Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.41
DOI: https://doi.org/10.24867/33BE22Stokic

BEZBEDNOST PODATAKA U KONTEKSTU BIG DATA

DATA SECURITY IN THE CONTEXT OF BIG DATA

Aleksa Stokić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu su istražene specifične pretnje i ranjivosti u okviru Big Data i analizirana primena savremenih tehnika i alata za bezbednost podataka. Posebna pažnja je posvećena principima kao što su autentifikacija, enkripcija i zaštita od brute force i SQL injection napada. Takođe, na primeru veb aplikacije je prikazan primer implementacije bezbednosnih mehanizama.*

Ključne reči: *Big Data, Bezbednost, 2FA, Jake lozinke, Enkripcija, Brute force, SQL injection*

Abstract – *In this paper, specific threats and vulnerabilities within Big Data were explored and the application of modern techniques and tools for data security wa analyzed. Special attention was given to principles such as authentication, encryption and protection against brute force and SQL injection attacks. Additionallz, the implementation of securit mechanisms was demonstrasted thtough the example of a web application.*

Keywords: *Big Data, Security, 2FA, Strong passwords, Encryption, Brute force, SQL injection*

1. UVOD

Big Data donosi značajne prednosti u analizi i donošenju odluka, ali istovremeno predstavlja ozbiljan izazov po pitanju bezbednosti i privatnosti korisnika. Ogromna količina i raznolikost podataka, koja često uključuje osetljive lične informacije, povećava rizik od zloupotrebe i otkrivanja identiteta. Cilj rada je da analizira pretnje i ranjovsti u okviru Big Data i prikaže primenu savremenih bezbedonosnih tehnika kao što su enkripcija, autentifikacija i zaštita od napada. Kao praktičan primer, razvija se veb aplikacija za turističku agenciju koja će demonstrirati implementaciju ovih mehanizama radi zaštite podataka korisnika.

2. BIG DATA

Big Data predstavlja jedan od najznačajnijih fenomena savremenog digitalnog doba. Rast obima, brzine i raznovrsnosti podataka zahteva nove pristupe njihovom skladištenju, obradi i analizi. Dok je tradicionalna obrada podataka ograničena kapacitetom računarskih sistema, Big Data omogućava upotrebu masivnih i razuđenih skupa podataka kako bi se iz njih izvukle vrednosti.

Ključne karakteristike Big Data opisuju se korz koncept "5V": obim, brzina, raznovrsnost, verodostojnost i vrednost. Upravo kombinacija ovih elemenata čini Big Data jedinim načinom da se odgovori na savremen potrebe u oblasti kao što su finansije, zdravstvo, industrija i trgovina.

Razvoj cloud infrastrukture omogućio je veću fleksibilnost i elastičnost u radu sa velikim podacima. Koncept Big Data as a Service (BDaaS) integriše prednosti cloud-a i analitičkih alata, pružajući organizacijama pristup računarskim resursima bez potrebe za sopstvenim skupim sistemima. Među najvažnijim tehnologijama ističu se Hadoop, MapReduce, Hive i Spark, koji omogućavaju paralelnu obradu i upravljanje velikim podacima.

Big Data danas predstavlja industriju koja menja tržište rada, stvara nove poslovne modele i podstiče razvoj digitalne ekonomije. Kompanije koje se oslanjaju na podatke beleže veću produktivnost, bržu reakciju na tržišne promene i bolje razumevanje korisnika. Istraživanja pokazuju da organizacije orjentisane na podatke imaju znatno veće stope rasta i inovacija u odnosu na konkurenciju.

Ipak, uz brojne prednosti javljaju se i izazovi, kao što su bezbednost i privatnsot. Pitanja regulacije, kao i etičke dileme u vezi sa korišćenjem podataka, ostaju otvorena i predstavljaju ključni pravac budućeg razvoja ove oblasti.

Zaključno, Big Data nije samo tehnološki već i ekonomski i društveni fenomen, koji značajno oblikuje poslovanje, nauku i svakodnevni život. Njegov dalji razvoj zavisiće od balansa između tehničkog napretka, regulatornih okvira i etičkih standarda u korišćenju podataka.

