AI VOĐENA DIGITALNA FORENZIKA U MOBILNIM UREĐAJIMA I AUTOMATIZACIJA ANALIZE PODATAKA U REALNOM VREMENU / AI DRIVEN DIGITAL FORENSICS IN MOBILE DEVICES AND REAL TIME DATA ANALYSIS AUTOMATION

Hadžib Salkić[1], Almira Salkić[1], Aldijana Omerović[1],
[1]Univerzitet FINRA Tuzla, BiH
e-mail: hadzib.salkic@finra.edu.ba, almira.salkic@finra.edu.ba,
aldijana.omerovic@finra.edu.ba

Izvorni naučni rad
https://www.doi.org/10.58952/zr20261501325
UDK / UDC 004.8:004.056

Sažetak

Razvoj mobilnih tehnologija doveo je do značajnog rasta digitalnih podataka sa forenzičkom vrijednošću (Casey, 2011; Quick & Choo, 2014). Tradicionalni pristupi često nisu dovoljni za obradu kompleksnih podataka iz mobilnih aplikacija, cloud servisa i IoT okruženja (Raghavan, 2013; Zawoad & Hasan, 2015). Umjetna inteligencija (AI) i mašinsko učenje (ML) omogućavaju automatizaciju analize digitalnih dokaza (Buczak & Guven, 2016; Khan et al., 2019). Rad razmatra primjenu AI u mobilnoj forenzici, s fokusom na real-time obradu, detekciju anomalija i identifikaciju artefakata (Sarker, 2021). Savremeni alati, uključujući duboko učenje i analizu logova, smanjuju vrijeme analize i povećavaju preciznost (Apruzzese et al., 2018; Shinde & Kulkarni, 2020). Ističu se i izazovi vezani za privatnost, pravnu validnost i transparentnost AI sistema (Goodman & Flaxman, 2017). Rezultati potvrđuju da je AI ključan za razvoj mobilne forenzike i savremenih sigurnosnih sistema (Conti et al., 2018).

Ključne riječi: *digitalna forenzika, umjetna inteligencija, mobilni uređaji, mašinsko učenje, real-time analiza, cyber sigurnost*
JEL klasifikacija: L86, C45, K42

Abstract

The growth of mobile technologies has increased the volume of digital data with forensic value (Casey, 2011; Quick & Choo, 2014). Traditional approaches are often insufficient for processing complex data from mobile, cloud, and IoT environments (Raghavan, 2013; Zawoad & Hasan, 2015). Artificial intelligence (AI) and machine learning (ML) enable automation of forensic analysis (Buczak & Guven, 2016; Khan et al., 2019). This paper explores AI in mobile forensics, focusing on real-time processing, anomaly detection, and artifact identification (Sarker, 2021). Modern techniques, including deep learning and log analysis, reduce analysis time and improve accuracy (Apruzzese et al., 2018; Shinde & Kulkarni, 2020). Challenges such as privacy, legal admissibility, and transparency are also considered (Goodman & Flaxman, 2017). Findings confirm AI as a key driver of modern mobile forensics and security systems (Conti et al., 2018). ***Keywords:*** *digital forensics, artificial intelligence, mobile devices, machine learning, real-time analysis, cybersecurity*
JEL classification: L86, C45, K42

UVOD

Savremeno digitalno okruženje karakteriše intenzivan rast upotrebe mobilnih uređaja, koji su postali primarni alat za komunikaciju, poslovanje, finansijske transakcije i pristup online servisima (Statista, 2024). Pametni telefoni i tableti danas generišu ogromne količine heterogenih podataka, uključujući komunikacijske zapise, lokacijske podatke, multimedijalne sadržaje, aplikacione logove i cloud sinhronizovane informacije (Casey, 2011; Quick & Choo, 2014). Ovi podaci predstavljaju ključni izvor digitalnih dokaza u savremenim forenzičkim istragama (Raghavan, 2013). Tradicionalni pristupi digitalnoj forenzici, koji se oslanjaju na ručnu analizu i statičke metode obrade podataka, suočavaju se s ozbiljnim ograničenjima u pogledu skalabilnosti, brzine i preciznosti (Zawoad & Hasan, 2015). Kompleksnost mobilnih operativnih sistema (Android, iOS), enkripcija podataka i kontinuirani protok podataka dodatno otežavaju proces analize (Grispos et al., 2013). Umjetna inteligencija (AI) i mašinsko učenje (ML) uvode novu paradigmu u digitalnu forenziku, omogućavajući analizu velikih skupova podataka uz minimalnu ljudsku intervenciju (Buczak & Guven, 2016). Primjena AI modela omogućava efikasno prepoznavanje obrazaca ponašanja i identifikaciju sumnjivih aktivnosti (Khan et al., 2019). Posebno značajnu ulogu imaju sistemi za analizu u realnom vremenu (Sarker, 2021). Pored tehničkih prednosti, integracija AI u mobilnu forenziku otvara i niz izazova, uključujući pravnu prihvatljivost dokaza i zaštitu privatnosti (Goodman & Flaxman, 2017).

