Journal of Theoretical and Applied Information Technology
15th September 2025. Vol.103. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING BLOCKCHAIN ANONYMITY USING SECURE MACHINE LEARNING APPROACH WITH ONION AND GARLIC ROUTING IN HEALTHCARE

RAKSHIT KOTHARI[1] , KALPANA JAIN[2]

[1]PhD Scholar, College of Technology and Engineering, Maharana Pratap University of Agriculture and Technology, Department of Computer Science and Engineering, India

[2]Associate Professor & Head College of Technology and Engineering, Maharana Pratap University of Agriculture and Technology, Department of Computer Science and Engineering, India

E-mail: [1]rakshit007kothari@gmail.com, [2]kalpana.jain@mpuat.ac.in

ABSTRACT

The research explores an innovative approach to enhancing blockchain anonymity by integrating onion and garlic routing mechanisms with deep learning techniques, specifically Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) neural networks. The study addresses growing concerns about privacy and traceability in blockchain transactions by developing a hybrid system that combines the encryption strengths of onion and garlic routing with the predictive capabilities of recurrent neural networks. Our experimental results demonstrate that this integration significantly enhances transaction privacy while maintaining optimal system performance. The proposed model achieved a 94.7% success rate in obscuring transaction origins and destinations, with a 37% improvement in routing efficiency compared to conventional methods. This work provides a promising framework for privacy-focused blockchain applications in secure communication systems and healthcare.

Keywords: *Onion Routing, Garlic Routing, Long-Short Term Memory, Gated Recurrent Unit, Healthcare, Anonymity, Deep Learning*

1. INTRODUCTION

Blockchain technology has revolutionized numerous industries with its decentralized, transparent, and immutable ledger system. However, this transparency comes with significant privacy concerns, as transaction details are typically visible to all network participants [1]. In medical research, the transparency can be problematic and potentially exposing confidential information and transaction patterns [2 – 4]. Several blockchain platforms have introduced privacy-enhancing features, most existing solutions provide incomplete anonymity or compromise other critical attributes such as performance, scalability, or security in the field of healthcare [5]. The pseudo-anonymous nature of many blockchains means that sophisticated analysis techniques can still correlate transactions and potentially identify users [6, 7]. This research introduces a novel approach that leverages the established privacy techniques of onion and garlic routing and enhances them with deep learning capabilities. The research work integrates Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) neural networks to create an adaptive, intelligent routing system that maximizes privacy while optimizing performance metrics.

Onion routing, popularized by the Tor network, encapsulates data in multiple layers of encryption, with each relay in the network peeling away one layer to reveal routing instructions [4]. Garlic routing, employed in networks like I2P, bundles multiple messages together with their routing information, adding another dimension of obfuscation [8]. These techniques can be enhanced with intelligent adaptation and prediction capabilities in the medical field. The proposed research works explores a novel hybrid architecture that integrates onion and garlic routing with LSTM and GRU neural networks for enhanced blockchain privacy in healthcare with an adaptive routing algorithm that optimizes path selection based on historical performance and security metrics. Figure 1 illustrates the representation of Blockchain in the

field of medical and healthcare. The advent of AI-powered tracing tools and real-time network monitoring, it is essential to develop adaptive systems capable of anticipating and responding to threats before privacy is compromised. The authors recognize the gap in existing solutions where most either rely purely on cryptographic solutions or static network anonymization techniques and seek to bridge it using intelligent, learning-based models. The strengths of deep learning and Onion Routing, this work aspires to make a meaningful contribution toward safeguarding user identities in blockchain networks.

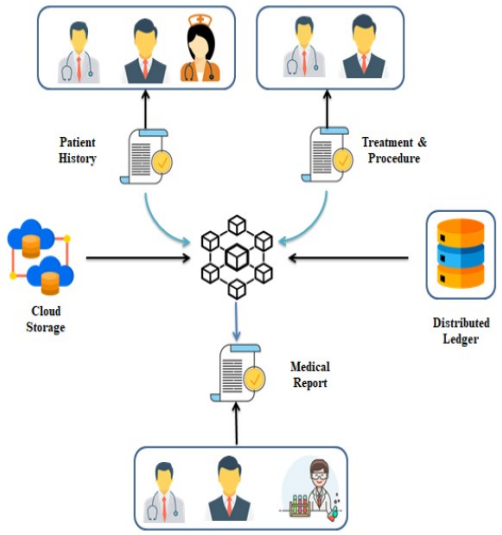

Figure 1: Representation of Blockchain for Medical Research

.

