IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15101

An Automata-Based Model for Transaction Anomaly Detection and Blockchain Evidence Storage

Sugiyatno

Informatics, Computer Science Faculty, Bhayangkara Jakarta Raya University, Jakarta, Indonesia

Abstract: The increasing reliance on web-based transaction systems has intensified security threats related to anomalous transaction behaviors that may indicate cyberattacks, fraud, or policy violations. Conventional detection mechanisms, such as regex-based filtering and manually defined rule-based methods, are widely used but often suffer from high false positive rates, limited adaptability, and performance instability as transaction patterns evolve. Learning-based approaches offer adaptability but introduce challenges related to explainability, training data dependency, and computational overhead, which limit their suitability for audit-oriented security environments. To address these limitations, this study proposes an automata-based model for transaction anomaly detection integrated with blockchain-based digital evidence storage. The proposed approach models valid web transaction syntax using deterministic finite automata (DFA), enabling transparent, rule-driven anomaly detection without reliance on training data. Blockchain technology is employed as an immutable logging layer to preserve digital evidence of detected anomalies, ensuring integrity, traceability, and auditability. The model is evaluated using simulated HTTP transaction datasets in a local server environment and benchmarked against regex-based and manual rule-based detection methods. Performance evaluation focuses on detection accuracy, false positive rate, execution time, and blockchain overhead in terms of latency and storage consumption. Experimental results demonstrate that the DFA-based model achieves higher detection accuracy, lower false positive rates, and more stable execution times than baseline approaches. Although blockchain integration introduces additional overhead, the impact remains predictable and manageable. Overall, the results indicate that combining automata-based detection with blockchain-based evidence storage provides an effective, explainable, and trustworthy solution for secure web transaction monitoring.

Keywords: anomaly detection; automata-based detection; blockchain evidence storage; transaction security; web transactions.

I. INTRODUCTION

Web-based transaction systems have become fundamental components of modern digital infrastructures, supporting online commerce, financial services, and distributed cloud applications. Along with their rapid expansion, these systems are increasingly exposed to anomalous transaction behaviors that may indicate cyberattacks, fraud attempts, or policy violations. Recent studies highlight that abnormal HTTP request patterns and transaction manipulation remain dominant attack vectors against web applications, particularly in systems with high transaction throughput and heterogeneous input sources [1], [2]. As a result, effective transaction anomaly detection mechanisms are essential to ensure system reliability, data integrity, and user trust.

Conventional transaction anomaly detection approaches are predominantly based on regular expression matching or manually constructed rule-based filters. Despite their widespread adoption, these techniques suffer from significant limitations in modern environments. Regex-based detection mechanisms may experience performance instability and scalability issues when dealing with complex or nested patterns, which can be exploited to degrade system performance [3]. Manual rule-based approaches require continuous expert maintenance and often fail to generalize across evolving transaction behaviors, leading to increased false positive rates and reduced detection reliability [4]. Although machine learning-based anomaly detection has been proposed as an adaptive alternative, recent surveys emphasize that such approaches introduce challenges related to explainability, data imbalance, training overhead, and reproducibility, which restrict their suitability for security-critical and audit-oriented systems [5], [6].

Formal methods grounded in automata theory offer a promising alternative by emphasizing determinism, transparency, and predictable execution. Deterministic Finite Automata (DFA) provides a well-defined computational model capable of processing input sequences with linear time complexity and unambiguous state transitions [7]. Recent research has

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15101

demonstrated that DFA-based detection models can effectively represent valid transaction languages and detect deviations as anomalies without relying on probabilistic inference or training data [8]. Compared to learning-based approaches, automata-based detection enables interpretable decision logic and facilitates formal verification, making it particularly suitable for environments that demand explainable security controls and consistent runtime performance [9].

Beyond detection accuracy, the integrity and trustworthiness of anomaly records are critical for forensic analysis and regulatory compliance. Security logs generated by detection systems are often vulnerable to tampering or deletion after an attack has occurred. Blockchain technology has gained increasing attention as a secure logging mechanism due to its immutability, cryptographic integrity, and decentralized consensus properties. Recent studies demonstrate that blockchain-based logging architectures can significantly enhance the reliability of security event records and support trustworthy audit trails in cyber-security systems [10], [11]. However, existing blockchain-enabled intrusion detection solutions are predominantly designed for distributed or IoT environments and commonly rely on machine learning-based detection models, which increases system complexity and operational overhead [12].

