Acta Informatica Pragensia
2025, Volume 14, Issue 3, 316–339
https://doi.org/10.18267/j.aip.260

PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

Article Open Access

EBSSPA: Efficient Deep Learning Model for Enhancing Blockchain Scalability and Security Through Fusion Pattern Analysis

Anuradha Hiwase [1], **Amit Pimpalkar** [2,3], **Barkha Dange** [3], **Nitin Thakre** [4], **Sakshi Jaiswal** [5], **Tejaswini Mankar** [6]

[1] Department of Computer Science and Engineering, Yashwantrao Chavan College of Engineering, Nagpur, Maharashtra, India
[2] Department of Computer Science and Engineering, Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India
[3] School of Computer Science and Engineering, Ramdeobaba University, Nagpur, Maharashtra, India
[4] Department of Computer Science and Engineering, Govindrao Wanjari College of Engineering and Technology, Nagpur, Maharashtra, India
[5] Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur, Maharashtra, India
[6] Department of Computer Science and Engineering, KDK College of Engineering, Nagpur, Maharashtra, India

Corresponding author: Amit Pimpalkar (pimpalkarap@rknec.edu)

Editorial Record

First submission received:
August 15, 2024

Revisions received:
October 13, 2024
December 3, 2024
January 13, 2025

Accepted for publication:
January 31, 2025

Academic Editor:
Zdenek Smutny
Prague University of Economics and Business, Czech Republic

This article was accepted for publication by the Academic Editor upon evaluation of the reviewers' comments.

How to cite this article:
Hiwase, A., Pimpalkar, A., Dange, B., Thakre, N., Jaiswal, S., & Mankar, T. (2025). EBSSPA: Efficient Deep Learning Model for Enhancing Blockchain Scalability and Security through Fusion Pattern Analysis. *Acta Informatica Pragensia*, 14(3), 316–339. https://doi.org/10.18267/j.aip.260

Abstract

Background: Blockchain technologies have come a long way, and integration of blockchain technologies into different fields is flourishing; however, there is a lack of blockchain platforms to manage the high network loads and more sophisticated security threats. These limitations impede the mass adoption of blockchain applications. One of the main reasons blockchain needs artificial intelligence (AI) is to integrate it for the widespread adoption of blockchain technology, as AI addresses scalability and security problems.

Objective: The article proposes a pattern analysis model to overcome scalability and security limitations in blockchain systems by applying advanced AI techniques.

Methods: To make the model scalable, the proposed model uses deep learning methods such as recurrent neural networks (RNNs) and long short-term memory (LSTM) networks. Furthermore, random forest and convolutional neural networks (CNNs) are applied to augment security operations as an effective classier and anomaly detector on transaction data and a real-time threat detection on transaction patterns using the CNNs. By analysing time series data and dealing with long-term dependencies, the model uses RNNs and LSTMs to enable the strategic introduction of the model to predict and control network loads.

Results: When the proposed model is tested against a curated cloud dataset, it significantly outperforms the state-of-the-art approach in all the performance parameters. More specifically, it has exhibited a 5.05% increase in processing speed, 8.05% improvement in energy efficiency, and 5.27%, 5.8%, 10.24% and 11.62% better attack analysis precision, accuracy, recall and AUC, respectively.

Conclusion: The synergistic interaction of the applied AI techniques results in a blockchain paradigm that is both scalable and resilient to new security threats. This significant improvement in performance parameters demonstrates the effectiveness of integrating AI with blockchain technology to overcome scalability and security limitations, thereby enabling the widespread adoption of blockchain applications.

Index Terms

Artificial intelligence; Blockchain technology; Scalability; Machine learning; Network congestion; Network load prediction; Real-time threat detection.

1 INTRODUCTION

AI on the blockchain is a giant step towards solving critical challenges facing the game-changing digital ledger system. Blockchain developers have always faced the challenge of scalability as they strive to create a decentralised and secure platform for storing data and running transactions. The need to support ever-growing applications apart from cryptocurrencies in finance, health and supply chain management domains has put the scalability and security of the blockchain platform in the limelight (Alsamhi et al., 2024). Though this excellent technology has promising potential, it lags behind some constraints. Most importantly, there is the scalability issue, where an increase in the number of users and transactions in the network leads to traffic congestion and slows the transaction speed. Such a scalability bottleneck affects user experience and inhibits a more general use of blockchain technology.

Moreover, there are security concerns, given that blockchain networks are increasing in complexity and value, making them more lucrative for cyberattacks, even from advanced sources, and calling for corresponding means of monitoring and responding to such threats. However promising, utilising AI in the blockchain space offers two exciting ways to solve the stated issues. AI algorithms, which can read through vast volumes of data to point out any patterns, are at the centre of interest in enhancing the scalability and safety of blockchain networks. By applying AI-based prescriptive analytics, we can proactively optimise transaction processing and resource management to deliver scalability in various use cases and manage network load effectively. At the same time, AI-based security systems offer a dynamic solution to detect and respond to potential threats through real-time identification and mitigation, thus enhancing the overall resilience of the infrastructure process (Olumide, 2018).

Incorporated approach to AI with blockchain technology allows us to maximise its scalability and security. With RNNs and LSTM networks, the model successfully predicts, and controls network loads and operates under varying conditions to maximise it. Random forest and CNNs add to the security framework, showing that random forest is best suited for anomaly detection in blockchain transactions, whereas CNNs are good at pattern recognition that may hint at potential threats. A comprehensive evaluation of synthetic datasets provides evidence of the superiority of our model compared to previous methods in terms of speed, energy efficiency, threat detection, and response accuracy. With this AI technology converging in blockchain, these AI technologies solve current scalability and security problems, and this will be a transformational paradigm in blockchain development. This presents an innovative approach to a more robust, efficient, and secure blockchain system with direct implications for different industries and social sectors. At last, this work poses new standards in the blockchain domain, playing a part in enabling future improvements that can alter how technology is adopted and utilised.

1.1 Motivation

The motivation behind the study is to address the gap created by the intrinsic limits of blockchain technology or, to be more specific, scalability and security. As blockchain applications proliferate in different industrial segments, the challenges become critical, and hence, innovation for technology sustainability is needed in the long term. In this study, combining AI with blockchain seems rather inventive when creating innovations in blockchain network performance and resilience (Bathula et al., 2024). Such a single challenge remains one of the main drivers behind the present scalability study. This increase in the volume of transactions in blockchain networks causes network congestion, which reduces the speed of transaction processing and the cost of processed transactions and, therefore, negatively influences the network's efficiency and attractiveness of blockchain technology to its users. While larger block sizes or higher frequencies can give some relief, they offer only partial relief as they tend to harm other properties like lowering security or increasing centralisation. For this reason, considering an AI model that would predictively manage network load so that it remains sustained and effective on the blockchain becomes a vital task.

Additionally, blockchain security has another looming crisis: the increasing complexity of cyberthreats. Although blockchain is decentralised and has cryptographic principles, attackers can attack the security of blockchain, which is well planned and executed because of the advanced persistent threats, leaving attack in their wake (Li et al., 2024). In this research, AI algorithms are used for real-time threat detection and response enabled by the blockchain with dynamic, proactive security that can detect and handle different threats in real-time in multiple applications.