3. BEZBEDNOST PODATAK U KONTEKSTU BIG DATA

Bezbednost po dataka u Big Data okruženjima predstavlja kompleksnu kombinaciju metodologija, tehnologija i dobrih praksi usmerenih na zaštitu poverljivosti, integriteta i dostupnosti podataka. Veliki obim, raznolikost i dinamika podataka koji potiču iz IoT uređaja, senzora i društvenih mreža nameću nove izazove koje tradicionalni modeli zaštita ne mogu u potpunosti rešiti. Pored tehničkih rizika, značajan problem predstavlja i privatnost, jer savremene analitike omogućavaju deanomalizaciju pojedinaca, zbog čega regulative poput GDRP i HIPAA propisuju stroge standarde obrade i čuvanja podataka.

Istorijski gledano, zaštita podataka evoluirala je od fizičkih mera i osnovne enkripcije, preko razvoja mrežnih protokola (SSL/TLS), do sveobuhvatnih pravnih okvira

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio Prof. Dr Aleksandar Kupusinac

kao što su GDRP i CCPA. Pored njih, međunarodni standardi poput ISO/IEC 27001 i PCI DSS definišu kontrole i procedure za bezbedno upravljanje inforamcijama. Tehnološki napredak doneo je i nove mehanizme – homomorfnu enkripciju, blockchain za integritet podataka, kao i koncepte diferecijalne privatnosti i k-anonimnosti.

U oblasti metodologija, posebno se ističu Risk Managment Framework (RMF), Security by Design, Zero Trust Architecture, Data Lifecycle i procene uticaja na privatnost (PIA/DPIA). Ovi okviri omogućavaju sistematičan pristup zaštiti podataka, od inicijalnog projektovanja, preko kontinuiranog upravljanja rizikom, do procene usaglašenosti sa regulativom.

Tehnološka implementacija zaštite obuhvata enkripciju u mirovanju i tranzitu, autentifikaciju i autorizaciju, zaštitu od brute force i SQL injection napada, kao i sisteme za logovanje i praćenje anomalija. Savremene Big Data platforme zahtevaju skalabilna rešenja koja mogu raditi u realnom vremenu i u distribuiranim cloud okruženjima.

Praktične mere podrazumevaju primenu enkripcije, segemntaciju mreže, kontrolu pristupa zasnovanu na ulogama, analizu mrežnog saobraćaja, kontinuirano praćenje cloud okruženja, redovno pravljenje rezervnih kopija i planove za brz odgovor na incidente. Podjednako je važna i obuka zapslenih, jer ljudski faktor često predstavja najslabiju kariku. Uočavanje internih pretnji i stalno praćenje usaglašenosti sa regulativom dodatno jača bezbedonosnu kulturu organizacije.

Bezbednost podataka u Big Data kontekstu nije samo tehnički izazov, već i strateško pitanje koje zahteva integraciju metodologija, tehnologija, praksi i regulatornih okvira. Samo takav holistički pristup omogućava izgradnju pouzdanih i održivih sistema koji štite podatke, grade poverenje i omogućavaju odgovorno korišćenje Big Data analitike.

4. IMPLEMENTACIJA BEZBEDONOSNIH PRAKSI

Intenzivan razvoj tehnologije, zajedno sa globalnom povezanošću, nametnuo je potrebu za sistematičnom implementacijom bezbedonosnih praksi koje osiguravaju integrtiet, povreljivost i dostupnost informacija. Ovaj rad daje pregled najvažnijih tehnika i metoda koje predstavljaju temelj moderne sajber bezbednosti, uz poseban naglasak na primenu u Big Data i veb sistemima.

4.1. Jake lozinke i autentifikacija

Jedna os osnovnih mera zaštite predstavlja upotreba jakih i jedinstvenih lozinki, koje značajno umanjuju rizik od neovlašćenog pristupa. Istraživanja pokazuju da složene lozinke sa njmanje 12 karaktera, kombinacija slova, brojeva i simbola, mogu izdržati brute force napade u vremenskom okviru od više hiljada godina. Ipak, lozinke same po sebi nisu dovoljne. Zato je u praksi sve zastupljenija dvofaktorska autentifikacija (2FA), koja uvodi dodatni sloj sigurnosti kombinovanjem faktora znanja (lozinka), posedovanja (tokeni, mobilni uređaj) i inherencije (biometrijski podaci). Otvoreni standardi kao što su FIDO, Oauth2.0, OpenID Connect i SAML omogućavaju interoberabilnost i otpornost na phishing napade, dok budući pravci uključuju autentifikaciju bez lozinki i koncepte decentralizovanog identiteta.

