BIOMETRIČNA VERIFIKACIJA KOT STORITEV V OBLAKU – PRIMER UPORABE

Jernej Bule, Đorđe Kesić, Peter Peer

Laboratorij za računalniški vid, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani, Tržaška cesta 25, 1000 Ljubljana
E-pošta: {jernej.bule, peter.peer}@fri.uni-lj.si, dordekesic.keso@gmail.com

POVZETEK: *Ko govorimo o avtentikaciji na internetu, v večini primerov še vedno mislimo na gesla. Eden izmed največjih problemov trenutnih avtentikacijskih pristopov je vsekakor dejstvo, da si mora uporabnik zapolniti preveliko število uporabniških imen in gesel, kar vodi k pozabljanju ali uporabi istih uporabniških imen in gesel za različne spletne strani. Rešitev tega problema lahko najdemo v uporabi biometrije. V članku predstavljamo biometrično verifikacijo kot storitev v oblaku in primer uporabe takšne storitve v aplikaciji za preverjanje prisotnosti študentov na predavanju.*

1. UVOD

Biometrija je relativno pogosto uporabljena v lokalnih okoljih (za privatno uporabo), medtem ko je njena uporaba na internetu zelo redka. Glavni razlog za to dejstvo so odprta vprašanja, ki se nanašajo predvsem na dostopnost, razpoložljivost in hitrost obstoječe biometrične tehnologije.

Glede na hitro naraščanje biometričnih podatkov in vedno večja pričakovanja uporabnikov bo v bližnji prihodnosti potrebno imeti visoko razširljive biometrične sisteme, ki bodo lahko operirali nad ogromno količino podatkov (procesorska moč) in hkrati zagotavljali ustrezne kapacitete za hrambo podatkov [1]. Teh lastnosti s tradicionalnimi biometričnimi sistemi ni mogoče zagotoviti. Mnogo strokovnjakov se strinja, da se rešitev nahaja v integraciji obstoječih biometričnih sistemov v oblačne platforme, ki omogočajo ustrezno razširljivost tehnologije, zadostno količino prostora za hrambo podatkov, možnost paralelnega procesiranja in z razširjeno uporabo mobilnih naprav tudi možnost dostopa do takšnih storitev preko mobilnega telefona [2]. Računalništvo v oblaku torej lahko rešuje vprašanja in probleme v zvezi z uporabo nove generacije biometričnih tehnologij, hkrati pa ponuja nove možnosti uporabe obstoječih biometričnih sistemov in aplikacij.

2. BIOMETRIJA IN STORITVE V OBLAKU

2.1. Storitve v oblaku

Način uporabe programske in strojne opreme se je v zadnjem času zelo spremenil. Uporaba storitev nameščenih na lokalnih računalnikih in strežnikih se zmanjšuje, medtem, ko se vse več uporabljajo oblačne storitve. Oblačne storitve so nameščene na

strežnikih ponudnikov oblačnih storitev, kar je v nasprotju s tradicionalnim pristopom nameščanja opreme na lokalne strežnike podjetja. Računalništvo v oblaku je načrtovano na način, da omogoča preprost in fleksibilen dostop do aplikacij, virov in različnih storitev. Storitve so največkrat nameščene v virtualnih okoljih in so v celoti vzdrževane s strani ponudnika. Uporabniki jih lahko dinamično prilagajajo glede na lastne potrebe. Ker ponudnik storitev priskrbi strojno in programsko opremo potrebno za pravilno delovanje, ni potrebe po lastni porabi virov za vzdrževanje. Primeri oblačnih storitev vključujejo spletna podatkovna skladišča (angl. online data storages), rešitve na področju varnostnih kopij, e-poštne storitve ipd. Bistvene prednosti, ki jih ta tehnologija prinaša so cenovna učinkovitost, skalabilnost, varnost, neodvisnost lokacije od naprave, varnostno kopiranje, redundanca.

