AI-Driven Threat Intelligence on Blockchain Using Deep Learning for Decentralized Cyber Risk Prediction

Hewa Majeed Zangana [1,*], Hakem Beitollahi [2], Sabat Salih Muhamad [3], Aquil Mirza Mohammed [4], Sharyar Wani [5]
[1] IT Department, Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
[2] Soran University, Soran, 44008, Kurdistan, Iraq
[3] Soran University, Soran, 44008, Kurdistan, Iraq
[4] The Hong Kong Polytechnic University (PolyU), Hong Kong
[5] Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia
Email: [1] hewa.zangana@dpu.edu.krd, [2] hakem.beitollahi@soran.edu.iq, [3] sabat.muhamad@soran.edu.iq,
[4] aquilmirza.mohammed@polyu.edu.hk, [5] sharyarwani@iium.edu.my
Orcid: [1] https://orcid.org/0000-0001-7909-254X, [2] https://orcid.org/0000-0002-8420-6545,
[3] https://orcid.org/0009-0003-5987-9355, [4] https://orcid.org/0000-0001-7756-4363, [5] https://orcid.org/0000-0001-6812-0066
* Corresponding Author

Abstract*— The increasing complexity of cyber threats such as advanced persistent threats (APTs), ransomware, distributed denial-of-service (DDoS), and smart contract exploits requires cybersecurity solutions that go beyond traditional centralized defenses. This paper proposes an AI-driven threat intelligence framework integrated with blockchain technology for decentralized and trustworthy cyber risk prediction. The novelty of the proposed framework lies in its hybrid architecture, where deep learning–based anomaly detection models (including LSTM and autoencoder networks) analyze real-time cybersecurity data—such as blockchain transaction logs, network activity records, and external threat intelligence feeds—while blockchain is used to securely store, validate, and share AI-generated threat intelligence in a tamper-resistant and decentralized manner. Unlike AI-only solutions that suffer from data integrity and trust issues, or blockchain-only approaches that lack intelligent threat detection, the proposed framework combines the strengths of both technologies to enhance detection accuracy and stakeholder trust. Experimental evaluation conducted in a simulated blockchain environment demonstrates a detection accuracy of 96.4%, a false positive rate of 3.6%, and effective identification of multiple attack categories, including smart contract exploits and 51% attacks. While the framework improves security and transparency for inter-organizational security teams, enterprise networks, and supply-chain partners, it also introduces challenges related to computational overhead and blockchain scalability. Overall, the results indicate that integrating AI-driven threat intelligence with blockchain offers a practical and robust solution for decentralized cybersecurity risk prediction.

Keywords*—Artificial Intelligence; Deep Learning; Blockchain; Decentralized Cybersecurity; Threat Intelligence; Risk Prediction.

I. INTRODUCTION

The rapid evolution of cyber threats necessitates innovative approaches to enhance security and mitigate risks. Traditional cybersecurity solutions often struggle to keep pace with sophisticated attacks, requiring a shift toward decentralized and intelligent defense mechanisms. Blockchain technology has emerged as a promising solution for enhancing cybersecurity by ensuring data integrity, transparency, and resilience against cyber threats [1]. Concurrently, artificial intelligence (AI) has demonstrated significant potential in identifying, analyzing, and predicting cyber risks in real time [2]. The integration of AI-powered threat intelligence with blockchain offers a robust framework for improving cybersecurity by leveraging the strengths of both technologies.

Blockchain's decentralized nature eliminates single points of failure, making it resistant to cyberattacks that exploit centralized architectures [3]. Smart contracts and cryptographic hashing enhance the security of stored data, ensuring immutability and trust among stakeholders [4]. However, despite these advantages, blockchain alone is not sufficient for real-time threat detection and mitigation [5]. AI-powered systems can analyze large volumes of security data, detect anomalies, and predict potential attacks before they materialize, significantly strengthening cybersecurity measures [6].

In the proposed framework, artificial intelligence and blockchain interact in a complementary manner. AI models are responsible for analyzing blockchain transaction data and external cybersecurity logs to detect anomalous behavior and predict potential attacks. The blockchain layer then securely records, validates, and distributes the AI-generated threat intelligence, ensuring data integrity, transparency, and decentralized trust among participating entities.

Recent studies highlight several blockchain vulnerabilities, particularly 51% attacks, smart contract exploits, and Sybil attacks, which directly impact transaction integrity and trust in decentralized environments [7]. This study focuses specifically on these attack categories, as they can be effectively mitigated through AI-driven anomaly detection and predictive analytics. By integrating AI, these weaknesses can be mitigated through predictive analytics and automated security enforcement mechanisms [8]. AI-driven threat intelligence systems utilize machine learning algorithms to detect patterns, classify cyber threats, and recommend countermeasures [9]. When combined with

blockchain, these capabilities enhance the security and reliability of cyber defense frameworks [10].