Iako značajno povećava bezbednost, ona nije imuna na napade. Slabosti mogu nastati usled zloupotrebe porcesa oporavka naloga, kompromitacije tokena ili nesigurnosti SMS kanala. Nacionalni instituti (na primer NIST) već preporučuju izbegavanje SMS-a u sistemima visokog rizika. Ipak, prednosti 2FA – jednostavnost, dostupnost i visok nivo sigurnosti – čine je jednim od najpouzdanijih rešenja za zaštitu digitalnih servisa.

4.2. Zaštita od brute force napada

Brute force napadi, zasnovani na sistematičnom isprobavanju kombinacija lozinki i ključeva, ostaju jedan od najrasprostranjenijih metoda kompromitovanja naloga. Iako su jednostavni i teoretski nepogrešivi, njihova efikasnost zavisi od dužine i složenosti akreditiva. Savremeni sistemi primenjuju više mera zaštite: ograničenje broja prijava, CAPTCHA mehanizme, crne liste IP adresa, praćenje mrežnog saobraćaja kao i uvođenje višefaktorske autentifikacije. Korisnicima se preporučuje upotreba jedinstvenih lozinki, mendžera lozinki i izbegavanje nebezbednih sajtova. Na ovaj način brute force napada postaju sve manje delotvorni, ali i dalje predstavljaju ozbiljnu pretnju ako se sistemi ne održavaju redovno i bezbednosno ne ažuriraju.

4.3. Primena enkripcije

Enkripcija predstavlja jedan od najmoćnijih mehanizma zažtite podataka, jer osigurava njihovu povreljivost čak i u slučaju presretanja i krađe. Primena obuhvata i podatke u mirovanju i podatke u prenosu, uz poseban značaj u oblastima finansija, e-trgovina i e-uprave. U Srbiji je ova oblast pravno uređena Zakonom o elektronskom dokumentu, dok GDRP na nivou EU posebno prepoznaje enkripciju kao preporučenu meru.

Najznačajniji algoritmi uključuju simetrični AES iasimtrični RSA. Simetrična enkripcija je brza i efikasna za velike količine podataka, ali zahteva siguran prenos ključeva. RSA rešava ovaj problem upotrebom javnih i privatnih ključeva, iako je računarski zahtevniji. U praksi se često primenjuje hibridni pristup – AES za sadržaj, RSA za razmenu ključeva. Glavni izazovi odnose se na upravljanje kriptografskim ključevima, kao i na rizike od zloupotrebe enkripcije u ransomware napadima.

4.4. Zaštita od SQL injection napada

SQL injection je jedna od najopasnijih veb ranjivosti koja omogućava napadaču manipulaciju upitima ka bazi podataka. Posledice uključuju neovlašćen pristup, krađu ili brisanje podataka, pa čak i eskalaciju privilegija. Ključne mere prevencije obuhvataju validiranje unosa, upotrebu parametrizovanih upita i skladištenje porcedura, kao i primenu belih lista za kontrolu unosa. Redovno skeniranje aplikacija alatima kao što su Burp Scanner ili Acunetix omogućava rano otkrivanje ranjivosti. Primeri iz prakse pokazuju da dinamičko kreiranje SQL upita putem konkatenacije string-ova predstavlja najveći rizik, dok parametrizovani upiti i savremeni okviri pružaju pouzdanu zaštitu.

Implementacije bezbedonosnih praksi nije više opcija, već je nužnost u digitalnom dobu. Jake lozinke, 2FA, enkripcija, zaštita od brute force i SQL injection napada predstavljaju temeljnemehanizme za izgradnju otpornih sistema. Međutim, svki od ovih mehanizama nosi svoja ograničenja i zahteva kontinuirano unapređenje. Budućnost bezbednosti leži u integraciji više faktora – biometrijskih, bihejvioralnih i decentralizovanih – koji zajedno mogu osigurati robusnije i prilagodljivije sisteme. Samo sistematičnim i sveobuhvatnim pristupom moguće je izgraditi poverenje korisnika i očuvati integritet inforamcionih resursa u sulovima stalno rastućih sajber pretnji.

5. INTEGRISAN PRIMER IMPLEMENTACIJE BEZBEDONOSNIH MEHANIZAMA U VEB APLIKACIJI

U okviru ovog rada razvijena je aplikacija koja služi kao ilustrativni primer integracije ključnih bezbedonosnih mera. Iako funkcionalno zasnovana na modelu turističke agencije, aplikacija ima primarno edukativni i demonstrativni karakter, pokazujući kako se kroz jedan sistem mogu implementirati mehanizmi autentifikacije, zaštite podataka u prenosu i skladištenju, kao i prevencije zlonamernih aktivnosti.