2.2. Biometrični sistemi

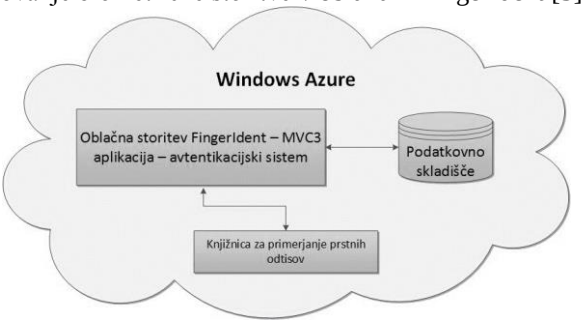
Biometrija se dandanes v svetu uveljavlja kot glavna metoda za identifikacijo in verifikacijo oseb. Ko govorimo biometriji, običajno mislimo na prstne odtise, obraz, šarenico, glas, hojo, podpis, itd. Biometrična identifikacija se nanaša na prepoznavanje posameznika na podlagi edinstvenih fizioloških ali vedenjskih značilnosti. V teoriji in praksi obstajata dva tipa biometričnih značilnosti. Prvi tip temelji na značilnostih, ki so pridobljene z direktnim fizičnim kontaktom z biometričnim čitalcem (npr. prstni odtis, vzorec šarenice itd.), medtem ko drugi tip ne zahteva fizičnega kontakta s čitalcem (npr. oblika obraza, glas itd.). V sistemih, kjer je zahtevana visoka stopnja varnosti, je identiteto osebe mogoče preverjati s kombinacijo več biometričnih metod, ob tem pa upoštevati stopnjo napake posamezne biometrične metode. Delovanje biometričnega sistema lahko razdelimo na dva glavna dela. To sta registracija uporabnika (ang. Enrollment) in proces identifikacije uporabnika (ang. Identification). V procesu registracije se s pomočjo biometrične naprave zajamejo podatki, v naslednji fazi pa se preveri kvaliteta zajetega vzorca. Če je kvaliteta ustrezna, se v zajetem vzorcu poiščejo značilnosti, ki se shranijo v bazo. V procesu identifikacije se na zajetem vzorcu poiščejo značilnosti, ki se primerjajo s tistimi, ki so shranjeni v bazi. Uporabnik se uspešno identificira, ko pride do ujemanja vzorcev [3].

Medtem, ko je osnovna zgradba biometričnih sistemov bolj ali manj enaka na vseh platformah (in različnih biometričnih modalnostih), vseeno obstajajo aspekti, ki so specifični za oblačne platforme. Ti aspekti in opis takšne rešitve so podani v naslednjem poglavju.

2.3. Oblačna biometrična storitev FingerIdent

Kot smo izpostavili že v prejšnjem poglavju, imajo biometrični sistemi v oblaku nekaj specifičnih lastnosti v primerjavi s tradicionalnimi biometričnimi sistemi. Kot prvo, biometrični motor je lociran v oblaku in ne na kakšni lokalni enoti, kot je to značilno za tradicionalne biometrične sisteme za kontrolo dostopa. Ta karakteristika omogoča, da je biometrična tehnologija dostopna od kjerkoli in ponuja možnosti za integracijo v katerokoli aplikacijo, ki ima dostop do interneta. Kot drugo, hranjenje biometričnih podatkov v oblaku naredi sistem zelo skalabilen in omogoča hitro ter zanesljivo

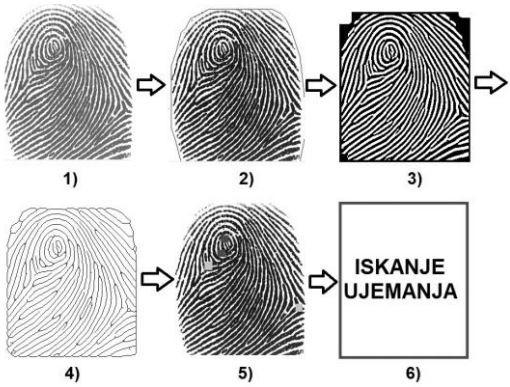
prilagoditev tehnologije ob širitvi baze uporabnikov [2]. V nadaljevanju poglavja predstavljamo delovanje biometrične storitve v oblaku – FingerIdent [3].



Slika 1 - Arhitekturna zgradba oblačne storitve FingerIdent.

Oblačna storitev FingerIdent teče kot .NET spletna storitev in je integrirana v oblačno platformo Microsoft Windows Azure [6], ki je oblačna platforma tipa PaaS. Poganja jo operacijski sistem Windows Azure, ki služi kot osnova vsem aplikacijam in zagotavlja storitve, potrebne za razvoj, upravljanje in gostovanje aplikacij. Za implementacijo smo uporabili ogrodje MVC3, predvsem zaradi enostavne integracije v oblačno platformo Windows Azure. V aplikacijo smo vgradili lastno knjižnico za primerjanje oseb na podlagi prstnega odtisa in implementirali ustrezno logiko za interakcijo z zunanjimi storitvami [3]. Pri tem smo med drugim morali zagotoviti tudi ustrezno kodiranje za prenos podatkov preko omrežja. Arhitekturna zgradba rešitve je predstavljena sliki 1.