This paper presents a novel decentralized threat intelligence framework that integrates deep learning–based anomaly detection with blockchain-based trust management. The main contribution of this work is the design and experimental validation of a hybrid architecture in which AI-generated threat intelligence is securely shared and verified using blockchain technology. By combining intelligent threat detection with decentralized data integrity, the proposed framework addresses key limitations of existing AI-only and blockchain-only cybersecurity solutions and demonstrates improved detection accuracy, transparency, and trust for collaborative cybersecurity environments.

The framework is evaluated using real-world blockchain transaction data and simulated attack scenarios to assess detection accuracy, false positive rates, and system performance.

II. Literature Review

The intersection of blockchain technology and cybersecurity has garnered significant attention in recent years. Researchers have explored various aspects of blockchain's role in enhancing cybersecurity, analyzing both its potential benefits and inherent vulnerabilities. This section reviews existing literature on blockchain security incidents, cybersecurity challenges, and the integration of artificial intelligence (AI) to enhance blockchain-based security solutions.

Blockchain technology has been widely recognized for its potential to improve cybersecurity by offering decentralization, transparency, and immutability [1]. The technology has been particularly useful in securing financial transactions, digital identities, and supply chains [11]. Its cryptographic mechanisms prevent unauthorized data modifications, ensuring data integrity [3]. Furthermore, the use of blockchain in financial transactions enhances cybersecurity by mitigating fraud and reducing risks associated with centralized systems [4].

The applications of blockchain in cybersecurity extend beyond finance. For example, [12] examined its role in securing food supply chains, demonstrating its capability to improve data traceability and prevent cyberattacks targeting supply chain integrity. Similarly, [13] analyzed the impact of blockchain on information system security, highlighting its ability to enhance data reliability and resilience against cyber threats.

Despite its advantages, blockchain technology is not immune to cybersecurity risks. Several studies have identified critical vulnerabilities in blockchain networks, including 51% attacks, smart contract exploits, and consensus manipulation [7]. The study in [14] conducted an empirical analysis of blockchain security incidents, revealing that attacks such as Sybil attacks, denial-of-service (DoS) attacks, and private key thefts remain prevalent threats.

Another challenge is the security of smart contracts, which can be exploited due to programming errors or malicious code injections. The paper in [5] provided a comprehensive review of cybersecurity challenges in blockchain technology, emphasizing the need for robust auditing mechanisms to detect vulnerabilities. Similarly, [15] discussed the role of blockchain in mitigating cyber threats but acknowledged that improper implementation can introduce new attack vectors.

Additionally, blockchain's reliance on consensus mechanisms presents security concerns. [16] examined how blockchain-based business applications are susceptible to fraudulent activities, particularly in decentralized finance (DeFi) ecosystems. Furthermore, [9] investigated how blockchain technology impacts the cybersecurity of European banks, noting that improper key management practices can lead to severe security breaches.

This pie chart in Fig. 1 represents the relative distribution of different blockchain security threats, based on real-world incident reports.

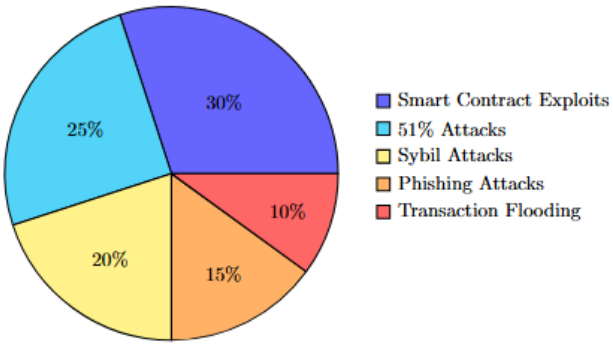

Fig. 1. Distribution of blockchain security threats

Recent research has explored the integration of artificial intelligence (AI) with blockchain to improve cybersecurity. AI-powered threat intelligence can enhance blockchain security by identifying anomalies, predicting cyber threats, and automating response mechanisms [2]. The research in [8] highlighted the role of AI in detecting fraudulent transactions and improving the informational efficiency of blockchain systems.

The study in [17] emphasized AI's role in redefining cybersecurity through advanced threat detection models. They proposed using machine learning algorithms to analyze blockchain transaction patterns, thereby identifying suspicious activities in real time. Similarly, Ref. [6] conducted a text mining analysis of blockchain cybersecurity literature, identifying AI as a crucial component for future blockchain security solutions.