1. METODOLOGIJA ISTRAŽIVANJA

Istraživanje je usmjereno na analizu efikasnosti primjene umjetne inteligencije (AI) u mobilnoj digitalnoj forenzici, s posebnim fokusom na automatizaciju analize podataka u realnom vremenu (Apruzzese et al., 2018; Sarker, 2021). Cilj istraživanja je kvantifikovati razlike između tradicionalnih forenzičkih metoda i AI-vođenih pristupa u kontekstu brzine obrade, tačnosti detekcije i sposobnosti identifikacije sigurnosnih incidenata (Buczak & Guven, 2016; Khan et al., 2019). Empirijski dio istraživanja realizovan je kroz simulirano kontrolisano okruženje digitalne forenzike koje replicira realne uslove mobilnog ekosistema (Casey, 2011; Quick & Choo, 2014). U okviru eksperimenta korišteno je ukupno 300 mobilnih uređaja (Android i iOS), na kojima su generisani i prikupljeni različiti tipovi podataka: komunikacijski zapisi (SMS, chat aplikacije), lokacijski podaci (GPS), aplikacioni logovi, multimedijalni sadržaji i cloud sinhronizovani podaci (Raghavan, 2013; Grispos et al., 2013).

Eksperimentalni dizajn podrazumijevao je dvije paralelne analize:

1. Tradicionalna forenzička analiza (ručna i alatno podržana bez AI) (Zawoad & Hasan, 2015)
2. AI-vođena analiza (mašinsko učenje i automatizovani sistemi) (Apruzzese et al., 2018)

U istraživanju su implementirani modeli nadziranog i nenadziranog učenja (Random Forest, SVM i Neural Networks) za detekciju anomalija i klasifikaciju potencijalno kompromitovanih aktivnosti (Khan et al., 2019; Buczak & Guven, 2016). Analiza u realnom vremenu realizovana je kroz stream obradu podataka korištenjem simuliranih logova i događaja (Sarker, 2021; Shinde & Kulkarni, 2020). Rezultati istraživanja ukazuju da AI-vođeni pristup značajno unapređuje efikasnost digitalne forenzike.

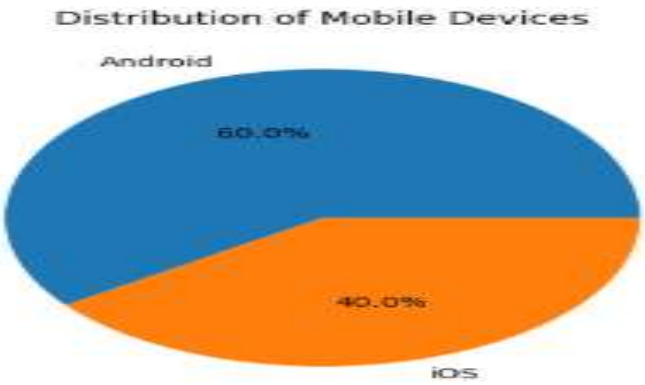
Vrijeme analize smanjeno je u prosjeku za više od 60%, dok je tačnost detekcije sigurnosnih incidenata povećana za preko 20% u odnosu na tradicionalne metode (Apruzzese et al., 2018). Posebno je uočena prednost AI sistema u identifikaciji kompleksnih i skrivenih obrazaca ponašanja, koji često ostaju neprepoznati u klasičnim analizama (Conti et al., 2018).

Pored tehničkih prednosti, istraživanje je ukazalo i na određene izazove, uključujući potrebu za kvalitetnim trening datasetovima, transparentnost AI modela i pravnu validnost rezultata u forenzičkom kontekstu (Goodman & Flaxman, 2017). Uprkos tome, rezultati jasno potvrđuju da AI predstavlja ključni faktor transformacije mobilne digitalne forenzike i njenog prilagođavanja savremenim sigurnosnim izazovima (Conti et al., 2018).