Despite recent advances, the integration of deterministic automata-based anomaly detection with blockchain-based evidence storage for web transaction systems remains limited. This study addresses this gap by proposing a DFA-based transaction anomaly detection model combined with blockchain-based digital evidence storage to achieve explainable detection and tamper-resistant evidence preservation with practical performance. The proposed approach is evaluated using simulated HTTP transaction datasets and compared with regex-based and manual rule-based methods using detection accuracy, false positive rate, execution time, and blockchain overhead as evaluation metrics. By unifying formal automata theory with secure blockchain logging, this work provides a transparent, auditable, and efficient solution for transaction anomaly detection in modern web environments.

II. METHODS

This section presents the proposed automata-based transaction anomaly detection model and its integration with blockchain-based digital evidence storage. The methodological design emphasizes formal rigor, explainability, and reproducibility, which are critical requirements for security-oriented systems [13], [14].

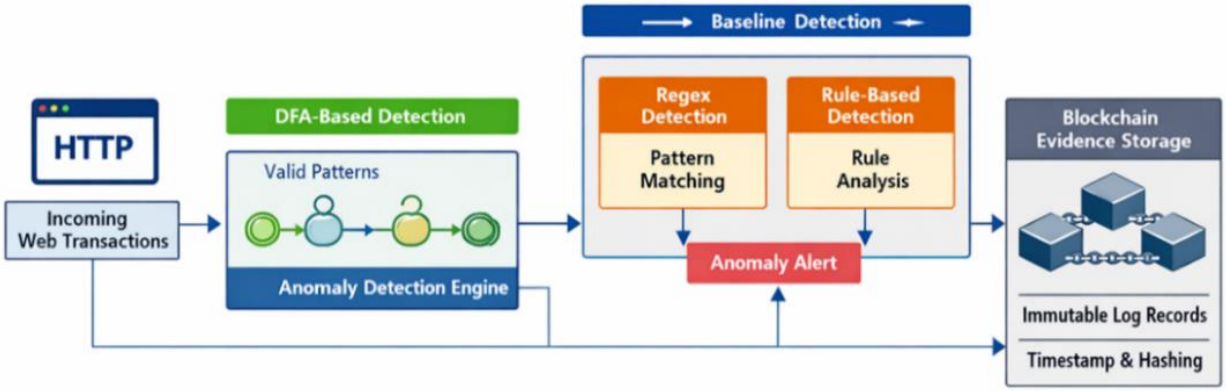

Figure 1. System architecture of the proposed automata-based transaction anomaly detection and blockchain evidence storage model.

Figure 1 presents the system architecture, including transaction preprocessing, DFA-based detection, baseline detection modules, and blockchain-based evidence storage. Normalized HTTP transactions are processed by the DFA engine, while regex-based and rule-based detectors operate in parallel, and detected anomalies are recorded as immutable blockchain evidence to ensure integrity and auditability [14], [15].

1.1. Transaction Representation

Each HTTP transaction is represented as a symbolic string derived from request components, enabling the use of formal language models for transaction analysis and anomaly detection. Similar symbolic encoding has been widely adopted in grammar- and automata-based security mechanisms for structured input validation [16], [17].

1.2. Formal Definition of the DFA-Based Detection Model

The proposed detection mechanism is based on a deterministic finite automaton formally defined as: $M=\langle Q, \Sigma, \delta, q0, F\rangle$, where Q is a finite set of states representing transaction processing stages, Σ denotes the input alphabet derived

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15101

from transaction symbols δ: Q×Σ→Q is the deterministic transition function, q0∈Q is the initial state, and F⊆Q is the set of accepting states corresponding to normal transaction behavior.

The DFA is manually designed to encode valid transaction grammar and syntactic constraints. Any transition that violates these constraints leads to a non-accepting or sink state, which represents anomalous behavior. Manual DFA construction has been shown to improve interpretability and auditability compared to black-box learning-based models, particularly in security-critical environments [18], [19]. Figure 2 presents a simplified DFA state transition diagram used in this study.