1.2 Primary tasks of key contributions

Task 1: Predicting and managing network load to enhance scalability

Task 2: Detecting and responding to security threats to improve overall system security

The first significant contribution is developing a blockchain model that uses AI to enhance scalability. The model employs RNNs and LSTM networks, which excel in time series analysis and detecting temporal patterns in transaction data. By accurately predicting and managing network load, this model can forecast potential congestion and make timely adjustments to optimise overall network performance.

Second, this contribution consists of constructing a robust security framework by integrating random forests and CNNs. Such a dual approach can detect anomalies and malicious activities in transaction data and transaction graphs, respectively. The techniques are integrated into the model, thereby significantly increasing the security functionalities of blockchain systems against cyber threats.

Thirdly, we empirically validate the model's effectiveness through extensive testing on a well-selected dataset for various real-world blockchain transaction types and sizes. This shows significant improvements in processing speed, energy efficiency, and precision and accuracy of attack analysis compared to existing methods.

This paper studies the potential of synergising AI and blockchain technology to create additional research paths for the future. It details how the world currently faces these problems and how AI addresses them and opens new capabilities around it for different uses in industries.

This paper will be structured to give an overall view of how blockchain scalability and security can be improved by the fusion pattern analysis (EBSSPA) model and its contribution to blockchain technology. Firstly, the paper introduces the problems encountered in blockchain systems and explains why scalability and security solutions are required. The proposed methodology is developing the EBSSPA model with integrated AI techniques and deep learning methods. The experimental studies and performance evaluation of the EBSSPA model are demonstrated in the results section, demonstrating its effectiveness in blockchain scalability and security improvement. The conclusion concludes with the essential findings and contributions of the paper, showing how the EBSSPA model could be applied in the real world.

2 LITERATURE REVIEW

It reviews the various accomplishments and technologies used to create better efficiency and security in blockchain by merging them with AI. This literature discusses several studies that lay the background to the proposed model to set up the state of research and identify the gap that needs to be filled for different scenarios. Jie et al. (2024) have discussed the development of a secure and flexible blockchain-based offline payment scheme that extends the application of blockchain techniques in the financial sector more than the conventional use of blockchain in the financial system. This piece underscored the importance of an intense security process, a theme that fits within current research on converting blockchain security using AI. Concerning the previous research, Jiaxing et al. (2024) studied blockchain-based auditing for big data in cloud storage. This scheme was based on blockchain for ensuring data integrity and security. They minimised system overheads while keeping good protection against malicious attacks using a deep reinforcement learning model. It improved transaction processing while lowering the network latency compared to the previous procedure. In Zhang et al. (2024), dynamic trust-based redactable blockchains were explored, and they provided some insights into the freedom of blockchains to update the data and its traceability of such data. Current research is a foundation of a flexible but secure and trusted blockchain, where AI effectively manages network loads and security responses.

Tandon et al. (2024) state that two blockchains can form a decentralised architecture to authenticate vehicles. Authentication and communication functions have been separated to make it efficient and secure. Our evaluations demonstrated an order of magnitude decrease in the computational cost, on average faster processing and a higher vehicle verification rate compared with existing methods. Dai et al. (2024) utilised declaration informing the balance of data immutability vs data redaction in blockchain systems through a redactable blockchain framework that uses a public trapdoor mechanism. The design of the present research's AI-enhanced model heavily depends on this balance, which retains the integrity of blockchain and improves scalability and security. In their work, Puneeth et al. (2024) and Bukola et al. (2024) developed an integrated blockchain and deep learning system for medical cyber-

physical systems that support both safe and secure data operations. Based on medical data analysis, the system reached an astounding 96% accuracy, and this vastly enhanced security provided a new vision for medical cyber-physical systems and security. For example, Kuznetsov et al. (2024) discussed the applicability of incorporating AI and blockchain from a security perspective, and this is an area that is closely similar to the proposed AI-driven blockchain model. Meanwhile, other studies like Zhang et al. (2024) and Qin et al. (2024) have shown other means of improving blockchain applications using dual blockchain assisted authentication framework and tri blockchain based information sharing, respectively. The study by Xu et al. (2024), the integration between traditional data security and blockchain technology was studied. They found limitations with scalability as user activities increased, bottlenecks brought about by the encryption and even possible security vulnerabilities. They devised a balanced approach to achieve practicality, efficiency, and robust security in their presence.

Echikr et al. (2024), Chen et al. (2023), and Bagchi et al. (2023) have conducted significant studies to show which blockchain applications can be directed in the copyright protection and internet of things (IoT) security issues. In turn, the present research investigates various applications where the AI incorporated approach is necessary and shows different applications that would benefit. Studies developed by Samuel et al. (2023) and Peng et al. (2023) recognise blockchain's role in IoMT systems and dual blockchain in IoMT systems for secure medical records sharing. This shows the growing need for more robust and scaled blockchain solutions in sensitive sectors and the need for present work to improve the chance of blockchain scalability and security using AI. Feng et al. (2023) and Zukaib et al. (2023) have investigated how to merge the best of the blockchain and machine learning with these new cryptographic technologies. More specifically, Feng et al. (2023) talk about the utilisation of multi-party signatures, and Zukaib et al. (2023) discuss systematically blockchain and machine learning in security electronic health records (EHR). This research continues this dialogue process centred on integrating complex technology with blockchain. Saraswat et al. (2024) designed a hybrid machine learning methodology based on logistic regression and random forest algorithms to address effective EHR management within a blockchain cloud combined system. Other algorithms were evaluated against the proposed model and achieved a high accuracy rate of 98.37%. Moreover, the latency and throughput of the blockchain-cloud integrated decentralised storage were superior to other storage methods when handling increased patient count.

Literature on integrating blockchain and AI has served to understand how blockchain systems can be developed to be secure and scalable. For example, Haritha & Anitha (2023) designed a multi-level security framework in a healthcare system, where the layered security mechanism was the central part of the proposed AI-integrated security model. Another study further emphasised Bendiab et al. (2023) on the security of autonomous vehicles using blockchain and AI underscored the potential of AI to boost blockchain security and, most likely, on the state-of-the-art blockchain security solutions. Given this, the results from this work are particularly relevant to this study, as integration of AI into blockchain can lead to better security. Xie et al. (2023) provide a secure multi-UAV task management scheme for the sat chain that illustrates the application of blockchain in completing the complex tasks, and it can greatly aid us in building a versatile and secure blockchain system. Wang et al. (2023) have introduced a protocol for permissioned blockchain that allows safe and private data sharing. Their work resonates with the conventional worries about the security of blockchain applications and stresses that privacy as the focus of security in blockchain networks is an issue that needs to be resolved. Liu et al. (2023) conducted a study on the capability of blockchain technology for sharing remote healthcare data to foster conditional anonymity and emphasise the capability of blockchain technology. More precisely, there is a fear about the security and privacy of health data.