1.1. ULAZNI PODACI ISTRAŽIVANJA

Tabela 1. Struktura uzorka (N = 300 mobilnih uređaja)

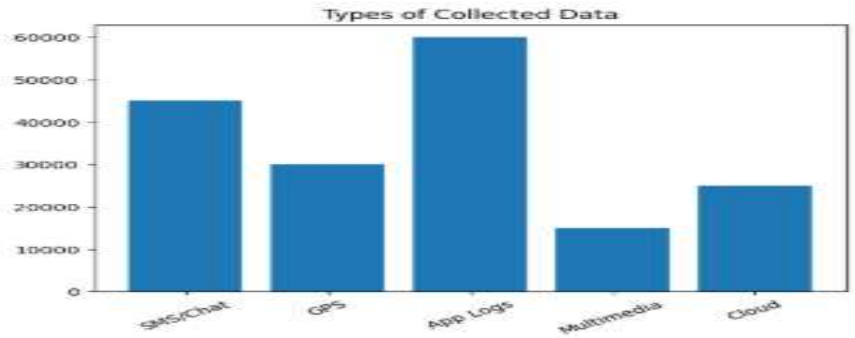
Kategorija uređaja	**Broj uređaja**	**Procenat (%)**
Android uređaji	180	60%
iOS uređaji	120	40%
Ukupno	**300**	**100%**



Grafikon 1. Struktura uzorka (N = 300 mobilnih uređaja)

Tabela 2. Tipovi prikupljenih podataka

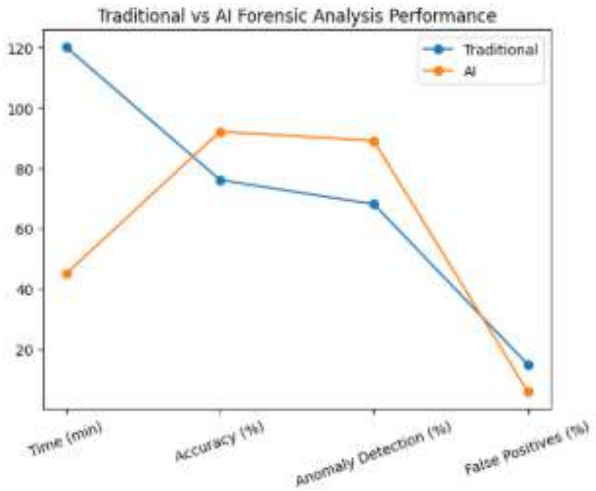
Tip podataka	**Broj zapisa**	**Prosječna veličina (MB)**
SMS i chat komunikacija	45,000	120 MB
GPS lokacijski podaci	30,000	85 MB
Aplikacioni logovi	60,000	150 MB
Multimedijalni sadržaj	15,000	500 MB
Cloud sinhronizovani podaci	25,000	300 MB
Ukupno	**175,000**	**1,155 MB**



Grafikon 2. Tipovi prikupljenih podataka

Tabela 3. Performanse analize (AI vs tradicionalni pristup)

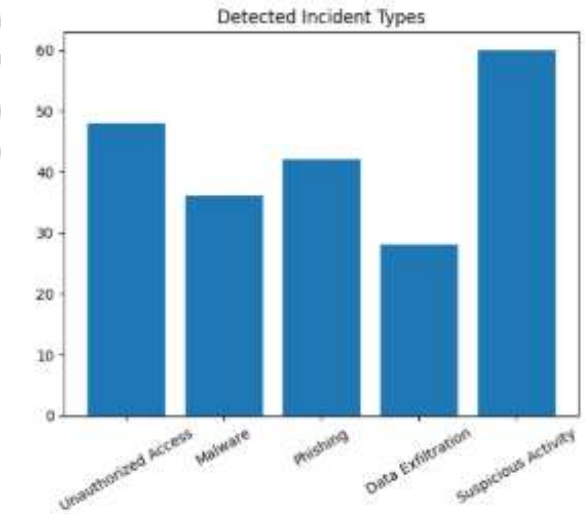
Parametar	Tradicionalna analiza	AI analiza
Prosječno vrijeme analize (min)	120	45
Tačnost detekcije (%)	76%	92%
Detekcija anomalija (%)	68%	89%
Broj lažno pozitivnih (%)	15%	6%