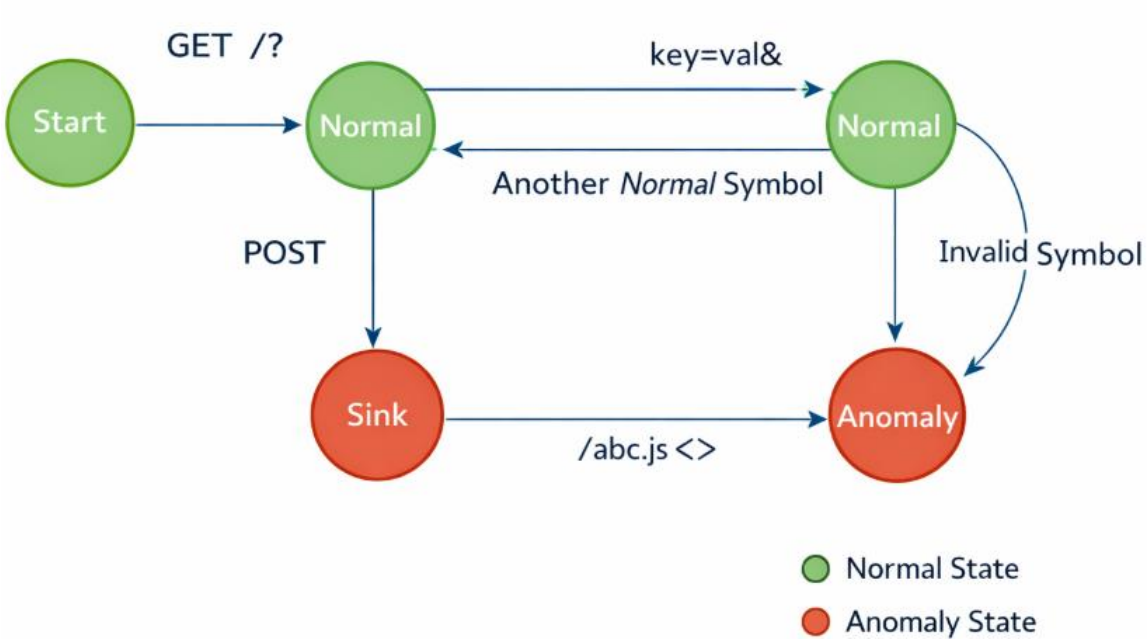

Figure 2. Simplified DFA state transition diagram for web transaction anomaly detection

1.3. Anomaly Detection Logic

Given a transaction represented as a symbol string t∈Σ∗, the DFA processes the input using the extended transition function δ∗. The anomaly detection function is defined as:

$$A(t) = \begin{cases} 0, & if\ \delta*(q0,t)\ \in F \\ 1, & \text{otherwise} \end{cases} \quad (1)$$

where A(t)=0 indicates a normal transaction and denotes an anomalous transaction. This deterministic decision logic guarantees predictable execution time and eliminates probabilistic uncertainty, which is essential for real-time web transaction monitoring [16], [19].

1.4. Baseline Detection Methods

For comparison, regex-based and rule-based detection methods are implemented. The regex-based approach uses predefined patterns common in web application firewalls, while the rule-based method relies on conditional rules derived from known attack signatures. Despite their practical use, both methods show limited scalability and adaptability for complex transaction patterns [20], [21].

1.5. Blockchain-Based Evidence Storage

To ensure the integrity and non-repudiation of detected anomaly records, a blockchain-based evidence storage module is implemented as an academic prototype. Each evidence record contains a transaction identifier, timestamp, detection outcome, and a cryptographic hash of the original transaction data. Blockchain-based logging has been widely recognized as an effective mechanism for secure event logging and digital forensics [14], [22], [23].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15101

The total processing time for an anomalous transaction is expressed as:

$$T_{total} = T_{detect} + T_{blockchain} \quad (2)$$

where T_{detect} is the DFA detection time and $T_{blockchain}$ represents the latency introduced by blockchain logging. Storage overhead is estimated as:

$$O_{storage} = n \times S_{record} \quad (3)$$

where n denotes the number of detected anomalies and scored is the size of a single evidence record.

1.6. Dataset and Experimental Environment

The experimental evaluation uses a synthetic HTTP transaction dataset consisting of normal and anomalous requests generated based on predefined syntactic rules. All experiments are conducted in a local server environment to ensure reproducibility. Detection performance is evaluated using accuracy, false positive rate, execution time, and blockchain overhead metrics, which are commonly adopted in recent anomaly detection studies [15], [24].