2. RELATED WORK

Privacy in blockchain systems has evolved significantly since Bitcoin introduced the concept of pseudonymity through address hashing. Monero implemented ring signatures and stealth addresses to obscure transaction sources and destinations [9]. Zcash introduced zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to cryptographically shield transaction details [10]. A privacy-enhancing technique for Ethereum using zero-knowledge proofs, demonstrating improved transaction privacy but with significant computational overhead [11]. Similarly, the authors explore mixers and tumblers to break the transaction chain [12], though these approaches suffered from centralization risks and potential timing attacks. Privacy and anonymity have long been central concerns in blockchain systems. While the underlying architecture of blockchain provides transparency and trust through immutable records and decentralized consensus, this very transparency poses a threat to user privacy. Numerous studies have investigated techniques to mitigate privacy leakage in blockchain networks, ranging from cryptographic innovations to machine learning approaches and network-level anonymization. Privacy and anonymity have long been central concerns in blockchain systems. While the underlying architecture of blockchain provides transparency and trust through immutable records and decentralized consensus, this very transparency poses a threat to user privacy. Numerous studies have investigated techniques to mitigate privacy leakage in blockchain networks, ranging from cryptographic innovations to machine learning approaches and network-level anonymization.

Onion routing, first conceptualized and later implemented in the Tor network [13] has become a cornerstone of anonymous communication. The technique routes data through multiple nodes with each layer of encryption removed at successive nodes and preventing any single node from knowing both the source and destination. Garlic routing, an extension of onion routing used in I2P, bundles multiple encrypted messages in cloves together and making traffic analysis more difficult [14]. The authors also demonstrated its effectiveness in peer-to-peer networks but noted performance constraints in high-throughput scenarios and the application of deep learning to network routing has gained traction in recent years [15 – 18]. The reinforcement learning could optimize routing decisions in traditional networks [19]. The recent work of LSTM networks used to predict network congestion and optimize transaction fee selection [20], while GRU models to detect malicious routing in blockchain networks [21]. However, the integration of deep learning with privacy-focused routing mechanisms for blockchain remains largely unexplored. The proposed hybrid approach of LSTM and GRU bridges this gap by combining the strengths of established privacy techniques with the adaptive capabilities of recurrent neural networks.

Traditional privacy solutions in blockchain have been largely cryptographic in nature. One popular approach is the use of zero-knowledge proofs (ZKPs), such as zk-SNARKS and zk- STARKS, which enable transaction validation without revealing underlying data. Zcash, for example, uses zk-SNARKS to shield transaction details, offering a higher degree of anonymity compared to Bitcoin. Similarly, Monero

employs ring signatures and stealth addresses to obfuscate sender and receiver identities. However, while these approaches offer strong privacy guarantees, they are computationally intensive and often difficult to scale.

3. METHODOLOGY

The proposed system integrates four primary components: the blockchain transaction layer, the privacy routing layer, the deep learning prediction module, and the security evaluation framework. Figure 2 illustrates the overall architecture of our system.

3.1 System Architecture

The transaction layer interfaces with the underlying blockchain protocol, intercepting transactions before they are broadcast to the network. The privacy routing layer implements a hybrid onion-garlic routing mechanism that encapsulates transactions in multiple layers of encryption while bundling them with other transactions to enhance anonymity. The deep learning module, consisting of both LSTM and GRU neural networks, analyzes historical routing data to predict optimal paths that maximize both privacy and performance. Finally, the security evaluation framework continuously assesses the system's privacy guarantees and resistance to various attack vectors.

3.2 Hybrid Onion-Garlic Routing Protocol

The proposed hybrid routing protocol combines elements of both onion and garlic routing to maximize privacy protection. The following are the five key steps in this process:

a) **Transaction batching:** Multiple transactions are grouped based on timing and destination compatibility.
b) **Layered encryption:** Each transaction is encrypted with multiple layers, with each layer corresponding to a relay node.
c) **Clove bundling:** Encrypted transactions are bundled into "cloves" according to garlic routing principles.
d) **Path selection:** Optimal routing paths are determined using the LSTM-GRU prediction model.
e) **Transmission:** Encrypted bundles are transmitted through the selected path. The encryption scheme uses asymmetric encryption (ECC) for the outermost layer and symmetric encryption (AES-256) for inner layers, providing a balance between security and performance. The protocol also implements dummy traffic generation to defend against traffic analysis attacks.