5.1. Tehnološki stek i arhitektura

Aplikacija je izgrađena primenom savremenog tehnološkog steka. Frontend je realizovan u React.js-u, koji omogućava komponentni razvoj jednostraničnih aplikacija i komunikaciju sa serverom preko HTTP zahteva (Axios). Backend je izgrađen u Python-u korišćenjem Flask framework-a, koji omogućava izgradnju RESTful API servisa i modularni arhitekturu. Za upravljanje podacima korišćenja je MongoDB NoSQL baza, pogodna za dinamične strukture. Arhitektura je troslojna, sa jasnom podelom na kontrolere (obrada zahteva), servise (poslovna logika) i repozitorijume (rad sa bazom), što doprinosi lakšem održavanju i proširivosti.

5.2. Implementacija bezbedonosnih mehanizama

5.2.1. Provera jačine lozinki

Prilikom registracije vrši se dvostruka provera lozinki korišćenjem regulatornih izraza. Ovaj mehanizam osigurava da lozinke zadovoljavaju minimalne kriterijume složenosti. Čime se umanjuje rizik od brute force napada.

```
28  const isStrongPassword = (password) => {
29      const regex = /^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[\W_]).{12,}$/;
30      return regex.test(password);
31  };
```

Slika 1. *Provera jačine lozinke na frontend delu aplikacije*

5.2.2. 2FA

Realizovana je integracija sa TOTP standardom putem PzOTP biblioteke i prikaza QR koda pomoću Qrcode modula. Nakon inicijalnog podešavanja, korisnik prilikom svkaog logovanja unosi jednokratni kod iz aplikacije kao što je Google Authenticator. Ovim se znatno povećava sigurnost prijave.

```
def generate_2fa_secret(email):
    secret = pyotp.random_base32()
    totp = pyotp.TOTP(secret)
    otp_uri = totp.provisioning_uri(name=email, issuer_name="MasterTuristickaAgencija")

    qr = qrcode.make(otp_uri)
    buffer = BytesIO()
    qr.save(buffer, format="PNG")
    qr_base64 = base64.b64encode(buffer.getvalue()).decode()

    return secret, qr_base64
```

Slika 2. *Generisanje QR koda u Python-u*

```
def verify_otp_code(email, otpCode):
    if not otpCode:
        return jsonify({'message': 'OTP code is required!'}), 400

    current_user = check_existing_user(email)
    secret = current_user['twoFASecret']
    result = verify_otp(secret, otpCode)

    if result:
        try:
            session.clear()
            session['passenger_id'] = str(current_user['_id'])
            session['email'] = str(current_user['email'])
            passenger_id = str(current_user['_id'])

            token_payload = {
                'passenger_id': passenger_id,
                'passenger_email': current_user['email'],
                'exp': datetime.utcnow() + timedelta(hours=1)
            }
            reset_failed_attempts(current_user['email'])
            token = encode(token_payload, os.environ.get('SECRET_KEY', 'MasterTuristickaAgencijaBack'), algorithm='HS256')

            return jsonify({'token': token}), 200

        except Exception as e:
            return jsonify({'error': str(e)}), 400
    else:
        return jsonify({'message': 'Invalid OTP code!'}), 400
```

Slika 3. *Servis za proveru OTP koda*

5.2.3. Zaštita od brute force napada

Implementirana je višeslojna strategija koja obuhvata globalni rate-limiting (Flask-Limiter), ograničenje broja zahteva po kritičnim rutama (/signin, /signup), kao i privremeno blokiranje naloga nakon više neuspelih pokušaja. Ovim se efikasno sprečavaju automatizovani napadi i kreiranje lašnih naloga.

```
12  @auth_signin_blueprint.route( rule: '/signin', methods=['POST'])
13  @limiter.limit("5 per minute")
14  def sign_in_controller():
```

Slika 4. *Ograničenje na maksimum 5 pristupa za rutu*

```
def sign_in_service(email, password):
    current_user = check_existing_user(email)
    if not current_user:
        return jsonify({'message': 'User with this email does not exist! Please check email or create account!'}), 400

    if int(current_user['lockUntil']) > int(time.time()):
        return jsonify({'message': 'Account temporarily locked. Try again later.'}), 400

    if not bcrypt.checkpw(password.encode('utf-8'), current_user['password']):
        if current_user['failedAttempts'] > 5:
            lock_time = int(time.time()) + 5 * 60
            set_lock(current_user['email'], lock_time)
            return jsonify({'message': 'Account locked. Try again later.'}), 400
        else:
            attemps = current_user['failedAttempts'] + 1
            increment_failed_attempts(current_user['email'], attemps)
            return jsonify({'message': 'Wrong password!'}), 400
```

