčanici omogućavaju privatnost lozinki kao i *two step* autentifikaciju ali i biometrijsku autentifikaciju. Upotreba aplikacija za mobilno plaćanje i elektronskih novčanika se vremenom sve više povećava te stoga raste potražnja za poboljšanim korisničkim iskustvom tokom interakcije sa ovim aplikacijama.

Oblast interakcije čovjek-računar (*Human computer interaction*) fokusira se na dizajn, evaluaciju i primjenu interaktivnih računarskih sistema za ljudske potrebe. Jedan aspekt *HCI*-a je upotrebljivost, tj. kvalitet interakcije sa aplikacijom ili sistemom. Aplikacije za mobilno plaćanje obično imaju komplikovanije funkcije od prosječnih aplikacija za pametne telefone. Funkcije tih aplikacija se tiču novca te potražnja za upotrebljivost i dobar dizajn koji daje osećaj sigurnosti je veći.

Kako se navodi u radu *E-wallet - designed for usability* [2] koncept e-novčanika i njegovih funkcija su pokazali da zbunjuju mnoge korisnike sa kojima se vršilo testiranje. Korisnici su imali poteškoća da razumiju kako se čuvaju valute i kako se same transakcije odvijaju. Potrebno je uvesti novu terminologiju koja je bliska velikom broju korisnika i svesti funkcionalnosti na način koji bi korisnicima bio intuitivan, tj.potrebno je da se ispoštuje deseti Nilsenov princip - Nalikovati stvarnosti. Takođe, potrebno je veliku količinu informacija predstaviti jasno, na minimalistički način. Ovo su samo neke od stvari koje se moraju ispoštovati kako bi aplikacija mogla da radi u okruženju sa ljudima koji nemaju ranija iskustva sa e-novčanicima. Prema *Com Score*-u [3] studiji samo 51 procenat potrošača koji su odgovorili je ikada čulo za digitalnu uslugu plaćanja koja nije *PayPa*l, a samo 12 procenata potrošača je ikada koristilo jednu takvu aplikaciju. Usluga plaćanja *PayPal*-om trenutno je ispred konkurencije u pogledu svijesti i upotrebe potrošača i čini se malo vjerovatnim da bilo koja od konkurentskih usluga može uskoro da smanji taj jaz (Slika 1).



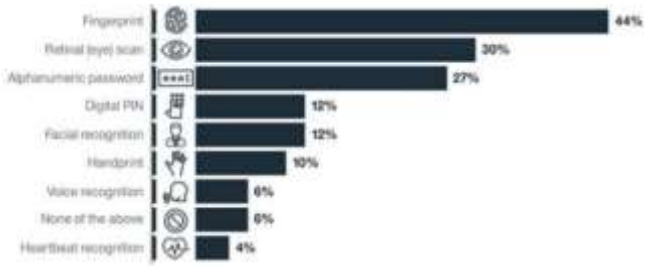
Slika 1. *Pregled zastupljenosti servisa e-wallet-a [3]*

3. RAZVOJ AUTENTIFIKACIJE I AUTORIZACIJE

Povjerenje je nešto na čemu se zasnivaju ljudski odnosi, te autentifikacija datira mnogo prije od dostupnih dokumenata koji o njoj govore. Razvoj Interneta i informaciono-komunikacionih tehnologija dovodi do digitalnog doba u kojem su problemi sa transakcionim metodama autentifikacije pojačani. Kako se navodi u studiji kompanije *IBM Security*, koja ispituje pogled potrošača u vezi sa digitalnim identitetom i autentifikacijom, ljudi daju prednost sigurnosti, a ne pogodnosti kada se prijavljuju u aplikacije i uređaje te se biometrija smatra sigurnijom od lozinki. Bezbednost je u pomenutoj anketi visoko rangirana kao glavni prioritet za bankarstvo.