Cai et al. (2023) have developed GTxChain, a secure IoT smart blockchain architecture using the graph neural network technique to integrate the AI into blockchain and the capability of blockchain to be developed in a better architecture to aid blockchain architectures in IoT applications. In a work that Alsamhi et al. (2023) did, they proposed blockchain-empowered security and energy efficiency in drone swarm consensus for environmental exploration. Blockchain was pinpointed as relevant to energy-efficient and secure consensus mechanisms for which the present study, focusing on efficient and secure systems, has an important consideration. In the healthcare data management systems that rely on data integrity and protection, Costta et al. (2023) showed the need for secure and scalable blockchain solutions in their introduced blockchain-based protocol, Sec-Health. Das et al. (2023) introduced an innovative blockchain-supported vehicle-to-vehicle communication system which uses blockchain-based contracts to bring valuable insights into the usage of blockchain technology for secure communication in intelligent transportation systems. This work uses blockchain for secure and efficient network systems, which is particularly relevant to the present study. Zhou et al. (2024) introduced a blockchain-enabled secure and efficient outsource secret

image sharing for wireless network computation. The research also pointed to the versatility of blockchain technology and its applications — particularly in secure data sharing, which is the main idea upon which the current work rests. Based on the lack of a comprehensive security framework for Blockchain in IoT networks, Rani et al. (2023) developed a blockchain security framework for running IoT-based Software-defined networks to provide a broader accountability of how blockchain enables network security, especially in the IoT ecosystem. Duan et al. (2023) conducted a comprehensive survey on attacks against cross-chain systems and their defence mechanism. For developing the AI-integrated security model that is presented in this study, it is essential for their analysis of the blockchain system vulnerabilities and strengths.

Similarly, Rao et al. (2023) presented a detailed study of blockchain integration for IoT-based vehicles regarding communication with security dimensions and problems. The research presented in the present paper was intended to address their work around secure and scalable blockchain solutions for complex communication networks and highlighted their emphasis on secure and scalable blockchain solutions for such networks. Vidal et al. (2022) deepen and discuss revocation mechanisms that increase the technical feasibility of some applications requiring corrective operations. First, the researchers raised the effectiveness of sovereign identity for student and university identity management through a proposed model that could be replicated in different systems and domains and across organisations. In this case, the conceptual framework was developed to integrate blockchain applications in Iran Police police task forces by Arabsorkhi & Ebrahimi (2022).

In analysing essential derivatives for blockchain adaptation at task force levels, the researchers adapted ESRC values and ranked them on a hierarchy from 'absolutely not worth using' to 'must be used' for blockchain adaptation. In an attempt to determine and select the blockchain applications, these were prioritised using the fuzzy Delphi method. This was evaluated by 14 expert panellists (high agreement) among members. The reliability of the statistics was also tested with a Cohen's kappa coefficient of 0.64. Ali et al. (2022), the authors proposed a blockchain framework for secure and scalable healthcare systems that rely on hybrid deep learning. Their framework ensures that medical data is only accessible to those who can, and it simplifies the task of analysing medical data in real time. Despite this, the integration provides better scalability, security and interoperability, while challenges such as computational complexity and regulatory compliance should be considered.

Table 1. *Summary of key findings from previous literature on blockchain systems.*

Scalability challenges	Merit	Demerit	Process/method	Parameter
Big data management	High scalability	High data processing time	Distributed data processing	Data volume
Big data cleansing	High data quality	High data processing time	Data preprocessing	Data accuracy
Big data collection	High data collection rate	High data storage requirements	Data collection protocols	Data freshness
Imbalanced big data	High accuracy	High computational complexity	Data balancing techniques	Data imbalance
Big data analytics	High data insights	High data processing time	Data analytics algorithms	Data insights
Big data machine learning	High accuracy	High computational complexity	Machine learning algorithms	Data accuracy
Scalability in big data	High scalability	High data processing time	Distributed data processing	Data volume
Efficiency in big data	High efficiency	High data processing time	Data preprocessing	Data accuracy
Precision in big data	High precision	High computational complexity	Data analytics algorithms	Data insights
Privacy in big data	High privacy	High data processing time	Data encryption	Data security

The main findings from the existing literature (including the scalability challenge, merits, demerits, method, and various parameters of the blockchain systems) are summarised in Table 1. According to the existing big data

management and analytics work, many limitations exist. The scalability and the ability to process significant data results in high data processing times and high computational complexities of this system. Data preprocessing and balancing techniques are also essential but time-consuming. It is also important to mention that data encryption and security measures are highly demanded but may affect data processing efficiency. The limitations in these proposals point to the need for faster and more scalable solutions that provide speeds in data processing, accuracy and security. This work advances the existing knowledge in the field of AI-enhanced blockchain technology and ultimately leads to the development of secure and scalable blockchain systems capable of satisfying the requirements of today's application. This research is focused on the areas with the most significant focus on security and scalability innovation, and these studies give a broader context in which the evolution of blockchain technology took place. This has established a consensus that researchers need more secure and scalable blockchain applications, which are getting more adopted across different domains. This thesis builds upon the efforts made in the past that have perceived the significance of secure and flexible blockchains, the equilibrium of the data immutability and unmasking, as well as AI as a possible supplement that can raise the scalability and security of the blockchain. The present study consolidates these findings and proposes an AI-integrated blockchain model to address the critical security and scalability challenges, aiming to set a new benchmark for developing highly robust, efficient and secure blockchain systems.

3 METHODOLOGY AND PROPOSED MODEL ARCHITECTURE

We have observed that current methods for increasing the efficiency of blockchain deployments are either overly complex or inefficient when applied to real-time network scenarios, as discussed in the previous section.

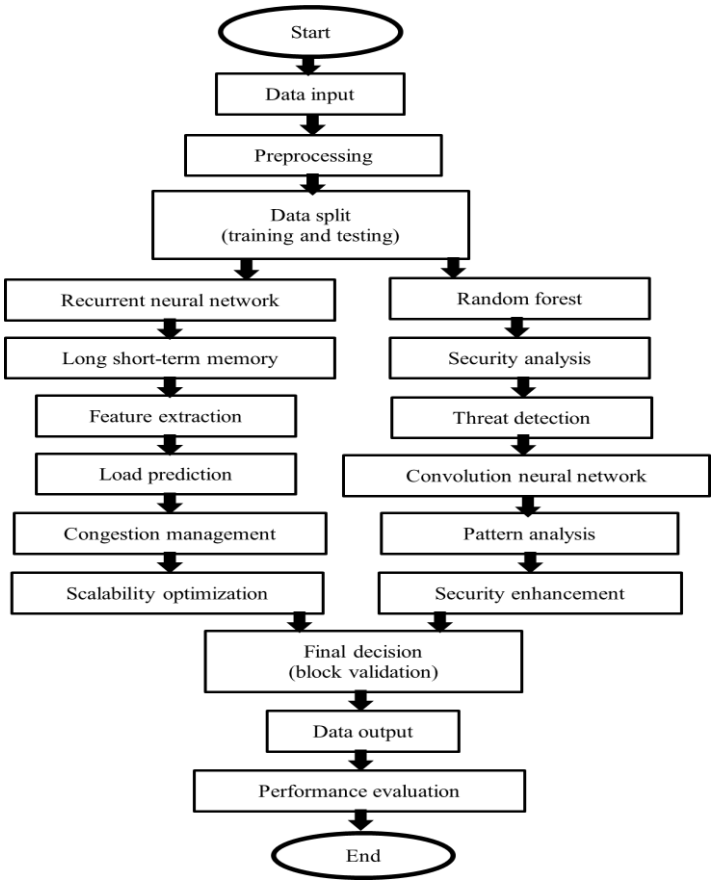


Figure 1. *Model architecture for proposed blockchain scalability and security operations.*