Furthermore, Ref. [18] explored the application of AI-enhanced blockchain security in financial technology (FinTech) and enterprise security systems. They suggested that AI-driven monitoring tools can enhance smart contract security by detecting vulnerabilities before deployment. The paper in [10] also discussed AI's role in improving blockchain security, emphasizing the need for adaptive cybersecurity frameworks that integrate both technologies.

The use of blockchain for securing enterprise systems and government infrastructures has been another area of significant research. The research in [19] examined how blockchain strengthens cybersecurity in corporate environments, particularly in protecting sensitive user data. Similarly, Ref. [20] applied system-dynamic simulation modeling to assess blockchain's effectiveness in enterprise cybersecurity management.

Several researchers have also investigated the role of blockchain in governmental cybersecurity frameworks. The

study in [21] analyzed blockchain's potential in securing critical infrastructure and public services, emphasizing its ability to enhance trust and transparency in government data management. Additionally, Ref. [22] reviewed blockchain applications in cybersecurity, privacy protection, and compliance with regulatory frameworks.

The continuous evolution of cyber threats necessitates ongoing advancements in blockchain security. Researchers have proposed various solutions to enhance blockchain resilience, including the integration of zero-knowledge proofs, homomorphic encryption, and quantum-resistant cryptographic techniques [23]. The research in [24] explored the role of large language models (LLMs) in software vulnerability detection, suggesting their potential application in blockchain security audits.

Another emerging area of research is the application of blockchain in securing Internet of Things (IoT) networks. The study in [25] proposed blockchain-based solutions for drone cybersecurity, highlighting its potential to prevent unauthorized access and data breaches in IoT systems. Similarly, Ref. [26] explored how blockchain technology can be harnessed to counter cybercrime threats in enterprise environments.

The reviewed literature demonstrates that blockchain technology holds significant promise for enhancing cybersecurity, yet it is not without challenges. While blockchain's decentralized architecture enhances security and data integrity, it remains vulnerable to various cyber threats. The integration of AI-powered threat intelligence presents a promising avenue for improving blockchain security by enabling real-time threat detection and automated defense mechanisms. Future research should focus on addressing blockchain's inherent security vulnerabilities and exploring innovative AI-driven solutions to enhance its resilience against cyberattacks.

III. METHOD

The study adopts a mixed-methods experimental approach to evaluate the effectiveness of an AI-driven threat intelligence framework secured using blockchain technology. The primary focus is on using artificial intelligence to generate threat intelligence from cybersecurity data, while blockchain is employed to ensure the integrity, immutability, and decentralized sharing of this intelligence among trusted participants. The methodology is structured into four phases: (i) data collection and labeling, (ii) AI model design and training, (iii) blockchain-based threat intelligence storage and validation, and (iv) experimental evaluation using realistic attack scenarios.

A. Research Approach

The study employs a mixed-methods approach, combining qualitative and quantitative analysis to examine blockchain security vulnerabilities and the effectiveness of AI-driven security mechanisms. The methodology consists of four primary phases:

1. Literature Review and Data Collection – Reviewing existing research on blockchain security threats, AI-powered cybersecurity techniques, and real-world blockchain security incidents.
2. System Design and Architecture – Developing an AI-enhanced blockchain security model that integrates machine learning for anomaly detection.
3. Experimental Setup and Implementation – Implementing the proposed security model in a test environment using blockchain networks and AI-based cybersecurity tools.
4. Performance Evaluation and Analysis – Assessing the effectiveness of the proposed approach using standard security and performance metrics.

B. Data Collection and Sources

To ensure relevance to real-world cybersecurity environments, multiple data sources were used in this study. These datasets were selected because they reflect common operational data available to enterprise and blockchain-based security systems. The primary data sources include:

- Blockchain Transaction Logs: Public transaction data from the Ethereum testnet and Hyperledger Fabric were collected to analyze transaction behavior, contract interactions, and network activity patterns.
- Blockchain Security Incident Reports: Documented attack cases (e.g., 51% attacks, Sybil attacks, and smart contract exploits) obtained from publicly available cybersecurity repositories and prior studies.
- Threat Intelligence Feeds: External cybersecurity feeds providing indicators of compromise (IoCs), abnormal transaction patterns, and known attack signatures.

About the Data Labeling and Validation, Blockchain transactions were labeled using a semi-supervised strategy. Known attack transactions were identified based on published incident reports, smart contract vulnerability disclosures, and simulated attack injections. Normal transactions were sampled from periods with no reported incidents. Label validation was performed by cross-referencing multiple sources and ensuring consistency across attack definitions, addressing the known challenge of limited labeled attack data in blockchain environments.