U prosjeku je 70% anketiranih izabralo bezbednost kao glavni prioritet, a 16% odabralo je privatnost, dok je 14% odabralo pogodnost. Za aplikacije na društvenim mrežama prioriteti su se skoro izjednačili - pogodnost (36 procenata), zatim bezbednost (34 procenta) i privatnost (30 procenata).

Istraživanje je takođe ispitalo mišljenja potrošača o sigurnosti različitih metoda prijave i otkrilo je da se na određene vrste biometrije gleda kao na sigurnije od lozinki, ali sigurnost i privatnost i dalje ostaju glavna briga kada je u pitanju usvajanje biometrije. Čak je 44 procenta ispitanih biometriju otiska prsta rangirao kao jedan od najsigurnijih načina autentifikacije, dok lozinke i PIN-ovi smatrani manje sigurnim (Slika 2). Najveća briga ljudi kod biometrijske potvrde identiteta bila je privatnost (55 procenata) i sigurnost.



Slika 2. *Zastupljenost metoda autentifikacije*

4. DIZAJNIRANJE FORMI ZA PLAĆANJE KREDITNOM KARTICOM

Prilikom dizajniranja formi za plaćanje kreditnom karticom radi maksimalne upotrebljivosti potrebno je obratiti pažnju na niz stvari. Prije svega je potrebno identifikovati minimalne podatke koji su potrebni za obradu uplate i sve drugo osim toga treba eliminisati. Što manje informacija je potrebno manja je vjerovatnoća da će korisnik pogriješiti a samim tim i vrijeme koje je potrebno za obavljanje plaćanja je manje i korisnisi su zadovoljniji. Na primjer, neke forme za plaćanje putem Interneta zahtjevaju unos imena vlasnika kartice a neke ne. Ime koje je navedeno na kartici se ne koristi prilikom obrade uplate i stoga ga treba eliminisati.

Takođe, još jedna stvar koju je potrebno ukloniti jeste i polje za unos tipa kreditne kartice. Naime, tip kreditne kartice se može identifikovati na osnovu prve cifre broja kartice. Ako je u pitanju cifra 4 riječ je o *Visa* kartici, ako je cifra 6 riječ je o *Discover* kreditnoj kartici, cifra 5 govori o *MasterCard* kartici dok cifra 3 na prvom mjestu identifikuje *American Express* karticu. Potrebno je takođe spriječiti moguće greške automatskom provjerom podataka. Nije potrebno čekati da korisnik inicira plaćanje klikom na dugme da bi se prikazala poruka o neispravnom unosu broja kreditne kartice.

5. ANALIZA SIGURNOSTI I UPOTREBLJIVOSTI DVA NAČINA PLAĆANJA KOJA PRUŽA NLB BANKA U BiH

Mobilno bankarstvo NLB mKlik je usluga koja omogućava brz, jednostavan i siguran pristup računima komitenta putem mobilnog telefona koji ima pristup Internetu. Koristeći mobilno bakarstvo moguće je vršiti transakcije u bilo kom trenutku gdje god se korisnik nalazi. Za korišćenje mKlika potrebno je da korisnik posjeduje odgovarajući mobilni uređaj koji ispunjava neophodne tehničke i telekomunikacione uslove.