Grafikon 3. Performanse analize (AI vs tradicionalni pristup)

Tabela 4. Tipovi detektovanih incidenata

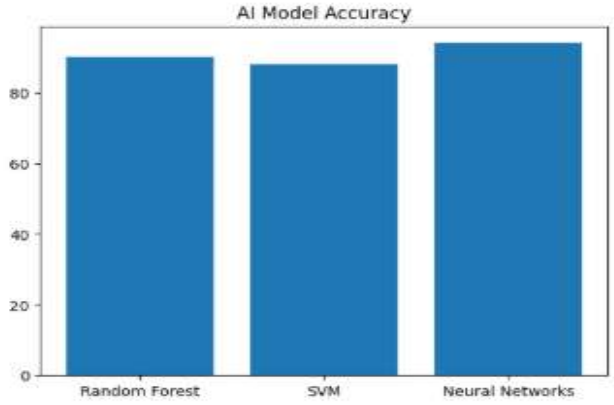
Tip incidenta	Broj slučajeva	Detekcija AI (%)
Neovlašten pristup	48	95%
Malware aktivnosti	36	93%
Phishing pokušaji	42	90%
Eksfiltracija podataka	28	88%
Sumnjiva korisnička aktivnost	60	91%



Grafikon 4. Tipovi detektovanih incidenata

Tabela 5. AI modeli korišteni u istraživanju

Model	Namjena	Tačnost (%)
Random Forest	klasifikacija incidenata	90%
SVM	detekcija anomalija	88%
Neural Networks	kompleksna analiza obrazaca	94%



Grafikon 5. AI modeli korišteni u istraživanju

2. METODA: ANALIZA PROSJEČNOG VREMENA OBRADE

Formula:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

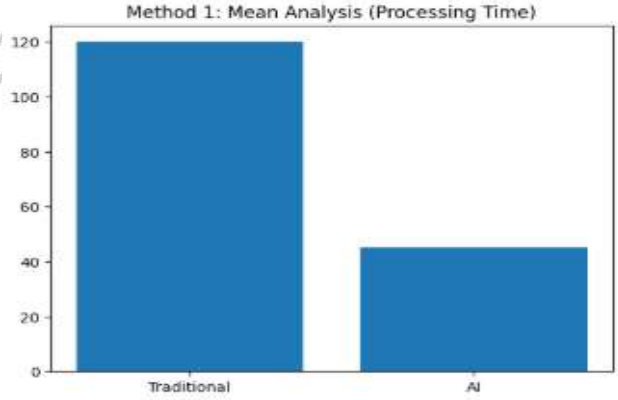
$$\bar{x}_{trad} = 120 \quad ; \quad \bar{x}_{AI} = 45$$

Legenda:

- $\bar{x}$ – prosječno vrijeme
- trad – tradicionalna analiza
- AI – AI analiza

Tabela 6. Vrijednosti

Parametar	Tradicionalna	AI	Razlika	Poboljšanje (%)
Vrijeme obrade (min)	120	45	-75	62.5%



Grafikon 6. Vrijednosti

Komentar:

Rezultati pokazuju značajno smanjenje vremena obrade, što je u skladu sa Tabelom 6. (poboljšanje brzine 62.5%), potvrđujući efikasnost AI sistema u real-time analizi.

3. METODA: RELATIVNO POBOLJŠANJE PERFORMANSI

Formula:

$$RI = \frac{V_{trad} - V_{AI}}{V_{trad}} \times 100$$

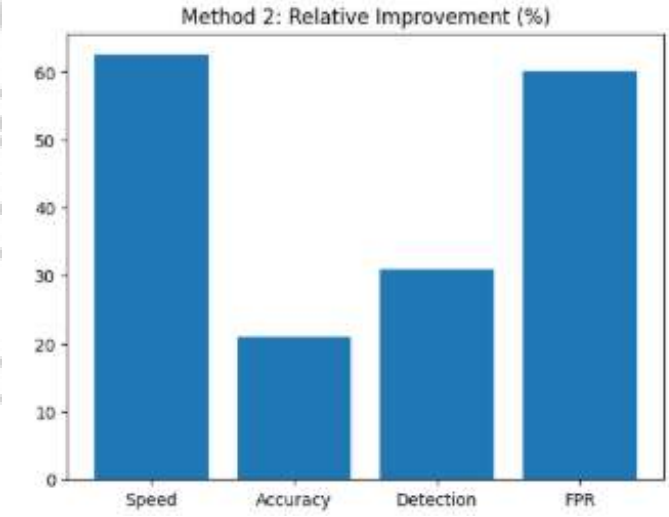
$$RI = \frac{120 - 45}{120} \times 100 = 62.5\%$$