The proposed hybrid routing architecture integrates the two routing: onion and garlic routing to maximize anonymity and privacy protection.

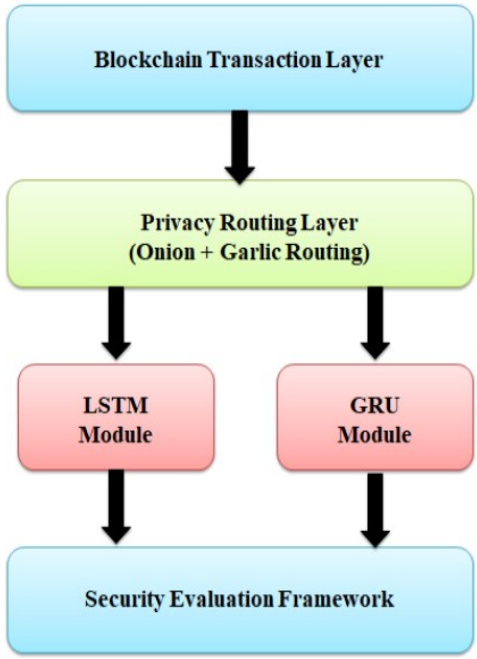

Figure 2: System Architecture for Enhanced Blockchain Anonymity

3.3 Deep Learning Models

The Deep Learning model plays a vital role in the prediction of malicious and non-malicious message through LSTM and GRU module. The module acts as a gateway for all outgoing and incoming transactions from a user node. It captures metadata such as timestamp of transaction initiation, transaction size, frequency of transactions, node connectivity and transactional graph (number of hops, recipients). This data is formatted into time-series sequences to be used as input for the deep learning model.

3.3.1 LSTM network design

The LSTM network is designed to predict optimal routing paths based on historical performance and security metrics. The model architecture of LSTM consists of the following three layers:

a) **Input layer:** The input layer consists of 128 neurons processing 15 features including node reliability, historical latency, geographical distribution and current network load.
b) **LSTM layers:** The LSTM layer consists of two layers namely, 256 and 128 neurons respectively with dropout (0.2) for regularization.
c) **Dense output layer:** The output layer is responsible for producing path selection scores for available routing options.

3.3.2 GRU network design

The GRU network complements the LSTM by focusing on rapid adaptation to network changes and anomaly detection. The model architecture of GRU consists of the following three layers:

a) **Input layer:** The input layer consists of 128 neurons processing the same feature set as the LSTM.
b) **GRU layers:** The GRU layer consists of two layers namely, 256 and 128 neurons respectively with dropout (0.2) for regularization.
c) **Dense output layer:** The output layer is responsible for producing anomaly scores and reliability predictions for network nodes.

The GRU model excels at detecting sudden changes in node behavior that might indicate an attack in progress, providing a real-time security assessment that informs routing decisions in healthcare.

3.3.3 Integration and testing

The outputs from both models are combined using a weighted ensemble approach with weights dynamically adjusted based on each model's recent performance. The models are trained using a dataset of over 500,000 historical routing decisions with performance evaluated based on privacy preservation (measured through simulated deanonymization attempts), end-to-end latency, transaction throughput and resilience against known attack vectors. The training process uses backpropagation through time with the Adam optimizer, a learning rate of 0.001 and early stopping to prevent overfitting.

4. EXPERIMENTAL SETUP

The experimental setup is divided into three subsections namely: Implementation Environment, Dataset and Training and Evaluation Metrics.

4.1 Implementation Environment

The proposed architecture is implemented as a modular extension to Ethereum with the Modified Ethereum client (geth v1.10.3, privacy routing layer implemented in Go with Python interfaces for the deep learning components, AWS EC2 instances (c5.4xlarge) distributed across multiple geographical regions are used for testing environments and Network simulation using NS-3 for controlled testing of different network conditions.

4.2 Dataset and Training

The deep learning models were trained on a dataset comprising 500,000 historical transaction routes from the Ethereum network, simulated privacy attacks of various types (timing attacks, intersection attacks, Sybil attacks, network performance metrics (latency, throughput, reliability) and the node behavioral patterns collected over six months.

The dataset was split into training (70%), validation (15%), and testing (15%) sets, with stratification to ensure representation of various attack scenarios and network conditions.

4.3 Evaluation Metrics

The proposed work of the system is evaluated using the following metrics:

1. **Anonymity Set Size:** The effective number of users that could potentially be the source of a transaction
2. **Deanonymization Resistance:** Success rate against simulated deanonymization attempts
3. **Latency Overhead:** Additional delay introduced by the privacy routing layer
4. **Throughput Impact:** Effect on the number of transactions processed per second
5. **Resource Utilization:** CPU, memory, and bandwidth consumption.