Slika 5. *Logika za blokiranje korisničkog naloga na backend delu aplikacije*

5.2.4. Zaštita od NoSQL injection napada

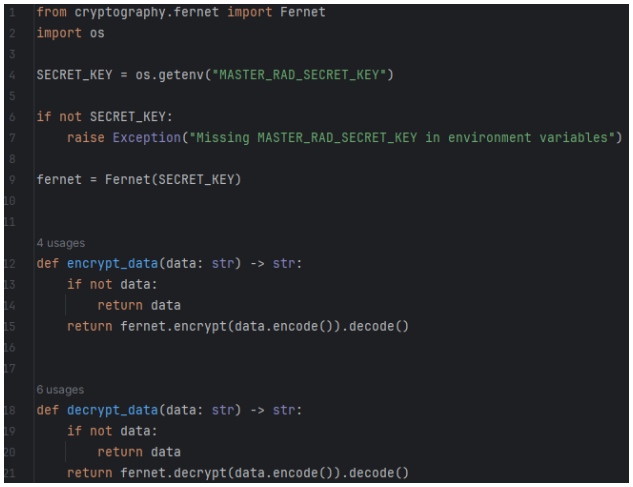
Kreiran je poseban validacioni servis koji proverava sve unose pre slanja u bazu. Pored regularnih izraza za verifikaciju formata, primenjuje se parametrizovaniupiti u pymongo biblioteci, čime se eliminiše rizik od direktne interpolacije korisničkog unosa u upit.

```python
def contains_sql_injection(value: str) -> bool:
    if not isinstance(value, str):
        return False

    patterns = [
        r"(?i)(\bor\b|\band\b)\s+\d+=\d+",
        r"(?i)drop\s+table",
        r"(?i)select\s.+\sfrom",
        r"(?i)insert\s+into",
        r"(?i)update\s+\w+\s+set",
        r"(?i)delete\s+from",
        r"['\";#`]",
        r"--",
    ]

    for pattern in patterns:
        if re.search(pattern, value):
            return True

    return False


10 usages
def validate_email(email: str) -> bool:
    pattern = r'^[\w\.-]+@[\w\.-]+\.\w+$'
    return re.match(pattern, email) is not None


def validate_username(username: str) -> bool:
    return bool(re.match( pattern: r'^\w{1,30}$', username))
```

Slika 5. *Izgled validacionog servisa na backend delu aplikacije*

5.2.5. Implementacija enkripcije

Osetljivi podaci (JMBG, broj pasoša) čuvaju se u šifrovanojformi korišćenjem simterične enkripcije (Fernet iz crzptography biblioteke). Tajni ključ se čuva u .env fajlu, što obezbeđuje minimalnu zaštitu od kompromitacije koda.



```python
from cryptography.fernet import Fernet
import os

SECRET_KEY = os.getenv("MASTER_RAD_SECRET_KEY")

if not SECRET_KEY:
    raise Exception("Missing MASTER_RAD_SECRET_KEY in environment variables")

fernet = Fernet(SECRET_KEY)


4 usages
def encrypt_data(data: str) -> str:
    if not data:
        return data
    return fernet.encrypt(data.encode()).decode()


6 usages
def decrypt_data(data: str) -> str:
    if not data:
        return data
    return fernet.decrypt(data.encode()).decode()
```

Slika 6. *Enkripcioni servis*

```
_id: ObjectId('686be3d252825d4d84704d97')
email : "stokic.aleksa.01@gmail.com"
password : Binary.createFromBase64('JDJiJDEyJHkuWSS6VDBVbGJEbHdsRUI4QWRyNXVBLlZxdGR2cUx2M2R5by9VV3Q1OU5TWWlyYW9MOEIy', 0)
first_name : "Aleksa"
last_name : "Stokic"
birthday : "2001-01-19"
is2FASetUp : true
twoFASecret : "Z5QOVSPF7Y3VADJMAXTQYCERVTNIH3SR"
failedAttemps : 0
lockUntil : 0
JMBG : "gAAAAABoa-PSQ-0-Z_1bJKx1KMnjOIei1Yqo7O4K487CxvUGthXEZwXdXPdLrMPb4u8ZC9e…"
passportNumber : "gAAAAABoa-PS3vSH91n1u5QVbPScyWLpO1UhSfUzY3g1M9WykcOS_Vuz3DCnPJpX20Cr5q…"
failedAttempts : 0
```

Slika 7. *Izgled enkriptovanih podataka iz baze*

Implementacija prikazanih mehanizama pokazuje da je moguće izgraditi veb apliakciju koja ispunjava savremene bezbedonosne standarde uz minimalne resurse i upotrebu dostupnih biblioteka. Sistem je edukativno osmišljen kako bi demonstrirao najčešće načine odbrane. Ipak, naglašeno je da svaki mehanizam ima svja ograničenja, pa se preporučuje kombinovanje više mera i njihovo kontinuirano unapređenje.