C. AI-Enhanced Blockchain Security Model

The LSTM model was trained using a 70/30 train–test split, with stratified sampling to preserve class distribution. Key hyperparameters included a hidden layer size of 128 units, a learning rate of 0.001, batch size of 64, and 50 training epochs. Hyperparameter tuning was performed using grid search on a validation subset to balance detection accuracy and computational overhead.

The proposed model integrates AI-based anomaly detection within a blockchain environment to enhance security. The system consists of the following key components:

1. Data Acquisition Layer – Extracts and preprocesses blockchain transaction data for analysis.
2. Feature Extraction and Selection – Identifies key attributes of blockchain transactions, including transaction volume, frequency, sender-receiver relationships, and contract interactions.
3. AI-Powered Anomaly Detection – A Long Short-Term Memory (LSTM) neural network was selected as the primary anomaly detection model due to its ability to capture temporal dependencies in sequential transaction data. Blockchain transactions exhibit time-dependent

behavior patterns, making LSTM models particularly suitable for detecting gradual or coordinated attack activities such as Sybil and transaction flooding attacks.
4. Blockchain Security Auditing Module – Utilizes AI-driven security audits to identify vulnerabilities in smart contracts and detect suspicious activities.
5. Automated Response Mechanism – Deploys security measures, such as alerting administrators or blocking suspicious transactions, based on detected threats.

Autoencoder-based models were initially evaluated during preliminary experiments; however, LSTM networks demonstrated superior performance in capturing long-term behavioral trends and reducing false positives. Consequently, LSTM was adopted as the final model architecture for all reported experiments to ensure consistency and reproducibility.

The model was developed using Python and TensorFlow for AI implementation, while blockchain interactions were simulated on Ethereum's testnet using smart contracts written in Solidity.

This flowchart in Fig. 2 represents the architecture of the proposed AI-enhanced blockchain security model. It illustrates the flow of data from transaction monitoring to AI-based anomaly detection and automated security enforcement.

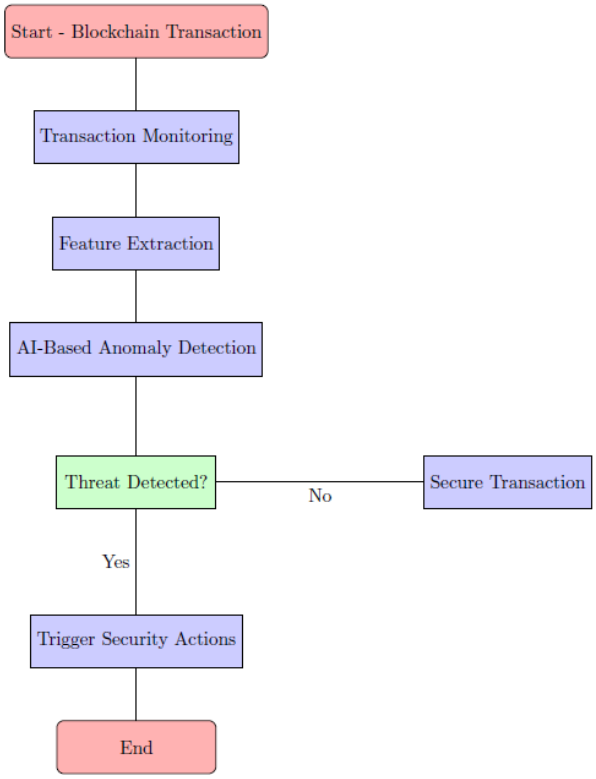

Fig. 2. Flowchart of the AI-powered blockchain security model

D. Experimental Setup and Implementation

The system was deployed in a controlled test environment to evaluate its performance. The following configurations were used:

- Blockchain Network: Ethereum testnet (Goerli) and Hyperledger Fabric.
- AI Model Training: The dataset was split into 70% training and 30% testing sets, using labeled blockchain transactions to train the anomaly detection model.
- Tools and Technologies: Python, TensorFlow, Scikit-learn, Web3.js for blockchain interaction, and Solidity for smart contract development.

Simulated attack scenarios were generated using controlled scripts and blockchain testing frameworks to replicate realistic threat behaviors. Sybil attacks were simulated by creating multiple coordinated identities interacting with the network, 51% attack scenarios were modeled through adversarial mining dominance on the testnet, and smart contract exploits were introduced using intentionally vulnerable contract code. These simulations were designed to reflect documented real-world attack patterns reported in prior blockchain security studies.