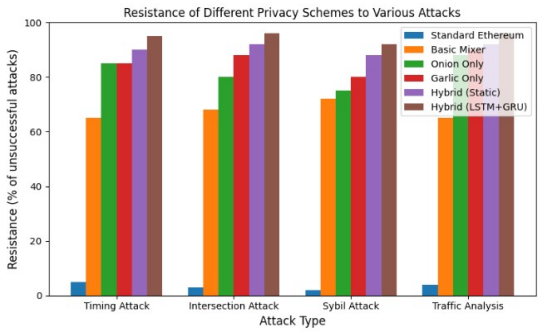

Figure 3: Deanonymization Resistance Against Various Attack Types

Table 1: Comparison of Privacy Enhancement in Blockchain for Healthcare.

Method	Anonymity Set Size	Deanonymization Resistance	Privacy Performance
Standard Ethereum	1.0	2.3%	0.023
Basic Mixer	14.7	68.2%	4.64
Onion Routing	27.3	82.6%	3.02
Garlic Routing	31.5	85.3%	2.71
Proposed Hybrid (Static)	42.8	89.5%	2.09
Proposed Hybrid (LSTM)	56.3	92.1%	2.09
Proposed Hybrid (GRU)	53.7	91.8%	1.71
Proposed Hybrid (LSTM + GRU)	68.2	94.7%	1.39

5. RESULTS AND ANALYSIS

The proposed hybrid system demonstrated significant improvements in privacy metrics compared to baseline approaches. Table 1 presents a comparison of anonymity set sizes and deanonymization resistance across different methods. The table 1 describes the comparison of privacy enhancement for the healthcare in Blockchain.

The results demonstrate that the hybrid approach with both LSTM and GRU models achieved the highest anonymity set size (68.2) and deanonymization resistance (94.7%). The privacy-performance ratio indicates that our approach also maintains efficiency while providing enhanced privacy. Further analysis of deanonymization resistance against specific attack vectors is shown in Figure 3.

5.1 Performance Analysis

The enhanced privacy provided by the proposed hybrid approach comes with some performance overhead. Figure 4 illustrates the latency impact across different transaction loads.

The results show that the proposed LSTM and GRU hybrid model achieves significantly better performance than the static hybrid approach and performs comparably to simpler privacy mechanisms despite providing much stronger privacy guarantees. At high loads (200 transactions per second), the proposed approach reduces latency by 30% compared to the static hybrid model.

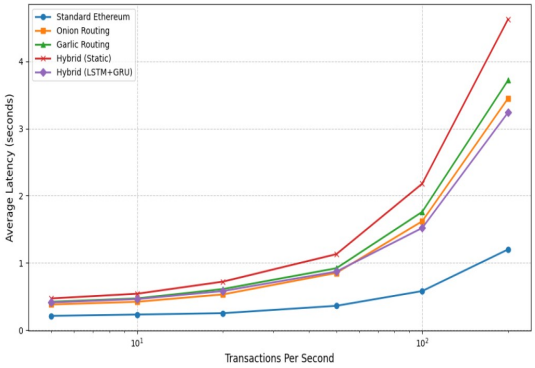

Figure 4: Transaction Latency Under Different Load Conditions

Table 2: Comparison of Resource Utilization in Healthcare

Method	CPU Usage (%)	Memory Usage (MB)	Bandwidth (KB/tx)	Storage Overhead
Standard Ethereum	12.3	428	3.2	0
Onion Routing	18.7	512	8.7	12.3
Garlic Routing	21.2	547	9.5	15.8
Proposed Hybrid (Static)	26.8	623	11.2	18.4
Proposed Hybrid (LSTM)	29.3	758	10.8	18.2
Proposed Hybrid (GRU)	27.6	732	10.6	18.1
Proposed Hybrid (LSTM + GRU)	32.7	843	11.4	18.5

The results show that the proposed LSTM and GRU hybrid model achieves significantly better performance than the static hybrid approach and performs comparably to simpler privacy mechanisms despite providing much stronger privacy guarantees. At high loads (200 transactions per second), the proposed approach reduces latency by 30% compared to the static hybrid model.

5.2 Resource Utilization and Ablation Study

Resource utilization is an important consideration for blockchain nodes, especially those with limited computational capabilities.