Posamezni koraki procesiranja prstnega odtisa, ki so izvedeni s pomočjo knjižnice za primerjanje odtisov so predstavljeni na sliki 2. V prvi fazi se prstni odtis zajame in loči od ozadja. Nato se izvedeta binarizacija in izboljšanje kvalitete slike. V drugi fazi se grebeni prstnega odtisa stanjšajo na en slikovni element, poiščejo se singularne točke, na koncu pa se izvede iskanje ujemanja.



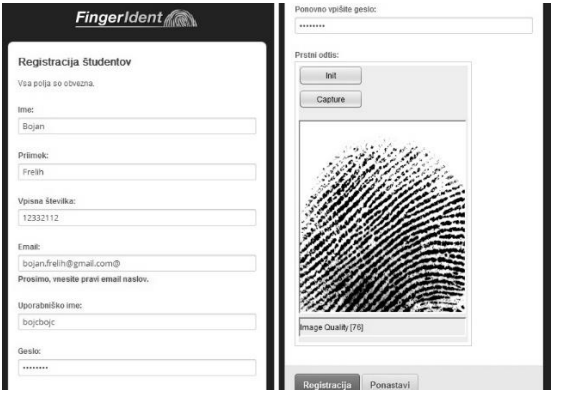
Slika 2 – Koraki procesiranja prstnega odtisa – 1) zajem odtisa, 2) segmentacija, 3) binarizacija in izboljšava kvalitete, 4) tanjšanje grebenov, 5) iskanje singularnih točk, 6) iskanje ujemanja.

Proces verifikacije poteka tako, da uporabnik na spletni strani, ki za avtentikacijo uporablja biometrično storitev FingerIdent, najprej vpiše uporabniško ime in zajame prstni odtis. Spletna aplikacija nato pošlje kodirano sliko oblačni storitvi v oblaku, ki sprocesira sliko (slika 2) in spletni aplikaciji sporoči rezultate ujemanja. Varnost predstavljene storitve je zagotovljena na več nivojih in sicer z uporabo HTTPS protokola za prenos podatkov, z uporabo certifikatov, z enkripcijo biometričnih značilk v podatkovni bazi, itd. Storitev je zasnovana modularno, kar pomeni, da so potencialne nadgradnje v smislu dodajanja novih biometričnih metod enostavne.

3. RAZVOJ OBLAČNE APLIKACIJE ZA KONTROLO PRISTOPA

Da bi lažje predstavili uporabnost biometrične storitve v oblaku smo razvili koncept aplikacije za kontrolo pristopa – AccessControlManagement, ki s pomočjo oblačnega sistema za verifikacijo beleži prisotnost študentov na predavanjih [5]. Identifikacija in verifikacija velikega števila ljudi v kratkem času je za človeka skoraj neizvedljiva naloga, medtem ko takšna aplikacija omogoča hitro in zanesljivo verifikacijo. Prednosti tako zasnovanega sistema, so v tem, da je vse skupaj nameščeno v oblaku in deluje neodvisno od prostora.