To mitigate these problems, this section addresses the design of an efficient model to enhance the scalability and security of blockchain through the fusion of pattern analysis operations. In the architecture of the proposed blockchain model, described in Figure 1, each component, that is, RNNs, LSTMs, deep forests and CNNs, plays an important, pivotal role in the overall effectiveness of the model. RNNs, designed to handle a data stream, are essential when analysing the temporal dynamics of blockchain transactions. We enable the model to acquire patterns

over time by deploying LSTMs, a more advanced version of RNNs, due to their ability to handle long-term dependency. The efficiency pathway, inspired by RNNs and LSTMs, focuses on scalability and network load management, whereas the security pathway, exploiting random forest and CNNs, focuses on anomaly detection and threat mitigation. Ensuring consistency and continuity of transaction data over a long period is highly relevant. Such reliability is beneficial in blockchain transactions, where sequential and interdependent transactions demand precise timing and coordination. Deep forests, because of their ensemble approach, bring high robustness to the model, particularly in classifying and detecting anomalies from the samples of transaction data samples.

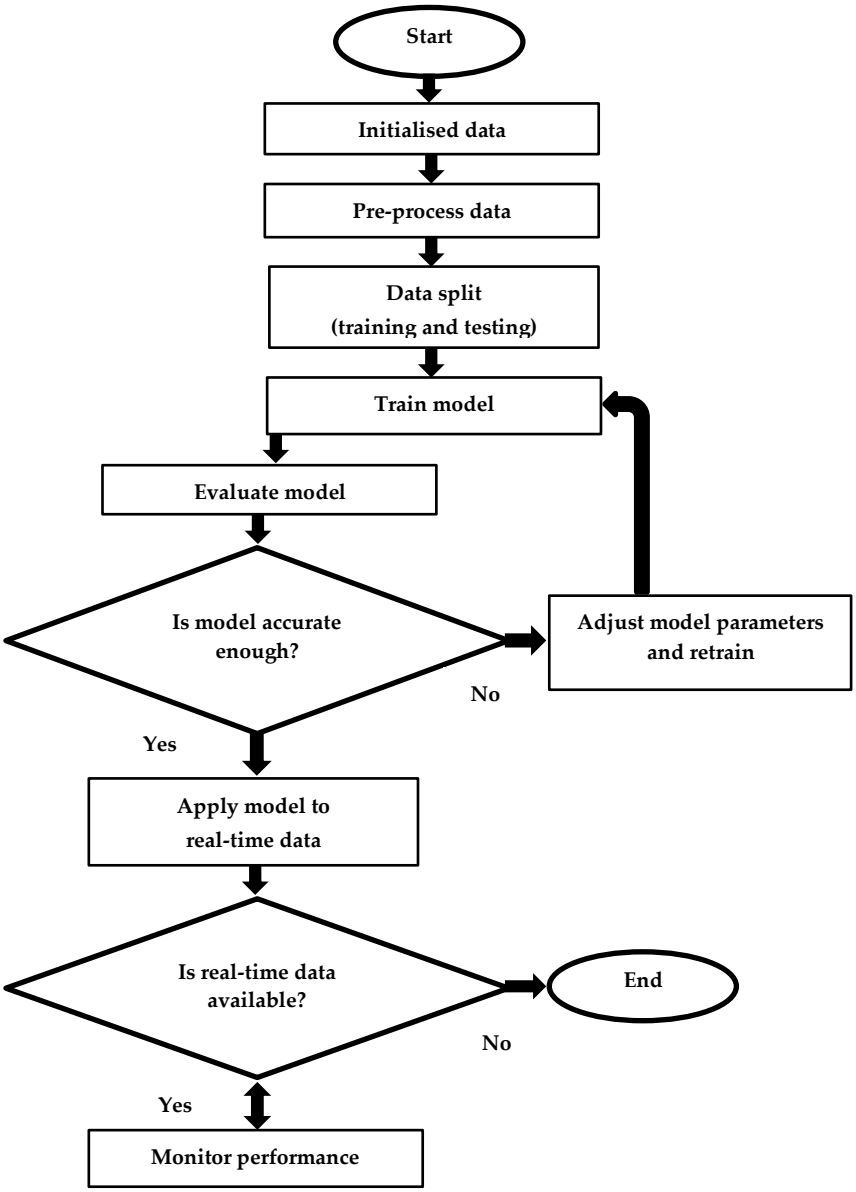


Figure 2. *The overall flow of the proposed scalability enhancement process.*

Using multiple decision trees provides refined data understanding, paramount in recognising anomalies that are vital indicators of security threats. By analysing the intricate patterns within transaction graphs, CNNs facilitate the detection of complex security threats, providing granular analysis vital for real-time threat detection and response sets. Altogether, these components make a complete system that pioneers scalability and security and sets a new development in blockchain technology that can withstand the complexities and demands of modern blockchain networks. Figure 2 illustrates the use of RNNs and LSTM networks to predict and manage network load, enhancing blockchain scalability. We collect network samples as input to achieve a comprehensive dataset that captures the temporal patterns in blockchain transactions. The strategic application of these neural network techniques enables effective forecasting and control of network congestion, significantly improving the scalability of blockchain systems. The design of the RNN-based LSTM process starts with formulating an RNN structure that is good at

handling sequential data samples. RNN encapsulates its functionality through a series of operations. Let *xt* represent the input at the timestamp *t*, and the hidden state *ht* is computed via Equation (1),

$$ht = \sigma(Whx * xt + Whh * ht_{-1} + bh) \quad (1)$$

where *Whx* and *Whh* are weight matrices, *bh* is the bias term and σ represents the tanh activation function process. The output *yt* of the RNN at the time *t* is then given by Equation (2),

$$yt = Wyh * ht + by \quad (2)$$

where *Wyh* and *by* are the output weight matrix and bias. To address the shortcomings of traditional RNNs, particularly the challenges associated with long-term dependencies, we have integrated LSTM units into this process. This strategic integration enables the model to effectively handle long-term dependencies and overcome the limitations of traditional RNNs. The LSTM modifies the RNN framework by introducing a memory cell *ct* and three gates: the input gate *it*, the forget gate *ft* and the output gate *ot*, represented as Equations (3), (4), (5), (6) and (7) as follows,