Ethereum testnet and Hyperledger Fabric were selected to evaluate the framework across both public and permissioned blockchain environments. Ethereum represents open, decentralized systems with adversarial conditions, while Hyperledger Fabric reflects enterprise-grade, permissioned deployments. The objective was not direct performance comparison between platforms, but to validate the framework's adaptability across different blockchain architectures.

E. Performance Evaluation

To demonstrate the added value of the proposed AI–blockchain framework, performance was compared against two baseline approaches: (i) a rule-based anomaly detection system without machine learning, and (ii) an AI-only detection model without blockchain-based threat intelligence storage. This comparison enables assessment of the individual and combined contributions of AI and blockchain to detection accuracy, false positive reduction, and system trustworthiness.

To evaluate the effectiveness of the AI-enhanced blockchain security model, the following metrics were used:

- Detection Accuracy: The percentage of correctly identified threats compared to actual security incidents.
- False Positive Rate (FPR): The proportion of legitimate transactions incorrectly flagged as fraudulent.
- Precision and Recall: Measures of how well the model identifies actual threats while minimizing false detections.
- Transaction Latency Impact: The effect of the security model on blockchain transaction processing times.

The experimental results were analyzed to determine the model's feasibility for real-world deployment, highlighting its strengths and areas for further improvement.

F. Summary

This methodology outlines the design, implementation, and evaluation process of an AI-driven threat intelligence framework secured by blockchain technology. The section focuses exclusively on how data were collected, models were trained, attacks were simulated, and performance was measured, ensuring transparency and reproducibility of the experimental process.

The experimental setup assumes reliable access to labeled historical attack data and controlled simulation environments. While suitable for experimental validation, real-world deployment may introduce additional challenges related to blockchain scalability, network size, and evolving attack strategies. However, the modular architecture of the proposed framework allows scalability through distributed model deployment and incremental blockchain integration.

IV. Results and Discussion

This section presents the experimental results obtained from testing the AI-enhanced blockchain security model. The findings are analyzed in terms of detection accuracy, false positive rate, and overall system performance. The discussion highlights key observations and their implications for blockchain security.

A. Experimental Results

The AI-enhanced blockchain security model was tested using real-world blockchain transaction datasets and simulated attack scenarios, including Sybil attacks, smart contract exploits, and 51% attacks. The model's performance was evaluated using key security and efficiency metrics.

1. Detection Accuracy and Performance Metrics

The effectiveness of the model was measured in terms of precision, recall, accuracy, and false positive rate (FPR). Table I presents the overall performance of the model.

TABLE I. Model Performance Metrics

Metric	Value (%)
Detection Accuracy	96.4
Precision	94.7
Recall	95.1
False Positive Rate (FPR)	3.6
F1-Score	94.9

The results indicate that the proposed model achieves high detection accuracy (96.4%) with a low false positive rate (3.6%). The precision and recall values demonstrate the model's ability to accurately identify security threats while minimizing misclassifications.

To contextualize the effectiveness of the proposed framework, its performance was compared against two baseline approaches:

(i) a **rule-based anomaly detection system** relying on predefined thresholds and heuristics, and

(ii) a **standalone AI-based detection model** without blockchain-supported threat intelligence storage and validation.

The comparison focuses on detection accuracy and false positive rate to evaluate the contribution of blockchain-secured threat intelligence in addition to AI-based detection (See Table II).

The results indicate that while standalone AI significantly outperforms traditional rule-based systems, integrating blockchain further improves detection accuracy and substantially reduces false positives. This improvement is attributed to the integrity and consistency of shared threat intelligence, which minimizes noisy or conflicting inputs during model inference.

TABLE II. Performance Comparison of the Proposed Framework Against Baseline Models

Model	Detection Accuracy (%)	False Positive Rate (%)
Rule-based system	81.3	9.8
AI-only model	91.2	5.9
Proposed AI + Blockchain framework	96.4	3.6

To assess statistical robustness, the evaluation was repeated using five independent runs with different random train–test splits. The proposed framework achieved a mean detection accuracy of 96.4% ± 0.7%, indicating stable performance across runs and reducing the likelihood of result bias due to data partitioning.

2. Impact of AI on Blockchain Transaction Processing

One potential concern when integrating AI-based security mechanisms with blockchain networks is the impact on transaction latency. Table III compares the average transaction processing times before and after deploying the AI-enhanced security model.

TABLE III. Transaction Processing Time Comparison

Scenario	Average Transaction Time (ms)
Without AI Security	215
With AI Security	298
Increase in Latency	+83 ms (≈38.6%)

Potential latency reductions can be achieved through lightweight model architectures, batch-based inference, and off-chain AI processing, where only verified threat intelligence outputs are committed to the blockchain rather than raw transaction data.