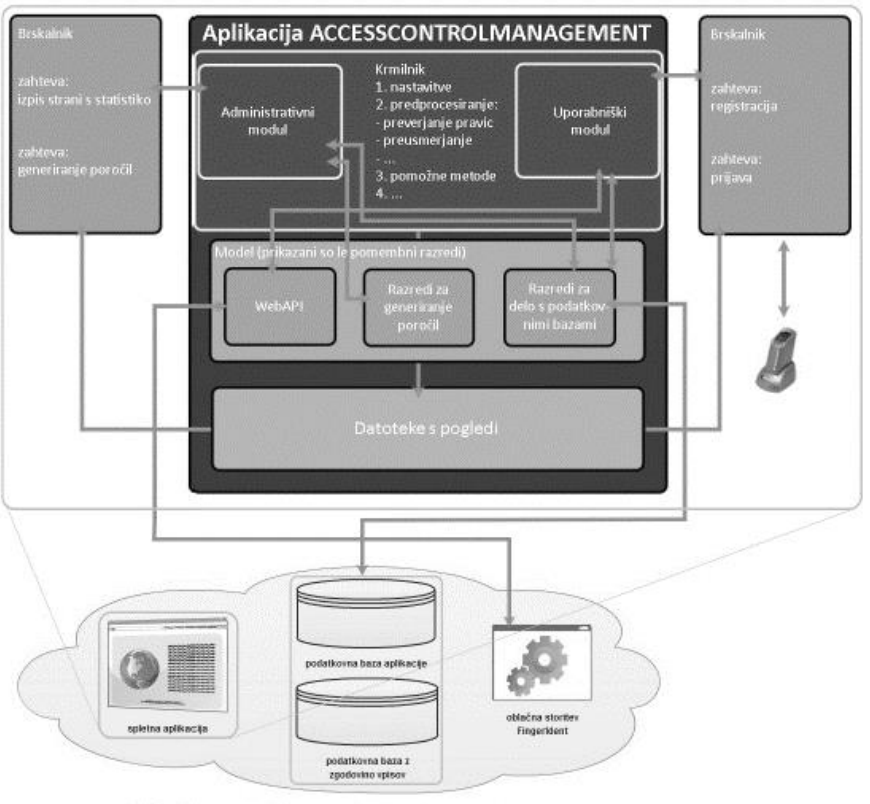
Aplikacijo sestavljata uporabniški in administrativni modul, kot je prikazano na sliki 4. Uporabniški modul je namenjen študentom in vsebuje formi za registracijo in prijavo (slika 3). Oba postopka se opravita s pomočjo bralnika prstnih odtisov in oblačne storitve FingerIdent. Administrativni modul uporabljajo profesorji. Njegov glavni namen je vpogled v statistiko o prisotnosti posameznih študentov pri posameznih predmetih in generiranje poročil.



Slika 3 - Registracija študenta v sistemu za kontrolo dostopa AccessControlManagement [5].

Zgradbo sistema bi lahko ločili na krmilnike, modele oz. logično plast in poglede. Vsaka zahteva, ki pride v sistem požene krmilnik, ki ji pripada. Ob zagonu krmilnika se najprej opravi inicializacija sistema, nato pa obdelava zahteve. Ta se v celoti izvede v krmilniku. Po končani obdelavi podatkov je te potrebno predstaviti še vizualno. To je naloga

pogledov. Preusmeritev na posamezen pogled se opravi s klicem posebne metode krmilnika. Dinamična vsebina pogledov je zapolnjena s spremenljivkami pogleda, ki se prav tako, pred klicem funkcije za preusmeritev, definirajo v krmilniku.



Slika 4 - Arhitekturna zgradba aplikacije AccessControlManagement [5].

Z izdelavo aplikacije smo dosegli večjo stopnjo zaščite proti goljufanju oz. ponarejanju identitet in avtomatizacijo procesa preverjanja prisotnosti študentov. Poleg tega pa aplikacija nudi konstanten vpogled v statistiko in možnost generiranja poročil.

4. REZULTATI

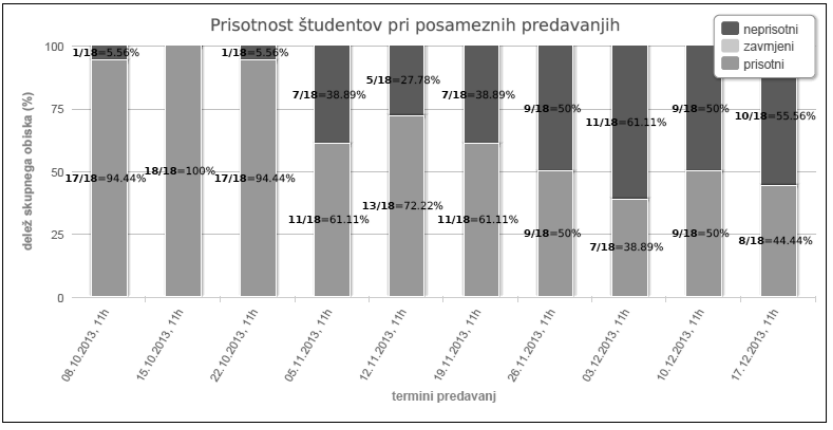
Razviti koncept smo testirali pri enem izmed predmetov na Fakulteti za računalništvo in informatiko, Univerze v Ljubljani. Sodelovalo je 18 študentov, katerih prisotnost se je beležila s pomočjo aplikacije za kontrolo pristopa AccessControlManagement in biometrične storitve v oblaku FingerIdent.