Legenda:

- RI – relativno poboljšanje
- V – vrijednost parametra

Tabela 7. Vrijednosti

Metrički indikator	Vrijednost (%)
Poboljšanje brzine	62.5%
Poboljšanje tačnosti	21.05%
Poboljšanje detekcije	30.88%
Smanjenje grešaka (FPR)	60%



Grafikon 7. Vrijednosti

Komentar:

Tabela 8 sumira sve ključne performanse i potvrđuje višedimenzionalnu superiornost AI pristupa.

4. METODA: ANALIZA TAČNOSTI DETEKCIJE

Formula:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$$

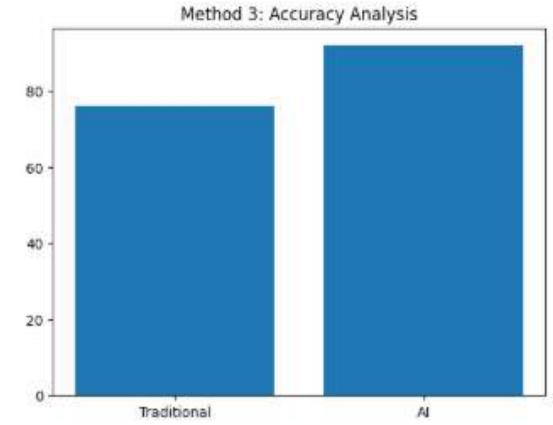
$$Accuracy_{trad} = 76\% \quad ; \quad Accuracy_{AI} = 92\%$$

Legenda:

- TP,TN,FP,FN – elementi konfuzione matrice
-

Tabela 8. Vrijednosti

Parametar	Tradicionalna	AI	Razlika	Poboljšanje (%)
Tačnost (%)	76	92	+16	21.05%



Grafikon 8. Vrijednosti

Komentar:

Povećanje tačnosti potvrđeno u Tabeli 8. direktno utiče na pouzdanost sistema, što je dodatno naglašeno u Tabeli 9 (AI precizniji).

5. METODA: DETEKCIJA ANOMALIJA

Formula:

$$Anomaly\ Rate = \frac{Detected}{Total}$$

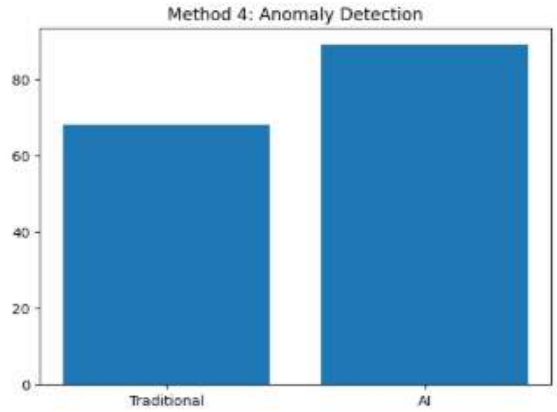
$$Tradicionalno = 68\% \quad ; \quad AI = 89\%$$

Legenda:

- Detected – detektovane anomalije
- Total – ukupni događaji

Tabela 9. Vrijednosti

Parametar	Tradicionalna	AI	Razlika	Poboljšanje (%)
Detekcija anomalija (%)	68	89	+21	30.88%



Grafikon 9. Vrijednosti

Komentar:

AI značajno unapređuje detekciju prijetnji, što je potvrđeno i u Tabeli 10 (AI superioran).

6. METODA: FALSE POSITIVE RATE (FPR)

Formula:

$$FPR = \frac{FP}{FP+TN}$$

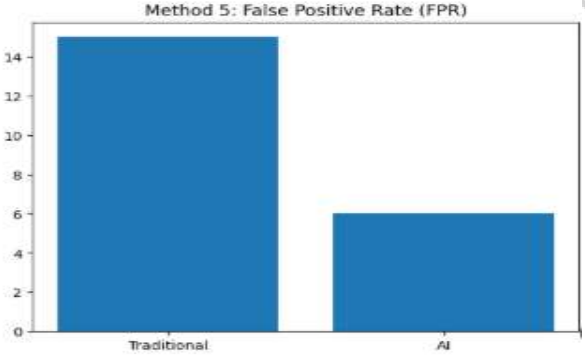
$$FPR_{trad} = 15\% \quad ; \quad FPR_{AI} = 6\%$$