The results indicate that while AI-based anomaly detection enhances security, it introduces a slight increase in transaction processing time (approximately 38.6%). This latency increase is due to the computational overhead required for real-time anomaly detection. Although the integration of AI introduces a latency increase of approximately 38.6%, this trade-off is acceptable for security-critical blockchain applications such as financial services, digital identity management, and inter-organizational threat intelligence sharing, where security and trust are prioritized over raw throughput. In contrast, high-throughput applications such as supply-chain tracking or IoT data streaming may require further optimization to balance latency and scalability.

This line chart in Fig. 3 illustrates how AI integration affects blockchain transaction processing time. It compares the average transaction time before and after implementing AI-based security. Fig. 3 shows a consistent increase in transaction processing time after integrating AI-based security, with no extreme spikes observed across transactions. This indicates that while latency increases, the system remains stable and predictable, which is essential for operational blockchain environments.

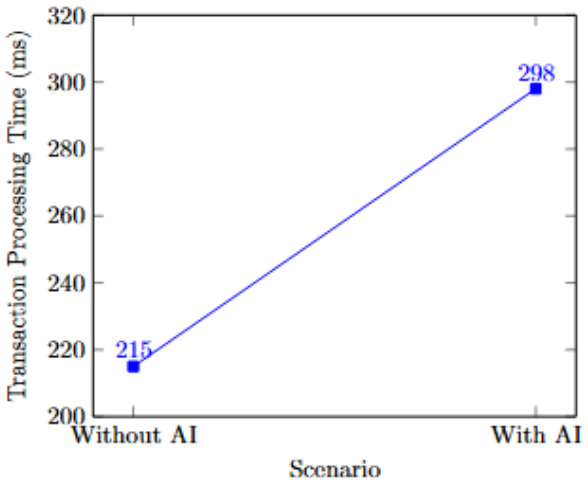

Fig. 3. Impact of AI on blockchain transaction processing time

3. *Effectiveness in Detecting Different Attack Types*

Although phishing attacks are not native blockchain-layer attacks, they were included in the evaluation as part of the external threat intelligence feeds used by the AI model. These attacks were represented through labeled indicators of compromise associated with fraudulent addresses and malicious transaction endpoints, allowing the framework to evaluate cross-domain threat intelligence rather than on-chain behavior alone.

The model was evaluated on its ability to detect different types of blockchain security threats. Table IV presents the detection rates for each attack type.

TABLE IV. DETECTION RATE PER ATTACK TYPE

Attack Type	Detection Rate (%)
Smart Contract Exploit	97.2
51% Attack	95.8
Sybil Attack	93.5
Phishing Attack	94.1
Transaction Flooding	96.0

The model performs exceptionally well in detecting smart contract exploits (97.2%) and 51% attacks (95.8%), which are among the most critical threats in blockchain security. The detection rate for Sybil attacks is slightly lower (93.5%) due to the complex nature of decentralized identity verification.

This bar chart in Fig. 4 visualizes the detection accuracy for different blockchain security threats, showing how well the model detects Smart Contract Exploits, 51% Attacks, Sybil Attacks, Phishing Attacks, and Transaction Flooding. As illustrated in Fig. 4, detection accuracy varies slightly across attack types, with the highest performance observed for smart contract exploits and transaction flooding. The comparatively lower detection rate for Sybil attacks reflects the inherent difficulty of identity-based attacks in decentralized systems, reinforcing the need for complementary identity verification mechanisms.

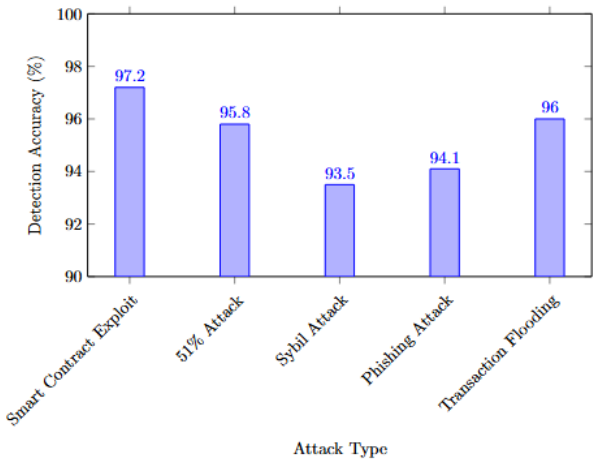

Fig. 4. Detection accuracy for different blockchain attack types

B. *Discussion*

1. *Strengths of the Proposed Model*

- High Detection Accuracy – The model effectively identifies security threats with an overall accuracy of 96.4%, reducing the risk of undetected attacks.
- AI-Powered Anomaly Detection – By leveraging deep learning techniques, the system can detect subtle patterns of fraudulent behavior that traditional rule-based security mechanisms might overlook.
- Low False Positive Rate – At 3.6%, the FPR is within acceptable limits, ensuring minimal disruption to legitimate transactions.