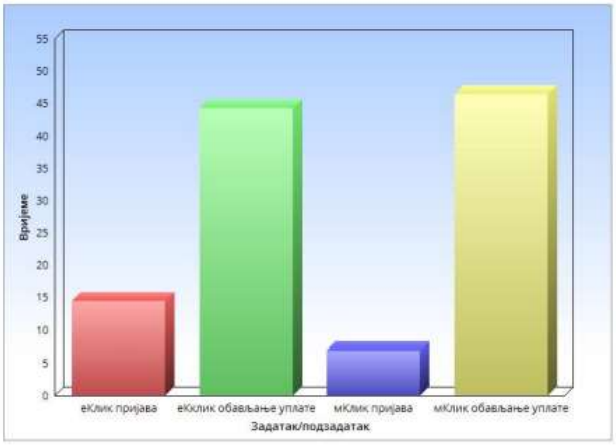
Za sam početak korišćenja potrebno je da korisnik bude klijent banke, tj. da ima kreiran račun u banci. Na osnovu statusa klijenta banke korisnik stiče mogućnost za korišćenje aplikacije za mobilno bankarstvo. Nakon potpisivanja ugovora, u roku od 24 časa klijent prima dva aktivaciona koda: jedan putem SMS-u a drugi putem mejla koji je klijent naveo u banci. NLB eKlik je usluga elektronskog bankarstva koja omogućava korisniku, fizičkom licu, da sa bilo kog mjesta gdje ima pristup internetu, 24 časa dnevno, bez čekanja u redovima, na siguran, brz i jednostavan način izvrši plaćanje svojih obaveza, prenos novca sa transakcionog na štedni račun, izvrši devizno plaćanje, kupovinu, prodaju ili konverziju valuta uz minimalne naknade, uvid u stanje i promjene na računu u domaćem i deviznom platnom prometu, pregled i štampu izvoda. Korisniku je omogućeno dobijanje informacija o stanju i promjenama na svim računima u banci (transakcionom, deviznom štednom, kreditnom i kartičnom).

5.1. Procjena efikasnosti

Za procjenu efikasnosti mKlik-a i eKlik-a za zadatak je izabrano prijavljivanje u sistem i izvršavanje nove transakcije kao najreprezentativnije funkcionalnosti ovih aplikacija. Vršenje nove transakcije je omogućeno na devizni račun, štedni račun, već sačuvan šablon, putem skeniranja i popunjavanjem uplatnice. Nakon odabranog načina i popunjavanjem forme, omogućen je prikaz uplatnice prije konačne potvrde. Nakon potvrde, proces se završava a korisnik se obaveštava o uspješnosti transakcije.

5.2. Rezultati analize

Urađena je analiza zadatka kombinovanjem miša i tastature ali i upotrebom isključivo tastature. Rezultati analize eKlik aplikacije pokazuju da se zadatak najbrže obavlja upotrebom isključivo tastature (58.61 sekunde). Sljedeći rezultat jeste kombinovanje miša i tastature prilikom prijavljivanja i popunjavanje uplatnice isljučivo putem tastature (61.73 sekunde). Treći rezultat za obavljanje ovog zadatka jeste prijavljivanje putem tastature a popunjavanje uplatnice kombinovanjem miša i tastature (64.58 sekunde). Najviše vremena za obavljanje opisanog zadatka jeste prijavljivanje i popunjavanje uplatnice kombinovanjem miša i tastature. Za obavljanje istog zadatka putem mKlik aplikacije potrebne su 53.36 sekunde. Može se zaključiti da je vrijeme izvršavanja uplate na drugi račun putem mKlik aplikacije kraće od vremena izvršavanja uplate putem eKlik aplikacije u bilo kom od prethodno opisanih slučajeva. Međutim, treba uzeti u obzir da forme nisu identične iako se radi o istom zadatku. Adresa primaoca je dodatno polje koje se koristi ako se uplaćivanje vrši putem mobilne mKlik aplikacije. Takođe, podjeljenost formi u više segmenata i iniciranje dugmeta za nastavak popunjavanja uplatnice su dodatni faktori koji su uticali na skoro izjednačavanje ovih vremena. Na Slici 3 se može vidjeti odnos vremena koje je potrebno da bi se korisnik prijavio na sistem preko eKlik i mKlik aplikacija kao i odnos vremena koje je potrebno da se obavi zadatak uplate na drugi račun. Prikazani su najbolji rezultati analize eKlik i mKlik aplikacija.