Integracija bezbedonosnih mehanizama u veb aplikaciji predstavlja uslov za njihovu pouzdanu i bezbednu upotrebu. Primer aplikacije turističke agencije pokazuje da pravilnom primenom validacije lozinki, 2FA, zaštite od brute force i NoSQL injection napada, kao i enkripcije osetljivih podataka, moguće je značajno umanjiti rizik od kompromitacije sistema. Rad pokazuje da kombinacija dobrih praksi, adekvatnog tehnološkog izbora i edukacije korisnika predstavlja najbolji pristup izgradnji otpornih i pouzdanih veb aplikacija u savremenom digitalnom okruženju.

5. ZAKLJUČAK

U eri digitalne transformacije i eksponencijalnog rasta količine podataka, bezbednost u Big Data okruženjima postaje jedan od ključnih preduslova za očuvanje integriteta, poverljivosti i dostupnosti informacija. Veliki podaci pružaju izuzetne mogućnosti za naprednu analizu i donošenje strateških odluka, ali istovremeno uvode broje izazove u pogedu zaštite osetljivih informacija i otpornosti sistema na sajber napade. Karakteristike velikih podataka zahtevaju nove, fleksibilne i skalabilne pristupe u dizajnu i implementaciji bezbedonosnih mera.

U ovom radu istraženi su ključni bezbedonosni aspekti Big Data okruženja, pri čemu su analizirane najčešće pretnje kao što su krđa identiteta, neovlašćeni pristup, brute force i injection napadi, kao i izazovi uporavljanja autentifikacijom i privatnošću. Teorijski okvir upotpunjen je praktičnim delom u okviru kojeg je razvijena veb aplikacija zasnovana na arhitekturi Flask-React.js-MongoDB. U aplikaciji su implementirani mehanizmi kao što su dvofaktroska autentifikacija, kontrola jakih lozinki, validacija unosa, enkripcija osetljivih podataka i ograničenje zahteva, čime je pokazano kako se kroz slojevit pristup može značajno povećati bezbednost sistema.

Rezultati ukazuju da ne postoji univerzalno rešenje za sve pretnje i da bezbednost mora biti tretirana kao kontinuirani proces koji podrazumeva stalno praćenje, prilagođavanje i unapređeje mehanizama. Posebno je istaknuta potreba za integracijom sistema za detekciju anomalija u realnom vremenu, primenom zero-trust arhitekture i korišćenjem mašinskog učenja u otkrivanju zloupotreba.

Zaključno, rad potvrđuje da je bezbednost podataka neodvojiv deo Big Data sistema i da samo interdisciplinarni pristup – koji kombinuje tehničke, organizacione i edukativne mere – može obezbediti pouzdanost i otpornost u savremenom digitalnom okruženju.

6. LITERATURA

[1] https://cloud.google.com/learn/what-is-big-data

[2]https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/

[3] https://www.turing.com/resources/big-data-security#what-is-big-data-security?

[4]https://www.keepersecurity.com/blog/2023/08/31/what-makes-a-strong-password/

[5]https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

[6]https://www.fortinet.com/resources/cyberglossary/brute-force-attack

[7]https://www.techtarget.com/searchsecurity/definition/encryption

[8]https://www.acunetix.com/websitesecurity/sql-injection/

Kratka biografija:

Aleksa Stokić je rođen 2001. godine u Požarevcu, Srbija. Završio je Požarevačku gimnaziju u Požarevcu, 2019. godine. Fakultet Tehničkih Nauka u Novom Sadu je upisao 2019. godine. Diplomirao je u septembru 2023. godine, smer Primenjeno softversko inženjerstvo. Uspešno je ispunio sve akademske obaveze i položio sve ispite predviđene master studijskim programom Primenjeno softversko inženjerstvo.

kontakt: stokic.aleksa.01@gmail.com