$$it = \sigma(Wxi * xt + Whi * ht_{-1} + Wci * ct_{-1} + bi) \quad (3)$$

$$ft = \sigma(Wxf * xt + Whf * ht_{-1} + Wcf * ct_{-1} + bf) \quad (4)$$

$$ct = ft \circ ct_{-1} + it \circ tanh(Wxc * xt + Whc * ht_{-1} + bc) \quad (5)$$

$$ot = \sigma(Wxo * xt + Who * ht_{-1} + Wco * ct + bo) \quad (6)$$

$$ht = ot \circ tanh(ct) \quad (7)$$

Here, $\circ$ represents the Hadamard product, and *W* with various subscripts represents the weight matrices for different gates and cell states. We represent the biased terms using the symbol *b* with appropriate subscripts. The ability of the LSTM to regulate the flow of information through these gates enables it to effectively preserve relevant information over long sequences, thereby mitigating the vanishing gradient issue that causes inefficiency in traditional RNNs. This capability is crucial in predicting network load in the blockchain environment, where transactions are sequential and interdependent over extended timestamp sets. We use the output from the LSTM layer to manage the scalability of blockchain networks that reflect the predicted network load. This controlling is articulated as Equation (8), which we have developed to optimise network performance.

$$St = \alpha * Lt + \beta * Tt \quad (8)$$

Here, *St* represents the scalability level at the timestamp *t*, *Lt* is the load predicted by the LSTM, *Tt* is the transaction processing capacity at the timestamp *t*, α and β are scaling coefficients adjusted based on network requirements. Furthermore, a feedback loop is incorporated to optimise the network performance, defined by Equation (9),

$$Ft = \gamma(Dt - St) \quad (9)$$

where *Ft* represents the feedback signal, *Dt* is the desired scalability level and γ is a correction factor for different network scenarios. This feedback ensures that the system adjusts dynamically to achieve the desired scalability, effectively responding to varying network conditions. This RNN-based LSTM process, with its intricate array of operations and mechanisms, stands as a testament to the sophistication of our model in enhancing blockchain scalability levels. Through this process, the model predicts network load with high accuracy and dynamically manages the scalability of the blockchain, ensuring optimal performance even under varying network conditions. This approach marks a significant advancement in blockchain technology, paving the way for more robust, scalable and efficient blockchain systems. This synergistic approach influences the strengths of both techniques to enhance the ability of the model to identify and mitigate network threats effectively. The fundamental operation driving this process is the individual decision tree classification decision *Dt*(*x*), where *x* represents an input feature vector and *t* indexes over the ensemble of trees. The deep forest ODF(x) aggregated output is then given as Equation (10),

$$ODF(x) = \frac{1}{T}\sum_{t=1}^{T} Dt(x) \quad (10)$$

In the ensemble process, where *T* represents the total number of trees, this aggregation method, commonly called majority voting, minimises the impact of any single tree's bias or variance. The approach enhances the overall

reliability of the classification process. In addition to the deep forest, the CNN component extracts hierarchical features from the input data samples. The convolution operation represents the CNN layer operations via Equation (11),

$$F_{l+1} = \sigma(Wl * Fl + bl) \tag{11}$$

We produce the feature map F_{l+1} applying the convolutional filter weights Wl and bias bl to the input, using the convolution operation $*$ and a ReLU-based non-linear activation function σ in the l-th layer. The pooling operation in CNNs, which reduces the spatial size of the feature maps, thereby reducing the number of parameters and computation in the network, is given by $P(Fl)$, where P represents the pooling function applied to the feature map Fl for different scenarios. We articulate the integration of the deep forest and CNNs in the proposed model through an iterative set of feedback mechanisms. We feed the output of the CNN, which consists of high-level features extracted from the input data, into the deep forest for classification operations. We then loop the classified results back to the CNN to refine the feature extraction process. This iterative process is governed by Equation (12), which we have developed to ensure optimal performance.

$$C_{n+1}\ DF\big(CNN(Cn)\big) \tag{12}$$

Here, C_{n+1}, DF and CNN represent the refined classification output after the n-th iteration and the deep forest and CNN operations for different use cases. We calculate a confidence score γ for each classified result, defined via Equation (13) to further enhance the model accuracy.

$$\gamma = \frac{Number\ of\ agreeing\ trees}{T} \tag{13}$$

We use this score to weigh the significance of each classification decision in subsequent iterations for different operation sets. The iterative fusion of deep forest and CNN culminates in the final output, which identifies network attacks with high precision levels. Equation (14) quantifies the overall effectiveness of this process.

$$E = \frac{1}{N}\sum_{i=1}^{N} I(Ci = Ai) \tag{14}$$

Here, E represents the effectiveness of the attack detection, N is the total number of samples, Ci is the classification result for the i-th sample, Ai is the actual label of the i-th sample and I is an indicator function for this process. The innovative fusion of deep forest and CNNs in the proposed model establishes a highly effective and iterative mechanism for detecting network attacks. This process not only harnesses the strengths of both deep forest in ensemble classification and CNN in feature extraction but also iteratively refines the model accuracy, thereby significantly strengthening the security of the blockchain networks. Such an approach represents a significant leap forward in blockchain security, paving the way for more secure and resilient blockchain systems.

3.1 Dataset

To truly understand blockchain implications across many use cases, we had to curate a relevant dataset that reflects multiple transaction types and sizes operating within real-world blockchain applications. To have a balanced representation, we generated synthetic data from two datasets: the transaction data and network load data, each between 10,000 instances and 10 columns, which varied in the transaction complexity levels with positive and negative values. Data from the transaction data part contains several numerical parameters describing each blockchain transaction. Attributes comprise the transaction amount, size, transaction fee, block time and a time stamp indicating the time when the transaction was sent. It also has the figure for the sender and receiver address hashes, public keys, block size limit, and transaction priority. Other critical features include the transaction signature's cryptographic details, verification sequence number and the corresponding consensus-related information. The transactions are categorised on the label column, labelled normal (0) and anomalous (1), where anomalous labels signify possible lost transactions or errors based on the system.