2. *Challenges and Limitations*

- Increased Computational Overhead – The integration of AI leads to an increase in transaction latency, which could affect blockchain performance in high-throughput environments.
- Data Dependency – While the model benefits from diverse data sources, its performance depends on the availability of representative attack samples. To mitigate this limitation, the study incorporated multiple data sources, simulated attacks, and external threat intelligence feeds. However, emerging zero-day attacks not represented in the dataset may still challenge detection performance.
- Adaptability to New Threats – While the model performs well on known attack types, its effectiveness against novel blockchain security threats requires continuous updates and retraining.

Unlike traditional approaches that focus solely on securing blockchain infrastructure, the primary contribution of this work lies in using blockchain to secure AI-generated threat intelligence itself. By ensuring that detected threats are immutable, verifiable, and transparently shared, the framework strengthens collaborative cybersecurity decision-making rather than only protecting the underlying ledger.

C. *Future Improvements*

To enhance the effectiveness and efficiency of the proposed model, future work should focus on:

- Optimizing AI Algorithms – Implementing lightweight deep learning models to reduce computational overhead.
- Incorporating Federated Learning – Federated learning could enable decentralized model training across organizations without sharing raw security data, directly addressing data sensitivity, privacy concerns, and centralized retraining limitations identified in this study.
- Expanding Attack Detection Capabilities – Continuously updating training datasets to include newly emerging blockchain attack patterns.

V. CONCLUSION

This study addressed the growing need for decentralized and intelligent cybersecurity defense mechanisms capable of responding to increasingly sophisticated threats. By integrating deep learning–based threat detection with blockchain-secured threat intelligence sharing, the proposed framework directly responds to limitations identified in existing centralized and single-technology solutions. Experimental evaluation demonstrated that the framework achieves high detection accuracy while maintaining low false positive rates, confirming its effectiveness in identifying multiple categories of blockchain-related cyberattacks.

Beyond performance, the key contribution of this work lies in its novel hybrid architecture, where blockchain is used not merely to secure infrastructure, but to ensure the integrity, transparency, and trustworthiness of AI-generated threat intelligence. This design enhances collaborative security decision-making among distributed stakeholders and supports trustworthy threat intelligence exchange. While the integration introduces additional computational overhead, the results indicate that such trade-offs are justified for security-critical application domains, including decentralized finance (DeFi), digital identity management, enterprise blockchain platforms, and inter-organizational supply chain systems.

To address the identified limitations, future research will focus on optimizing AI model architectures to reduce latency, expanding training datasets to improve resilience against emerging and zero-day attacks, and adopting federated learning approaches to enable decentralized model training without exposing sensitive security data. These directions directly target scalability, privacy, and adaptability challenges highlighted in this study.

Overall, this research demonstrates that securing AI-driven threat intelligence through blockchain technology can significantly strengthen trust, transparency, and robustness in modern cybersecurity systems. As blockchain adoption continues to expand across critical digital infrastructures, the proposed framework provides a strong foundation for next-generation, decentralized, and intelligent cyber defense solutions.

REFERENCES

[1] A. Banafa, *Blockchain Technology and Applications*. River Publishers, 2022, https://doi.org/10.1201/9781003337393.

[2] N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Blockchain and AI for the next generation energy grids: Cybersecurity challenges and opportunities," *Information & Security*, vol. 43, no. 1, pp. 21–33, 2019, https://doi.org/10.11610/isij.4302.

[3] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189–208, 2020, https://doi.org/10.1080/23270012.2020.1731721.

[4] K. J. Smith and G. Dhillon, "Assessing blockchain potential for improving the cybersecurity of financial transactions," *Managerial Finance*, vol. 46, no. 6, pp. 833–848, 2020, https://doi.org/10.1108/MF-06-2019-0314.

[5] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: A scoping review," *Human Behavior and Emerging Technologies*, vol. 2022, no. 1, p. 7384000, 2022, https://doi.org/10.1155/2022/7384000.

[6] R. Prakash, V. S. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022, https://doi.org/10.1016/j.jjimei.2022.100112.

[7] H. Hasanova, U. Baek, M. Shin, K. Cho, and M. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019, https://doi.org/10.1002/nem.2060.

[8] C. Gurdgiev and A. Fleming, "Informational efficiency and cybersecurity: Systemic threats to blockchain applications," in *Innovations in Social Finance: Transitioning Beyond Economic Value*, 2021, pp. 347–372, https://doi.org/10.1007/978-3-030-72535-8_16.