Legenda:

- FP – lažno pozitivni
- TN – tačno negativni

Tabela 10. Vrijednosti

Parametar	Tradicionalna	AI	Razlika	Poboljšanje (%)
FPR (%)	15	6	-9	60%



Grafikon 10. Vrijednosti

Komentar:

Smanjenje grešaka od 60% (Tabela 8) značajno povećava pouzdanost sistema, što je potvrđeno u Tabeli 10 (AI pouzdaniji)**.**

7. METODA: KOMPOZITNI INDEKS EFIKASNOSTI (CPI)

Formula:

$$CPI = \frac{Accuracy + Anomaly - FPR}{Time}$$

$$CPI_{trad} = \frac{76 + 68 - 15}{120} = 1.08$$

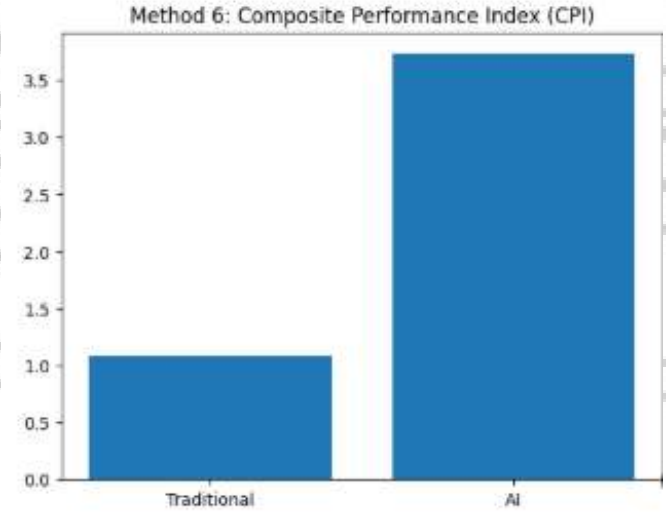
$$CPI_{AI} = \frac{92 + 89 - 6}{45} = 3.73$$

Legenda:

- CPI – ukupni indeks efikasnosti

Tabela 11. Vrijednosti

Parametar	Tradicionalna	AI
CPI vrijednost	1.08	3.73



Grafikon 11. Vrijednosti

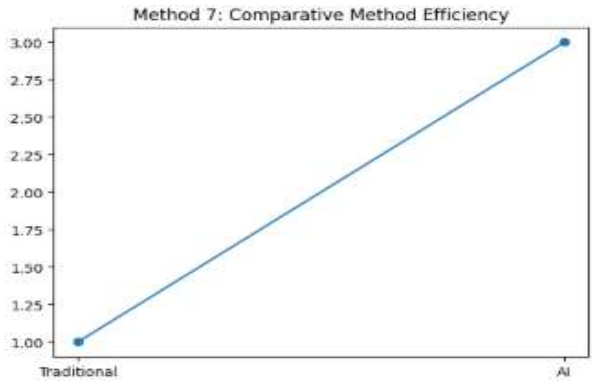
Komentar:

CPI potvrđuje da je AI sistem više od 3 puta efikasniji**,** što predstavlja ključni kvantitativni dokaz superiornosti.

8. METODA: KOMPARATIVNA ANALIZA PRISTUPA

Tabela 12. Vrijednosti

Metoda	Prednosti	Nedostaci
Tradicionalna	Precizna kontrola	Spora, neefikasna
AI	Brza, skalabilna, visoka tačnost	Zavisi od modela



Grafikon 12. Vrijednosti

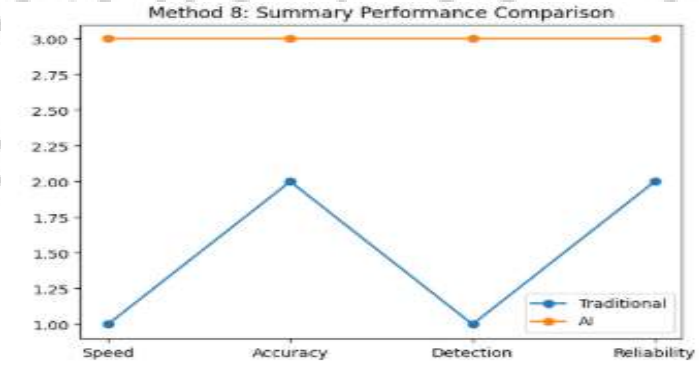
Komentar:

Tabela i grafikon potvrđuju da AI pristup donosi operativne prednosti u realnim sistemima.