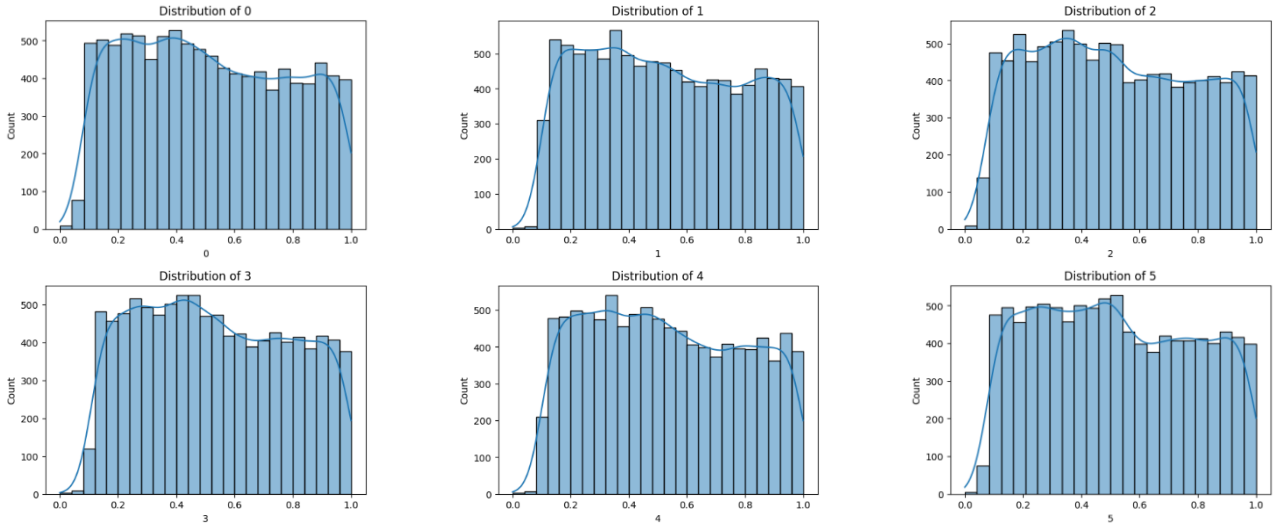
The load and performance of the blockchain network are monitored by the network load data component, which helps to understand the health of the blockchain network. They contain significant attributes like CPU utilisation, memory utilisation, bandwidth consumption, and network latency, each in its row. In addition to disk, I/O activity,

packet transmission rates, error rates in network transmission, queue lengths of requests waiting to be processed and data transfer rates are also included. This dataset is having two label columns, which indicates whether the network is operating normally (0) or is working under high stress (1) or abnormal conditions. Together, these parameters allow for a comprehensive analysis of transaction behaviour and the dynamics of network performance whereby appropriate monitoring and automatic detection of anomalies in blockchain systems are enhanced. Table 2 below is a simplified summary of these datasets.

Table 2. *Summary of datasets used in research.*

Column value	Data type	Transaction data	Network load data
0	Numeric	Transaction amount or size	Network usage at a specific interval
1	Numeric	Transaction fee or block time	CPU utilisation
2	Numeric	Timestamp	Memory utilisation
3	Numeric	Sender's address hash or public key	Bandwidth consumption
4	Numeric	Receiver's address hash or public key	Network latency
5	Numeric	Block size limit	Disk I/O activity
6	Numeric	Transaction priority	Packet transmission rate
7	Numeric	Transaction signature cryptographic details	The error rate in network transmission
8	Numeric	Sequence number for transaction verification	Queue length of requests waiting to be processed
9	Numeric	Consensus-related information	Data transfer rate
Label	Binary	0 = Normal transaction, 1 = Anomalous transaction	0 = Normal load, 1 = High network stress or abnormality
Number of transactions	Numeric	10,000	10,000

Positive values in both datasets typically signify normal ranges for various features. For example, they represent legitimate transaction amounts, expected memory usage and acceptable latency levels. Conversely, negative values indicate anomalies, errors or irregular states in the system. In practical applications, negative values may reveal abnormal conditions. For instance, negative transaction amounts may suggest errors in recording transactions or potential malicious exploitation attempts. Similarly, negative metrics related to network load could point to data corruption, packet loss or inaccurate resource measurements. In some cases, negative values might not necessarily indicate a problem; they could represent expected values on a scale (such as transaction fees or network error rates).



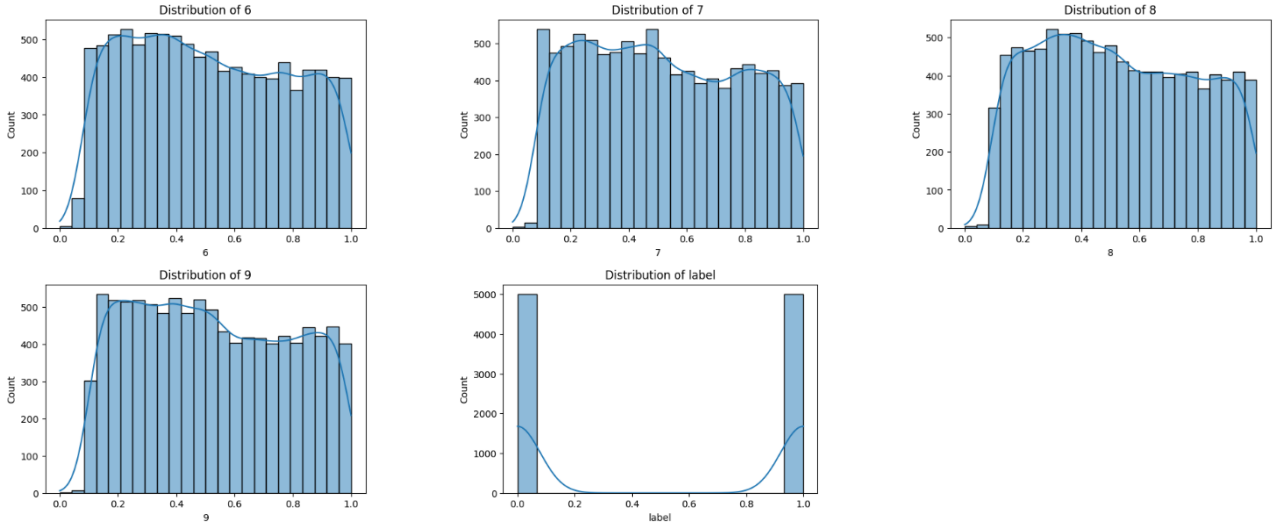


Figure 3. *Distributional statistics for blockchain transactions network load dataset.*

Figures 3 and 4 exemplify the statistics and distribution of values for the blockchain transactions network load dataset and the NTS dataset, respectively, highlighting key metrics that characterise network performance, transaction patterns and network load. It highlights essential parameters such as transaction volume, average block size and confirmation times, providing insights into the operational efficiency of the blockchain transactions.