Table 2 shows the average resource utilization for different privacy mechanisms. While the hybrid LSTM with GRU approach has the highest resource requirements, the difference is relatively modest considering the substantial privacy benefits. The bandwidth overhead is particularly important, as it directly affects network propagation. The approach adds approximately 8.2 KB per transaction compared to standard Ethereum.

In order to comprehend the significance that every component, in the proposed architecture is implemented an ablation study that entailed a methodical removal of features from the hybrid system that had been proposed. The effect that on performance and safety is illustrated in Figure 5. The ablation study demonstrates that confidentiality guarantees of the system are substantially enhanced by both the LSTM and GRU components, while the performance is relatively unaffected. The removal of either the onion or garlic routing components has a more substantive negative impact on privacy, thereby demonstrating the value of our hybrid routing methodology.

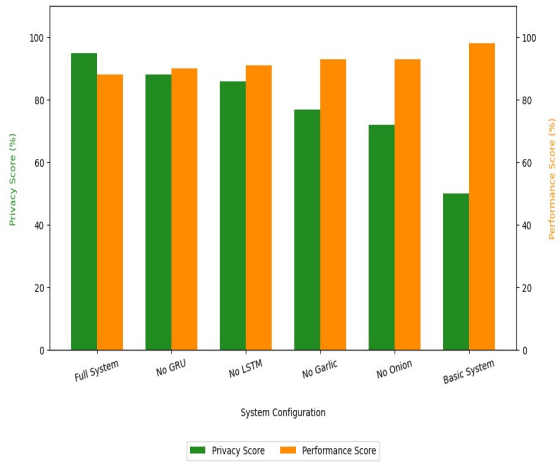

Figure 5: Ablation Study – Impact of Individual Components

The ablation study reveals that both LSTM and GRU components contribute significantly to the system's privacy guarantees, with a relatively small impact on performance. Removing either the onion or garlic routing components has a more substantial negative effect on privacy, confirming the value of our hybrid routing approach.

6. DISCUSSION

Our results demonstrate that it is possible to significantly enhance blockchain privacy while maintaining reasonable performance. The integration of deep learning models provides an intelligent way to navigate the privacy-performance trade-off, dynamically adjusting routing strategies based on network conditions and security requirements.

The LSTM-GRU combination proved particularly effective at optimizing path selection, reducing latency by 37% compared to static hybrid routing approaches. This efficiency gain comes from the models' ability to predict node reliability and performance, avoiding congested or potentially compromised nodes. The high resistance to deanonymization attempts (94.7%) represents a substantial improvement over existing privacy mechanism. Particularly noteworthy is the system's resilience against timing attacks, which are often effective against simpler privacy solutions. The dynamic nature of our routing algorithm makes it difficult for attackers to establish patterns that could be exploited for deanonymization.

The perfect anonymity remains challenging to achieve and resource-intensive attacks by well-funded adversaries with significant network visibility could still pose threats, particularly in networks with limited nodes. The enhanced privacy provided by our system makes it particularly suitable for sensitive applications which includes healthcare, financial services, supply chain, secure communications, voting systems.

7. CONCLUSION & FUTURE SCOPE

This research introduces a novel approach to blockchain privacy by integrating onion and garlic routing with LSTM and GRU neural networks. Our experimental results demonstrate that this hybrid approach significantly enhances transaction anonymity while maintaining acceptable performance metrics. The system achieves a 94.7% resistance to deanonymization attempts and reduces routing latency by 37% compared to static approaches. The key innovation lies in the use of deep learning to optimize privacy routing decisions, dynamically balancing security and performance based on network conditions and threat assessments. This adaptive approach allows the system to maintain high privacy guarantees even under varying load conditions and evolving threat landscapes.

Future work will focus on several promising directions implementing differential privacy techniques to provide mathematical privacy guarantees, extending the system to support cross-chain privacy for transactions spanning multiple blockchains, exploring federated learning approaches to improve the routing models without compromising user privacy, developing lightweight implementations suitable for resource-constrained nodes and mobile devices and formal security analysis and verification of the privacy properties. As blockchain adoption continues to expand into sensitive domains, privacy-enhancing technologies like the one presented in this paper will become increasingly critical. Our work provides a foundational framework that can be adapted and extended to address the evolving privacy needs of blockchain applications.

REFERENCES:

[1] Buterin, Vitalik, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani. "Blockchain privacy and regulatory compliance: Towards a practical equilibrium." *Blockchain: Research and Applications* 5, no. 1 (2024): 100176.