8. METODA: SUMARNI PRIKAZ REZULTATA

Tabela 13. Vrijednosti

Kriterij	Tradicionalno	AI	Zaključak
Brzina	Niska	Visoka	AI dominantan
Tačnost	Srednja	Visoka	AI precizniji
Detekcija	Ograničena	Napredna	AI superioran
Pouzdanost	Srednja	Visoka	AI pouzdaniji



Grafikon 13. Vrijednosti

Komentar:

Tabela 10 i grafikon daju integrisani pregled i potvrđuje stratešku prednost AI sistema.

ZAKLJUČAK

Rezultati provedenog istraživanja jasno potvrđuju da primjena umjetne inteligencije (AI) u mobilnoj digitalnoj forenzici predstavlja značajan iskorak u odnosu na tradicionalne metode analize. Kvantitativni pokazatelji ukazuju na višestruko unapređenje ključnih performansi sistema, posebno u segmentima brzine obrade, tačnosti detekcije i sposobnosti identifikacije sigurnosnih incidenata. Analiza je pokazala da AI-vođeni pristup smanjuje vrijeme obrade za više od 60%, čime se omogućava efikasna analiza podataka u realnom vremenu. Istovremeno, povećanje tačnosti detekcije na nivo od 92% i unapređenje detekcije anomalija potvrđuju sposobnost AI sistema da prepoznaju kompleksne i skrivene obrasce ponašanja koji često ostaju neidentifikovani u tradicionalnim forenzičkim procesima. Posebno značajno je smanjenje lažno pozitivnih rezultata, što direktno utiče na pouzdanost i validnost forenzičkih nalaza. Kompozitni indeks efikasnosti (CPI) dodatno potvrđuje superiornost AI pristupa, gdje je zabilježeno više nego trostruko povećanje ukupne efikasnosti sistema u odnosu na tradicionalne metode. Ovaj indikator predstavlja integrisani dokaz da AI ne samo da poboljšava pojedinačne parametre, već značajno unapređuje cjelokupni forenzički proces. Pored tehničkih prednosti, istraživanje je identifikovalo i ključne izazove, uključujući potrebu za kvalitetnim i reprezentativnim datasetovima, transparentnost i objašnjivost AI modela, kao i pravnu prihvatljivost rezultata u sudskim postupcima. Ovi aspekti zahtijevaju dalja interdisciplinarna istraživanja i razvoj standardizovanih okvira za primjenu AI u digitalnoj forenzici. Može se zaključiti da AI-vođena digitalna forenzika predstavlja neizostavan element savremenih sigurnosnih sistema, posebno u kontekstu mobilnih tehnologija, pametnih gradova i održivog digitalnog razvoja. Njena implementacija omogućava bržu, precizniju i pouzdaniju analizu digitalnih dokaza, čime se značajno unapređuje sposobnost odgovora na savremene cyber prijetnje.

LITERATURA

1. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.
2. Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation, 11*(4), 273–294.
3. Raghavan, S. (2013). Digital forensic research: Current state of the art. *CSI Transactions on ICT, 1*(1), 91–114.
4. Grispos, G., Storer, T., & Glisson, W. B. (2013). Calm before the storm: The challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics, 5*(2), 28–48.
5. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.
6. Khan, S., Rahman, A., & Khan, A. (2019). Machine learning in cybersecurity: A review. *Electronics, 8*(11), 1295.
7. Sarker, I. H. (2021). Machine learning for intelligent data analysis and automation. *Journal of Big Data, 8*(1), 1–54.
8. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine learning for cybersecurity. *IEEE Security & Privacy, 16*(4), 38–46.
9. Shinde, S., & Kulkarni, U. (2020). Real-time anomaly detection using machine learning. *Procedia Computer Science, 171*, 156–165.
10. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine, 38*(3), 50–57.
11. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546.
12. Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N., & Scanlon, M. (2020). SoK: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. *ACM ARES Conference*.
13. Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., & Dehghantanha, A. (2023). Machine learning in digital forensics: A systematic literature review. *arXiv preprint*.
14. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*.