Slika 3. *Odnos vremena potrebnog za obavljanje definisanog zadatka*

Svaka mBanking aplikacija zahtjeva mobilni ili tablet uređaj, dok za eBanking je potreban desktop računar ili laptop. Mobilno bankarstvo zahtjeva od korisnika da na svom pametnom telefonu preuzme zvaničnu aplikaciju odgovarajuće banke da bi koristio širok spektar usluga koje banka nudi. U slučaju transakcija sa *3D Secure* zaštitom korisnik se redirektuje na drugu stranicu na kojoj unosi dodatni sigurnosni kod što se rezultuje dužim vremenom za obavljanje transakcije. U slučaju mKlik aplikacije sam pristup telefonu je zaštićen (šablon, pin, otisak prsta, ili prepoznavanje lica) te se mogućnost pristupu transakcionim podacima smanjuje.

S druge strane, na eKlik aplikaciji kao veb aplikaciji korisniku je data mogućnost čuvanja lozinke i korisničkog imena. Ako je korisnik sačuvao ove podatke stečena je mogućnost prijavljivanja na eKlik nalog čime su svi transakcioni podaci i mogućnost obavljanja transakcija izloženi zloupotrebi.

Korišćenjem mKlik aplikacije korisnik ima veći osjećaj sigurnosti i kontrole. Korisnik, takođe, ima osjećaj posjedovanja aplikacije i samim tim osjećaj pri radu je mnogo pozitivniji u odnosu na eKlik aplikaciju u kojoj se korisnik nalazi na sajtu banke. Dobra implementacija opcija *Undo* i *Redo* korisniku daje veću slobodu upoznavanja sa aplikacijom i mogućnostima koje ona nudi.

Veb aplikacija, eKlik, u mnogo većoj mjeri je ispoštovala deseti Nilsenov princip „Nalikovati stvarnosti“ jer sam interfejs podsjeća za stvarnu situaciju (Slika 4). S druge strane mKlik aplikacija nije ispoštovala ovaj princip jer je uplatnica izdvojena po segmentima prilikom popunjavanja forme.

Slika 4. *Izgled uplatnice na eKlik aplikaciji*

6. NFC TEHNOLOGIJA

Svi današnji pametni telefoni opremljeni su tzv. *NFC* (*Near Field Communication*) tehnologijom. Radi se o uobičajenoj bežičnoj tehnologiji koja se razvila zahvaljujući rastu sistema za plaćanje putem Interneta. *NFC* kao i *Bluetooth* i *Wi-Fi* radi na principu slanja informacija preko radio talasa. Danas jedna od najčešćih upotreba *NFC*-a su identifikacione kartice za pristup određenim mjestima poput poslovnih zgrada i privatnih garaža. *NFC* plaćanja su izuzetno sigurna i za razliku od podataka na kartici sa magnetnom trakom, koja je statična, podaci koji su uključeni u *NFC* transakciju su šifrovani i dinamični.

Prednosti koje nudi *NFC* plaćanje su viši stepen sigurnosti, brže obavljanje plaćanja kao i smanjen trošak elektronike, međutim, ograničenja koja postoje su rad u kratkim dometima te je mala brzina prenosa podataka. Iako su *NFC* transakcije sigurnije od standardnog plaćanja kreditnom karticom ova tehnologija nije potpuno bez rizika. Hakeri mobilnih telefona su razvili načine neovlašćenog pristupa ličnim finansijskim podacima uskladištenim na telefonima te se još uvijek radi na bezbednosti. Takođe, problem koji je češći jeste gubljenje telefona što rezultuje mogućnosti da će vlasnik telefona na kojem se nalaze finansijski podaci biti opljačkan. Upravo zbog ovoga su transakcije sa *NFC* tehnologijom obično ograničene po vrijednosti.