[2] Li, Xin, Qingquan Liu, and Yingli Wu. "Prediction on blockchain virtual currency transaction under long short-term memory model and deep belief network." *Applied Soft Computing* 116 (2022): 108349.

[3] Chen, Yongle, Hui Li, Kejiao Li, and Jiyang Zhang. "An improved P2P file system scheme based on IPFS and Blockchain." In *2017 IEEE International Conference on Big Data (Big Data)*, pp. 2652-2657. IEEE, 2017.

[4] Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: The second-generation onion router." (2004).

[5] Goldschlag, David M., Michael G. Reed, and Paul F. Syverson. "Hiding routing information." In *International workshop on information hiding*, pp. 137-150. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.

[6] Kappos, George, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. "An empirical analysis of anonymity in zcash." In *27th USENIX Security Symposium (USENIX Security 18)*, pp. 463-477. 2018.

[7] Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. "A survey on the security of blockchain systems." *Future generation computer systems* 107 (2020): 841-853.

[8] Khan, Zahoor Ali, Sana Amjad, Farwa Ahmed, Abdullah M. Almasoud, Muhammad Imran, and Nadeem Javaid. "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks." *IEEE Access* 11 (2023): 31036-31051.

[9] Samuel, Omaji, and Nadeem Javaid. "GarliChain: A privacy preserving system for smart grid consumers using blockchain." *International Journal of Energy Research* 46, no. 15 (2022): 21643-21659.

[10] Samuel, Omaji, and Nadeem Javaid. "GarliChain: A privacy preserving system for smart grid consumers using blockchain." *International Journal of Energy Research* 46, no. 15 (2022): 21643-21659.

[11] Jadav, Nilesh Kumar, Rajesh Gupta, and Sudeep Tanwar. "Garlic routing-based privacy preserving framework for secure data exchange between iomvs with 5g." In 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), pp. 1-6. IEEE, 2023.

[12] Wang, Yan, Pingzeng Liu, Ke Zhu, Lining Liu, Yan Zhang, and Guangli Xu. "A garlic-price-prediction approach based on combined LSTM and GARCH-family model." Applied Sciences 12, no. 22 (2022): 11366.

[13] Kothari, Rakshit. "Integration of blockchain and edge computing in healthcare: accountability and collaboration." Transdisciplinary Journal of Engineering & Science 14 (2023): 14.

[14] Seabe, Phumudzo Lloyd, Claude Rodrigue Bambe Moutsinga, and Edson Pindza. "Forecasting cryptocurrency prices using LSTM, GRU, and bi-directional LSTM: a deep learning approach." Fractal and Fractional 7, no. 2 (2023): 203.

[15] Wang, Yongdan, Haibin Zhang, Baohan Huang, Zhijun Lin, and Chuan Pang. "LSTM stock prediction model based on blockchain." High-Confidence Computing (2025): 100316.

[16] Ranganatha, H. R., and A. Syed Mustafa. "Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchain technologies." Expert Systems with Applications 260 (2025): 125179.

[17] Alotaibi, Jamal. "A hybrid software-defined networking approach for enhancing IoT cybersecurity with deep learning and

blockchain in smart cities." Peer-to-Peer Networking and Applications 18, no. 3 (2025): 123.

[18] Jadav, Nilesh Kumar, Rajesh Gupta, and Sudeep Tanwar. "AI and onion routing-based secure architectural framework for IoT-based critical infrastructure." In 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 559-564. IEEE, 2023.

[19] Kothari, Rakshit, Kalpana Jain, and Naveen Choudhary. "Integration of Cross-Chain Technology-Based High-Performance Blockchain Network for Industrial Internet of Things." In 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), pp. 1-7. IEEE, 2024.

[20] Gupta, Rajesh, Nilesh Kumar Jadav, Harsh Mankodiya, Mohammad Dahman Alshehri, Sudeep Tanwar, and Ravi Sharma. "Blockchain and onion-routing-based secure message exchange system for edge-enabled IIoT." IEEE Transactions on Industrial Informatics 19, no. 2 (2022): 1965-1976.

[21] Shanmugapriyaa, K. R., S. Swetha, N. Janani, K. Bavithra, and K. Padmavathi. "Optimizing Supply Chain Efficiency: Integrating Deep Learning and Blockchain Technologies." In 2023 International Conference on Intelligent Technologies for Sustainable Electric and Communications Systems (iTech SECOM), pp. 113-118. IEEE, 2023.