[9] M. M. Rahman, A. Elshamly, S. U. Rehman, Z. Jameel, and R. Hameed, "Blockchain technology and its impact on European banks' cyber security and data integrity," *Journal of Namibian Studies: History Politics Culture*, vol. 34, pp. 1796–1813, 2023, https://doi.org/10.59670/jns.v34i.3449.

[10] S. Yeasmin and A. Baig, "Unblocking the potential of blockchain," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, IEEE, 2019, pp. 1–5, https://doi.org/10.1109/ICECTA48151.2019.8959713.

[11] C. Catalini, "Blockchain technology and cryptocurrencies: Implications for the digital economy, cybersecurity, and government," *Georgetown Journal of International Affairs*, vol. 19, pp. 36–42, 2018, https://doi.org/10.1353/gia.2018.0005.

[12] N. Etemadi, Y. G. Borbon, and F. Strozzi, "Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review," in *Proceedings of the XXIV Summer School "Francesco Turco" – Industrial Systems Engineering*, Bergamo, Italy, 2020, pp. 9–11, https://www.summerschool-aidi.it/images/papers/session_3_2020/ID-38.pdf.

[13] A. N. S. Putro, S. Mokodenseho, N. A. Hunawa, M. Mokoginta, and E. R. M. Marjoni, "Enhancing security and reliability of information systems through blockchain technology: A case study on impacts and potential," *West Science Information System and Technology*, vol. 1, no. 1, pp. 35–43, 2023, https://doi.org/10.58812/wsist.v1i01.166.

[14] A. Alkhalifah, A. Ng, M. J. M. Chowdhury, A. S. M. Kayes, and P. A. Watters, "An empirical analysis of blockchain cybersecurity incidents," in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, IEEE, 2019, pp. 1–8, https://doi.org/10.1109/CSDE48274.2019.9162381.

[15] E. A. Antonyan and O. S. Rybakova, "Blockchain technologies for security against cyber attacks," *Bulletin of the National Academy of Sciences of the Republic of Kazakhstan*, vol. 4, no. 386, pp. 21–26, 2020, https://doi.org/10.32014/2020.2518-1467.99.

[16] I. A. Shah, N. Z. Jhanjhi, and A. Laraib, "Cybersecurity and blockchain usage in contemporary business," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 49–64, https://doi.org/10.4018/978-1-6684-5284-4.ch003.

[17] M. Omar and H. M. Zangana, *Redefining Security With Cyber AI*. IGI Global, 2024, https://doi.org/10.4018/979-8-3693-6517-5.

[18] V. P. Sriram, S. Sanyal, M. M. Laddunuri, M. Subramanian, V. Bose, B. Booshan, C. Shivaram, M. Bettaswamy, S. Booshan, and D. Thangam, "Enhancing cybersecurity through blockchain technology," in *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*, IGI Global, 2023, pp. 208–224, https://doi.org/10.4018/978-1-6684-5284-4.ch011.

[19] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017, https://doi.org/10.1016/j.telpol.2017.09.003.

[20] M. Sadigov, O. Kuzmenko, and H. Yarovenko, "Blockchain technology based system-dynamic simulation modeling of enterprise's cyber security system," in *Proceedings of the 55th International*

Scientific Conference on Economic and Social Development, Baku, Azerbaijan, Jun. 18–19, 2020, pp. 399–408, https://essuir.sumdu.edu.ua/handle/123456789/85701.

[21] A. Tezel, E. Papadonikolaki, I. Yitmen, and M. Bolpagni, "Blockchain opportunities and issues in the built environment: Perspectives on trust, transparency and cybersecurity," in *Industry 4.0 for the Built Environment: Methodologies, Technologies and Skills*, Springer, 2021, pp. 569–588, https://doi.org/10.1007/978-3-030-82430-3_24.

[22] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, and J. Platts, "Cybersecurity, data privacy and blockchain: A review," *SN Computer Science*, vol. 3, no. 2, p. 127, 2022, https://doi.org/10.1007/s42979-022-01020-4.

[23] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, 2016, pp. 463–467, https://doi.org/10.1109/IC3I.2016.7918009.

[24] M. Omar and H. M. Zangana, *Application of Large Language Models (LLMs) for Software Vulnerability Detection*. IGI Global, 2024, https://doi.org/10.4018/979-8-3693-9311-6.

[25] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, IEEE, 2020, pp. 1–9, https://doi.org/10.1109/WF-IoT48130.2020.9221466.

[26] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: Harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 167–172, 2023, https://doi.org/10.34306/ijcitsm.v3i2.120.