Postopek verifikacije je bil takšen, da se je vsak študent, ki je bil prisoten na predavanjih verificiral preko profesorjevega računalnika. Aplikacija je konec predavanja generirala

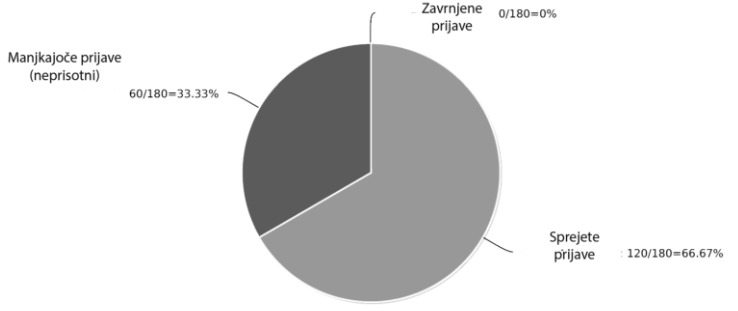
poročila, ki jih je profesor dobil po e-pošti. V poročilu je vidna statistika za vsakega študenta posebej, kakor tudi povzetek prisotnosti študentov v celotnem obdobju predavanj. Povzetek poročila o prisotnosti študentov pri predavanju je prikazan na sliki 5 in 6 ter v tabeli 1. Iz grafa na sliki 5 je vidno, da je bila udeležba na predavanjih na začetku skoraj 100%, potem pa je postopoma začela padati, medtem ko se iz statistike na tabeli 1 enostavno določi, kdo je zadostil pogojem prisotnosti pri predmetu (npr. vsaj 70% udeležba na predavanjih). Na sliki 6 je predstavljen skupni delež sprejetih, zavrnjenih in manjkajočih prijav.

Tabela 1 - Primer tabelarične statistike prisotnosti študentov pri predmetu.

Ime in Priimek	**Vpisna številka**	**Prisotnost (%)**
Jože Novak	123456	30%
Miha Novak	123457	70%
Luka Novak	123458	100%
Nejc Novak	123459	90%



Slika 5 - Graf prisotnosti študentov na posameznih predavanjih.



Slika 6 - Skupni delež sprejetih, zavrnjenih in manjkajočih prijav.

5. ZAKLJUČEK

Biometrične storitve v oblaku imajo zelo velik tržni potencial in prav zato privabljajo interes številnih raziskovalcev in razvojnih ekip iz celega sveta. V tem članku smo predstavili koncept prenosa obstoječe biometrične tehnologije v oblak in predstavili primer uporabe takšne storitve v aplikaciji za preverjanje prisotnosti. Aplikacija za preverjanje prisotnosti z uporabo biometrije nudi višjo stopnjo zaščite in hkrati avtomatizira proces beleženja prisotnosti.

Storitev biometrične verifikacije v oblaku bi bila zelo uporabna predvsem v sistemih, kjer je zahtevana povečana stopnja varnosti, kot recimo v spletnem bančništvu, v raznih trgovalnih platformah ali v aplikacijah javne uprave, kjer se nahaja veliko število osebnih podatkov.

LITERATURA

[1] D. Balfanz et al., "The future of authentication", *IEEE Security & Privacy*, vol. 10, str. 22-27, 2012.

[2] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud for Big Data Biometrics: Meeting the performance requirements of the Next Generation Biometric Systems," in *Proceeding of the IEEE World Congress on Services*, str. 597-601, 2011.

[3] P. Peer, J. Bule, J. Žganec-Gros, V. Štruc. "Building cloud-based biometric services". *Informatica*, vol. 37, no. 1, str. 115-122. 2013.

[4] H. Vallabhu and R.V. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," *International Journal of Soft Computing and Engineering*, vol. 2, str. 163-165, 2012.

[5] Đ. Kesić, "Oblačna spletna aplikacija za podporo sistemu za verifikacijo na podlagi prstnega odtisa", diplomsko delo na univerzitetnem študiju, Fakulteta za računalništvo in informatiko Univerze v Ljubljani, Slovenija, 2013.

[6] M. Tulloch, "Introducing Windows Azure", Microsoft Press, ZDA, 2013.