7. 3D SECURE 2 - MEĐUNARODNI SIGURNOSNI STANDARD

Za korisnika platne kartice *3D Secure 2* podrazumijeva da se transakcije koje se obavljaju kod Internet trgovaca, koji takođe podržavaju navedeni standard, dodatno potvrđuju jednokratnom lozinkom koju korisnik dobija putem SMS poruke. Internet trgovci koji podržavaju pomenuti protokol su sigurni te je mogućnost zloupotrebe svedena na minimum. U analizi koja se sprovela pokazalo se da transakcije sa *3D* zaštitom zahtjevaju više vremena i korisnikove pažnje. Minimalno dodatno vrijeme koje je potrebno iznosi 11.24 sekunde u idealnom slučaju. Ovaj vid zaštite je svakako korak naprijed kada su u pitanju sigurne transakcije, međutim, reakcija korisnika i nije. Preusmjeravanje kupaca na drugu stranicu može uticati na poslovanje trgovaca i ono je glavna mana korišćenja spoljne usluge za plaćanje. Ovim se smanjuje povjerenje i može se rezultirati napuštenim prodavnice. Takođe, potrebno je razmotriti koliko koraka kupci moraju da prođu prilikom plaćanja. Loše dizajniran postupak plaćanja može naštetiti broju prodaja čak i ako trgovci pružaju najbolji proizvod ili uslugu. Ovo se dešava zato što se redirektuje na potpuno drugačiju stranicu te se preusmjeravanjem oduzima prilika za prikazivanje dodatnih ponuda čime se broj potencijalnih kupovina smanjuje. U kontekstu ljudskog osjećaja mKlik aplikacija se pokaza boljom prije svega zbog toga što se koristi posebna aplikacija gdje je sam pristup telefonu zaštićen te je krajnja potvrda transakcije lakša.

8. ZAKLJUČAK

Zahvaljujući sve većoj upotrebi *online* kupovine, sistemi plaćanja preko Interneta postaju dominantan oblik plaćanja. Od elektronskih sistema plaćanja se zahtjeva veća jednostavnost korišćenja, dostupnost i brzina. U budućnosti se očekuje značajnija primjena sistema plaćanja preko Interneta za servise i proizvode koji se realizuju u *G2C (Government to Consumer)* i *B2B (Business to Consumer)* formama elektronskog poslovanja [4]. Dizajniranje grafičkog korisničkog interfejsa je složen i odgovoran posao posebno ako je potrebno uraditi dizajn za različite tipove korisnika. S druge strane, u sistemima koji su se opisivali mora biti obezbeđena sigurnost podataka kako bi korisnici osjećali prijatnost tokom plaćanja. Analiza je pokazala da forme koje danas postoje nisu najbolje te je potrebno da poslodavci, koji još uvijek sadrže nedostatke koji su navedeni, uklone dijelove formi koji opterećuju korisnika i povećavaju mogućnost za njihove greške. Mobilna mKlik i veb eKlik aplikacija imaju i prednosti i mana. Zajednička prednost svih veb aplikacija jeste mogućnost rada bez obzira na operativni sistem koji ja instaliran na korisnikovom računaru. Danas je korisnički interfejs postao jedan od glavnih segmenata prilikom kreiranja aplikacija. Budući razvoj aplikacija će sigurno više da uključuje potencijalne korisnike koji će predstavljati najvažniju ulogu za unapređenje aplikacija, postojećih i novih proizvoda i usluga.

9. LITERATURA

[1] „Trade”, https://www.trade.gov/methods-payment [Datum pristupa: 15.04.2021.]

[2],,Diva-portal”,http://www.diva-portal.org/smash/get/diva2:1322382/FULLTEXT01.pdf [Datum pristupa: 23.04.2021.]

[3],,Statistal”,https://www.statista.com/chart/873/consumer-awareness-and-usage-of-digital-walletservices [Datum pristupa: 25.04.2021.]

[4],,IEEE Citation Guidelines2”, https://ieee-dataport.org/sites/default/files/analysis/27/IEEE%20Citation%20Guidelines.pdf [Datum pristupa: 10.05.2021.]

Kratka biografija:

Dragana Mihajlović je rođena u Srbinju 1997. god. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Računarstvo i automatika odbranila je 2021.god.

kontakt: draganamihajlovic1609@gmail.com