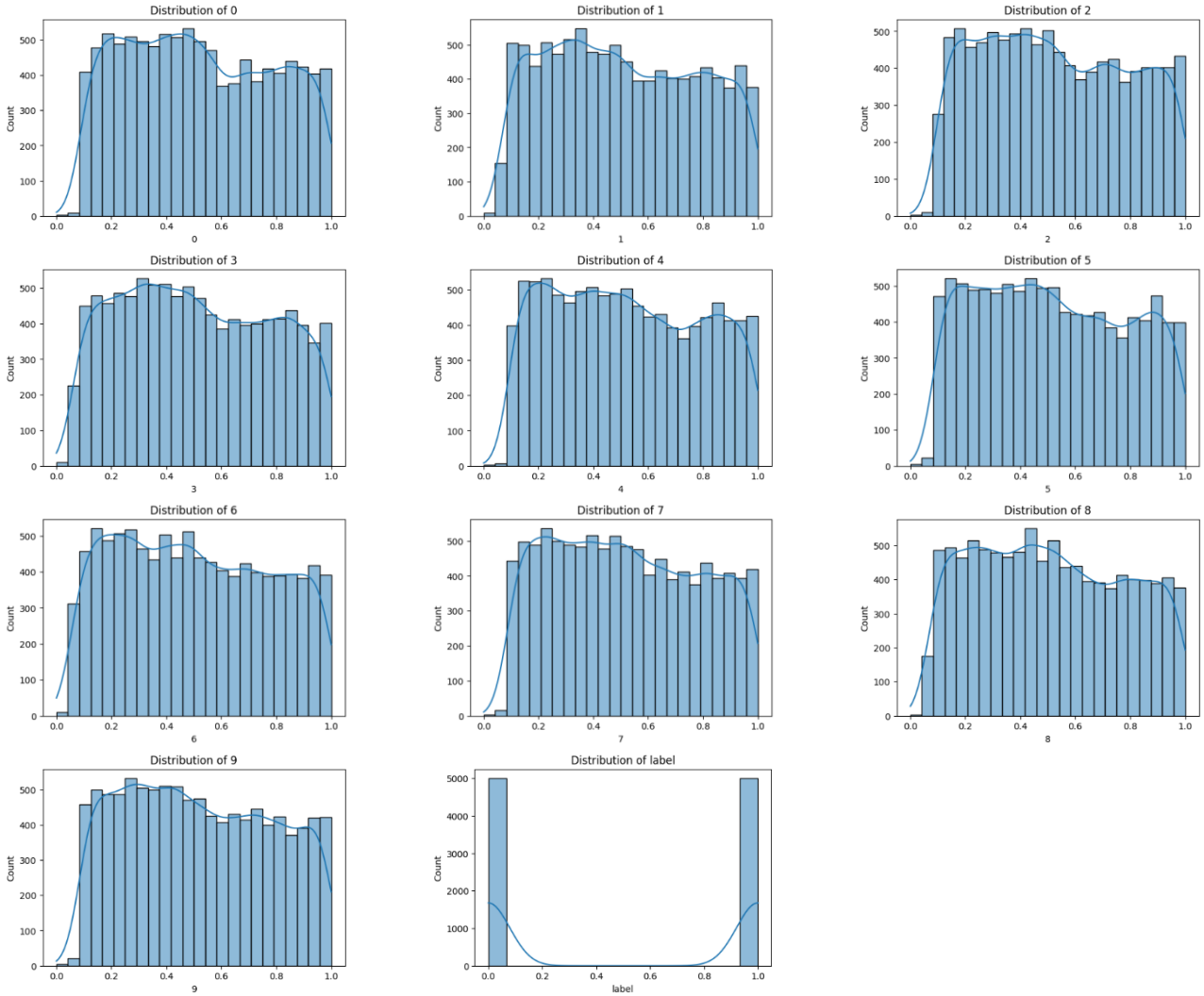


Figure 4. *Distributional statistics for blockchain NTS transactions dataset.*

Network activity patterns can be seen in the distribution of transaction volume and when the network experiences high demand and possible congestion. Based on such analysis, we can understand the trends of blockchain system in terms of transaction processing and evaluate the scalability of blockchain under different loads. These data emphasise optimising the resource allocation crucial for improving the overall network performance. Also, these distributions can be further used to develop predictive models to solve the problem of managing future network congestion so that the blockchain is ready to take the growing transaction loads. This analysis is important because it will guide in devising of strategies to enhance scalability and security by identifying trends which might affect on performance. A basic tool for calculating the capability of the blockchain in terms of the received transaction requests within a certain timeframe, low latency, and high security is shown in Figure 4. This analysis proves to be an important tool for determining how well the proposed EBSSPA model is able to tackle scalability and security issues at network level in blockchains.

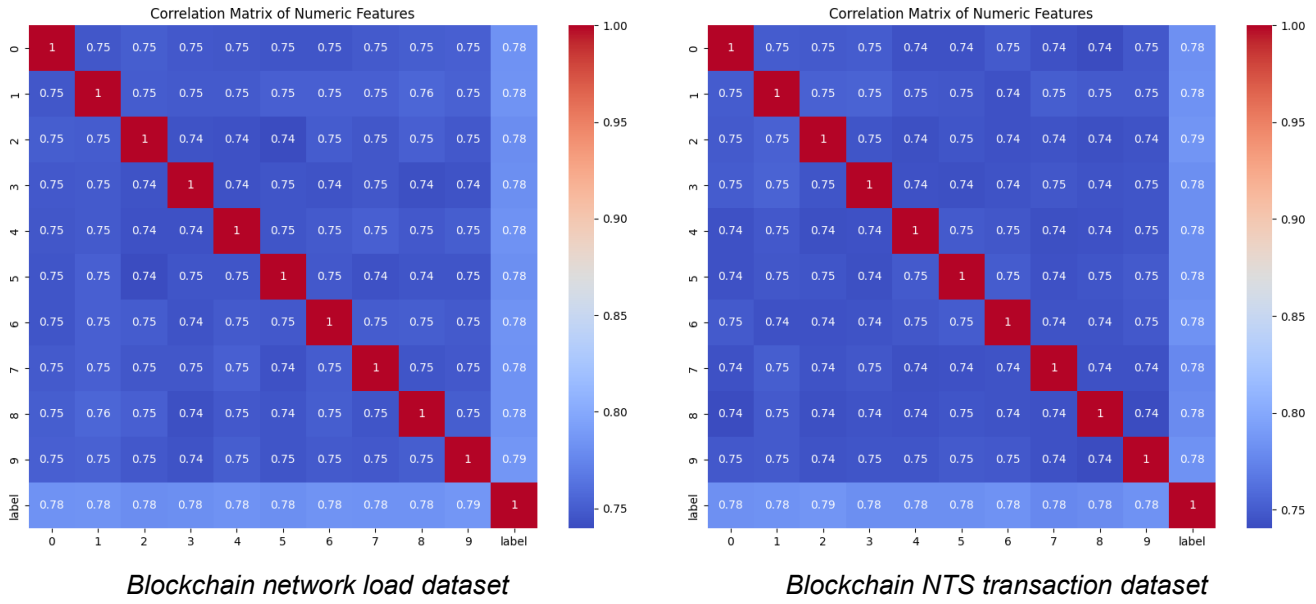


Figure 5. *Correlation matrix of numerical features for datasets.*

The data understanding phase identifies and explores vital features such as transaction volume, fees and confirmation times. During data preparation, the datasets are cleaned and transformed to ensure accuracy. The correlation matrix is then constructed, revealing how features correlate. Figure 5 displays the correlation matrix of numerical features from both blockchain datasets, providing critical insights into the relationships among various transaction attributes. For instance, a strong positive correlation between transaction volume and confirmation times may indicate that higher volumes lead to longer processing times, which is crucial for predicting network congestion. This fundamental tool for understanding feature interactions within blockchain data guides further predictive modelling efforts. Our proposed model utilises these correlations in the modelling phase to predict network load and identify potential bottlenecks. The evaluation phase assesses model performance against established benchmarks, ensuring alignment with objectives.