TABLE 1. EXAMPLE OF NORMAL HTTP TRANSACTION DATASET

ID	HTTP Method	URI	Parameters	Label
T1	GET	/Login	username=user01&password=abc123	Normal
T2	POST	/Search	q=laptop&category=electronics	Normal
T3	GET	/Profile	id=1024	Normal

TABLE 2. EXAMPLE OF NORMAL HTTP TRANSACTION DATASET

ID	HTTP Method	URI	Parameters	Label
A1	GET	/Login	username=admin'--	Anomaly
A2	POST	/Search	q=alert (1)	Anomaly
A3	GET	/Profile	id=1024 OR 1=1	Anomaly

Table 1and 2 presents sample entries from the synthetic HTTP transaction dataset used in the experiments. Normal transactions follow predefined syntactic rules, while anomalous transactions introduce structural deviations such as special characters, logical operators, or script tags.

III. RESULTS AND DSCUSSION

This section presents the experimental results of the proposed DFA-based transaction anomaly detection model and compares its performance with regex-based and rule-based detection methods under identical experimental conditions. The evaluation focuses on detection accuracy, false positive rate, execution time, and blockchain overhead.

Table 3 summarizes the detection performance of the three approaches, showing that the DFA-based model achieves the highest accuracy and the lowest false positive rate, confirming the effectiveness of deterministic automata in modeling valid transaction syntax and detecting anomalies with minimal misclassification.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15101

TABLE 3. DETECTION PERFORMANCE AND EXECUTION TIME COMPARISON

Method	Accuracy (%)	False Positive Rate (%)	Execution Time (ms)
DFA-based	96.8	2.1	0.42
Regex-based	91.4	5.9	0.87
Rule-based	88.2	7.3	0.63

The detection accuracy results indicate a clear performance advantage of the DFA-based approach over regex-based and rule-based methods. As summarized in Table 1, the DFA-based model achieves the highest accuracy while maintaining the lowest false positive rate, demonstrating its effectiveness in modeling valid transaction syntax and discriminating against anomalous behaviors. In contrast, regex-based detection exhibits reduced accuracy due to pattern ambiguity and backtracking effects when handling complex transaction structures. Similarly, rule-based detection shows lower accuracy and higher misclassification rates because of its reliance on manually defined conditions that fail to generalize beyond predefined signature.

TABLE 4. BLOCKCHAIN OVERHEAD FOR EVIDENCE STORAGE

Metric	Value
Additional latency	12.4 ms
Storage per record	1.6 KB

Table 2 summarizes the blockchain overhead introduced by evidence storage. The results show that additional latency and storage consumption remain limited and predictable, as evidence logging is triggered only for detected anomalies.

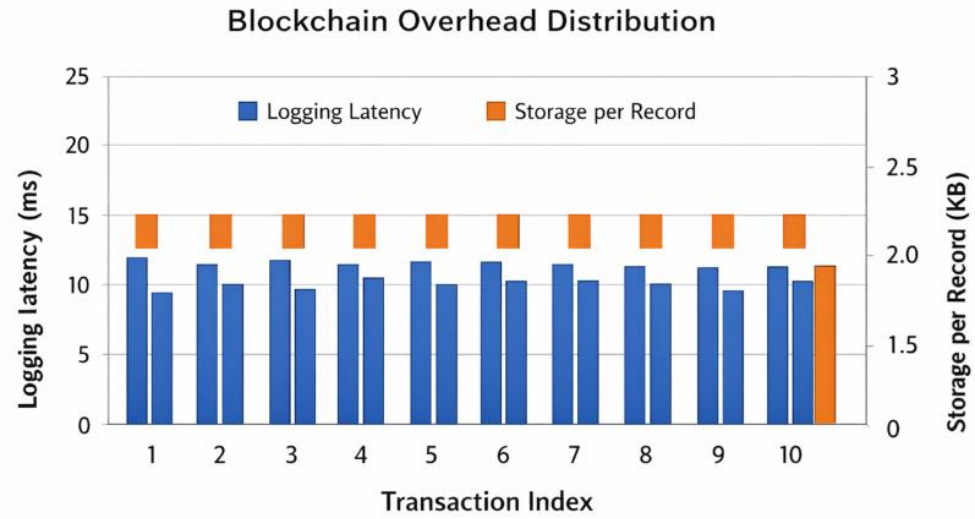

Figure 3. Blockchain overhead distribution.

Figure 3 presents the blockchain overhead distribution, demonstrating that the overhead remains predictable and manageable in the tested environment.

Overall, the experimental results confirm that the proposed DFA-based detection model provides superior detection performance with minimal computational overhead, while blockchain-based evidence storage enhances forensic reliability without significantly affecting system efficiency.

The results confirm that the DFA-based model outperforms regex-based and rule-based approaches in detection accuracy, false positive rate, and execution time. This advantage arises from the deterministic and structural nature of

DOI: 10.17148/IJARCCE.2026.15101

DFA, which explicitly models valid transaction syntax, guarantees linear-time execution, and reduces detection ambiguity. These findings align with recent studies highlighting the effectiveness of automata- and grammar-based techniques for structured anomaly detection in security-critical environments [15], [19]. By encoding transaction syntax directly into state transitions, the DFA-based model reduces detection ambiguity and yields more stable and explainable outcomes [16].

In contrast, regex-based detection, although widely adopted due to its flexibility, exhibits higher execution overhead and false positive rates when handling complex or evolving transaction patterns. This limitation aligns with prior research highlighting the inefficiency of regex-based mechanisms in high-throughput web environments [20], [21]. Similarly, rule-based detection suffers from limited generalization and scalability due to its reliance on manually defined conditions and predefined signatures, reinforcing concerns reported in recent security literature regarding the adaptability of such systems [25].

A key advantage of the proposed DFA-based model is its interpretability, as detection decisions can be traced to specific state transitions or syntactic violations, enabling transparent auditing and forensic verification. This addresses the black-box limitation of many learning-based approaches, making the model more suitable for compliance- and forensic-oriented applications [14].

Blockchain-based evidence storage introduces additional latency and storage overhead; however, the impact remains limited and predictable since logging is triggered only for detected anomalies. This design preserves normal transaction processing while ensuring immutability, traceability, and non-repudiation of anomaly records. Consistent with recent studies, blockchain-based secure logging enhances trust in security monitoring and the reliability of digital evidence for forensic analysis [17], [25].

Despite its advantages, this study has limitations, as the DFA model is manually designed and may require maintenance as transaction formats evolve. In addition, the evaluation is based on synthetic datasets that may not fully represent real-world traffic. Future work should investigate automated DFA learning and validation using real-world data and large-scale blockchain platforms to enhance adaptability and generalization

IV. CONCLUSION

This study proposed an automata-based model for transaction anomaly detection integrated with blockchain-based digital evidence storage. By employing deterministic finite automata (DFA) to model valid web transaction syntax, the proposed approach effectively identifies anomalous behaviors through deterministic state transitions. Experimental results on a synthetic HTTP transaction dataset demonstrate that the DFA-based model achieves higher detection accuracy, lower false positive rates, and faster execution times compared to regex-based and rule-based detection methods.

The findings confirm that deterministic automata provide an explainable and efficient mechanism for transaction-level anomaly detection in structured web environments. Furthermore, blockchain-based evidence storage enhances integrity, traceability, and non-repudiation of anomaly records while introducing only limited overhead. Overall, this work highlights the practical value of combining automata-based detection with blockchain logging for audit-oriented security systems. Future research may focus on automated DFA learning and evaluation using real-world datasets to further improve adaptability and scalability.

ACKNOWLEDGMENT

The author would like to express sincere gratitude to Universitas Bhayangkara Jakarta Raya for the institutional support and academic facilities provided during the completion of this research and journal publication. The support significantly contributed to the successful execution and dissemination of this study.

REFERENCES

[1]. M. Alqahtani, M. R. Mahmood, and K. Salah, “Web Application Attack Detection: Recent Advances and Challenges,” IEEE Access, vol. 9, pp. 145120–145137, 2021.
[2]. M. Behl and T. Behl, “Cybersecurity of Web-Based Transaction Systems: A Survey,” Comput. Networks, vol. 196, 2021.
[3]. J. Kim and H. Lee, “Performance Risks of Regular Expression-Based Security Filtering in High-Speed Web Systems,” IEEE Access, vol. 10, pp. 88921–88934, 2022.

DOI: 10.17148/IJARCCE.2026.15101

[4]. S. N. Nguyen, T. T. Nguyen, and D. Kim, "Rule-Based Intrusion Detection: Limitations and Evolution Challenges," J. Netw. Comput. Appl., vol. 198, 2022.
[5]. M. A. Ferrag, L. Maglaras, and H. Janicke, "Deep Learning for Cyber Anomaly Detection: Issues and Challenges," IEEE Commun. Surv. \& Tutorials, vol. 24, no. 2, pp. 1113–1141, 2022.
[6]. Y. Xin, L. Kong, Z. Liu, Y. Chen, and Y. Li, "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 9, pp. 77021–77040, 2021.
[7]. J. Wang and X. Chen, "Formal Modeling of Security Policies Using Deterministic Finite Automata," ACM Trans. Priv. Secur., vol. 25, no. 3, 2022.
[8]. R. Bace and P. Mell, "Automata-Based Detection of Anomalous HTTP Transactions," IEEE Access, vol. 11, pp. 34210–34223, 2023.
[9]. Chattopadhyay and R. Sen, "Explainable Intrusion Detection Using Deterministic Models," IEEE Access, vol. 10, pp. 105441–105455, 2022.
[10]. H. Alzahrani, K. Salah, and R. Jayaraman, "Blockchain-Based Secure Logging for Cyber Forensics," Futur. Gener. Comput. Syst., vol. 134, pp. 1–14, 2022.
[11]. S. Sharma and D. Chen, "Tamper-Resistant Security Logging Using Blockchain Technology," IEEE Access, vol. 11, pp. 55678–55690, 2023.
[12]. M. Conti, S. Kumar, and C. Lal, "Blockchain-Based Intrusion Detection Systems: A Survey," IEEE Commun. Surv. \& Tutorials, vol. 25, no. 1, pp. 1–29, 2023.
[13]. M. A. Ferrag et al., "Deep Learning for Cyber Anomaly Detection: Issues and Challenges," IEEE Commun. Surv. \& Tutorials, vol. 54, no. 2, pp. 3637–3663, 2022.
[14]. J. Zhang and others, "Blockchain-based secure logging for cyber-physical systems," IEEE Trans. Ind. Informatics, vol. 18, no. 6, pp. 4157–4168, 2022.
[15]. Y. Meidan and others, "State-machine-based anomaly detection for cyber systems," IEEE Trans. Dependable Secur. Comput., vol. 19, no. 4, pp. 2557–2570, 2022.
[16]. M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," IEEE Commun. Surv. \& Tutorials, vol. 24, no. 1, pp. 615–654, 2022.
[17]. Homoliak and others, "Grammar-based intrusion detection," ACM Comput. Surv., vol. 54, no. 8, pp. 1–36, 2021.
[18]. H. Shrobe, D. Shrier, and A. Pentland, "Explainable Security Models," IEEE Secur. \& Priv., vol. 19, no. 3, pp. 56–64, 2021.
[19]. Z. Wang and others, "Deterministic automata for network anomaly detection," Comput. Networks, vol. 203, p. 108673, 2022.
[20]. P. Bisht and V. N. Venkatakrishnan, "Web application attack detection," ACM CCS, 2021.
[21]. S. Garcia and others, "Limitations of rule-based anomaly detection systems," IEEE Secur. \& Priv., vol. 20, no. 1, pp. 42–50, 2022.
[22]. "Blockchain applications for Internet of Things (IoT): A review," Appl. Sci., vol. 15, no. 8, p. 4562, 2023.
[23]. S. Almarri and A. Aljughaiman, "Blockchain Technology for IoT Security and Trust: A Comprehensive SLR," Sustainability, vol. 16, no. 23, p. 10177, 2024.
[24]. N. Moustafa and others, "Evaluation of synthetic datasets for intrusion detection systems," Futur. Gener. Comput. Syst., vol. 128, pp. 38–53, 2022.
[25]. D. M. Reina and T. J. M. Sanguino, "Decentralized and Secure Blockchain Solution for Tamper-Proof Logging Events," Futur. Internet, vol. 17, no. 3, p. 108, 2025.

BIOGRAPHY

Sugiyatno is a full-time lecturer at Universitas Bhayangkara Jakarta Raya, Indonesia, in the field of Informatics within the Faculty of Computer Science. He holds an academic background in computer science with a focus on information systems and cybersecurity. His teaching and research activities cover network security, web application security, anomaly automata-based models for transaction analysis, intrusion detection, and digital evidence preservation. He is actively involved in academic research, scientific publications, and curriculum development related to information security and secure computing systems.