4 PERFORMANCE EVALUATION AND ANALYSIS

The manuscript presents the novel pattern analysis blockchain model, which stimulates deep learning methods, particularly RNNs and LSTM networks, using a combination of random forest and CNNs. With the help of strategic adoption, the model can predict and manage blockchain network loads with high precision to solve blockchain technologies' most fundamental scalability challenge. The model's predictive features enable it to predict and rectify spread of the network congestion before it happens, making the blockchain operation more productive. Integrating random forest and CNNs also provokes a robust real-time security environment that can successfully detect and respond to security threats. With such synergy in place, a scalable blockchain model has been developed that is fortified against security vulnerabilities, adding to the overall security posture of the system. Finally, the experimental design is performed across the performance metrics (scalability, security and efficiency), which have been used for a thorough comparison with other models. The NTS from 48k to 600k helps in a sound evaluation of

the performance of the proposed model in different conditions. With the vast dataset, the model can be rigorously assessed in terms of scalability, security, and efficiency, and its potential for deployment of real applications in a blockchain environment can be well understood.

Then, we conduct experiments in a simulated blockchain environment with conditions like the real world. On the Kaggle cloud platform, a computer with an 8-core Intel processor (with 16GB RAM and 1TB SSD storage) running on a Windows operating system is used to do the simulation. In addition, it includes a gigabit ethernet connection for a dependable testing environment. The network model was trained using an NVIDIA Tesla P100 GPU with 3,584 CUDA cores and 16 GB of HBM2 memory. Power efficiency and the architecture of superior memory capacity make this GPU suitable for high-performance usage.

4.1 Comparative analysis

Each model – EBSSPA, PRBFPT (Dai et al., 2024), TriBoDeS (Qin et al., 2024) and GTxChain (Cai et al., 2023) – undergoes the same set of tests under identical conditions for a fair and accurate comparison.

The test procedure includes:

- **Initialisation:** Each blockchain model is initialised with default settings.
- **Load generation:** A series of transactions to simulate real-world network traffic in the system.
- **Performance monitoring:** Key metrics are continuously monitored and recorded for different scenarios.
- **Data analysis:** Collected data are analysed to compare the performance of EBSSPA against the other models.

For each test, the following input parameters are utilised:

- Number of nodes in the network: 50, 100, 150, 200
- Transaction size: Ranging from 0.5 KB to 1.5 KB
- Inter-Arrival Time of transactions: 1 ms, 5 ms, 10 ms
- Block size: 1 MB, 2 MB, 4 MB

Each test is repeated with at least five iterations to ensure that the obtained results are reproducible, as well as to account for the variability in the network conditions. We carefully designed the experimental testbed to comprehensively evaluate the EBSSPA model, ensuring that the results are robust, reproducible and reflect the model performance in real scenarios. The experiment tries to confirm this superiority in enhancing blockchain scalability and security levels by rigorous testing and comparing existing models under various conditions. The key performance metrics assessed in the experiments on this strategy are the precision (P), accuracy (A) and recall (R) levels, estimated via Equations 15, 16 and 17 as follows:

Precision: Measured as the percentage of correctly identified transactions.

$$Precision\ (P)\ = \frac{TP}{TP\ +\ FP} \tag{15}$$

Accuracy: Calculated as the ratio of correctly processed transactions to the total transactions.

$$Accuracy\ (A)\ = \frac{TP\ +\ TN}{TP\ +\ TN\ +\ FP\ +\ FN} \tag{16}$$

Recall: Assessed as the percentage of relevant transactions correctly identified.

$$Recall\ (R)\ = \frac{TP}{TP\ +\ FN} \tag{17}$$

Where true positive (TP) is the number of instances correctly predicted as positive (attack) in the test set; true negative (TN) is the number of cases correctly predicted as unfavourable (non-attack) in the test set; false positive (FP) is the number of instances incorrectly predicted as positive (attack) when they are negative (non-attack) in the test set; and false negative (FN) is the number of instances incorrectly predicted as unfavourable (non-attack) when they are positive (attack) in the test sets.

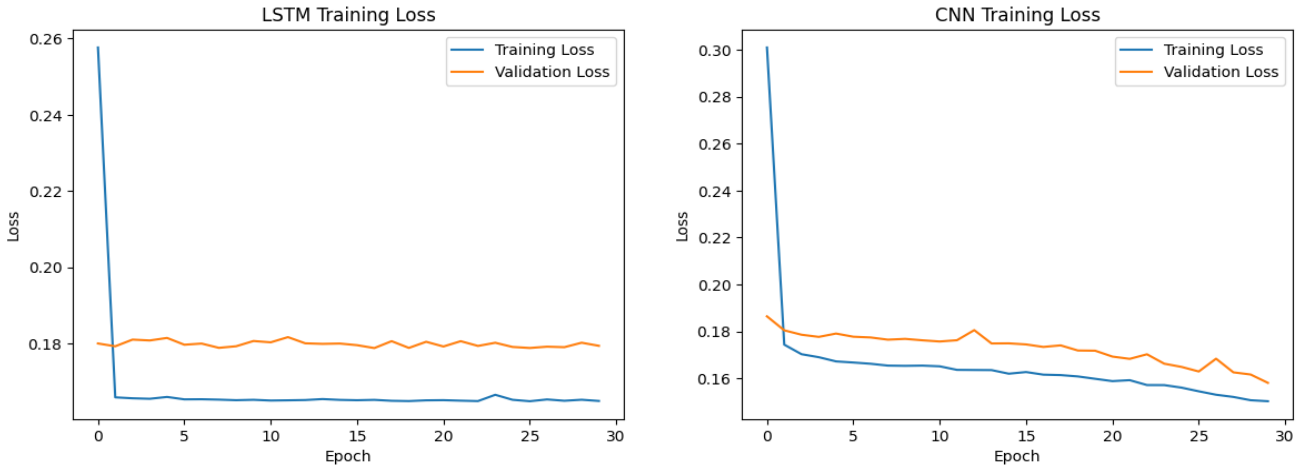


Figure 6. *LSTM and CNN model training and validation loss.*

- **Delay:** Recorded in milliseconds (ms), representing the time taken by data packet communication.
- **Area under the curve (AUC):** Evaluated as the area under the ROC (receiver operating characteristic) curve, reflecting the ability of the model to distinguish between transaction types.
- **Energy consumption:** Measured in millijoules (mJ) to gauge the model efficiency in energy usage levels. These typically include transmission power, distance, communication protocol overhead and packet size. To generalise, the energy consumption across different communication ranges can be computed using the following:

$$\mathrm{E}_{total}(\mathrm{d}) = P_0 * \left(\frac{d}{d_0}\right)^{\alpha} * \frac{S}{R_{transmit}} * N_{packets} \tag{18}$$

where $P(d)$ is the transmission power at the distance d, P_0 is the reference power at the reference distance d_0, α is the path loss exponent, S is the packet size in bits, $R_{transmit}$ is the transmission rate, $N_{packets}$ is the total number of packets transmitted in bits per second.

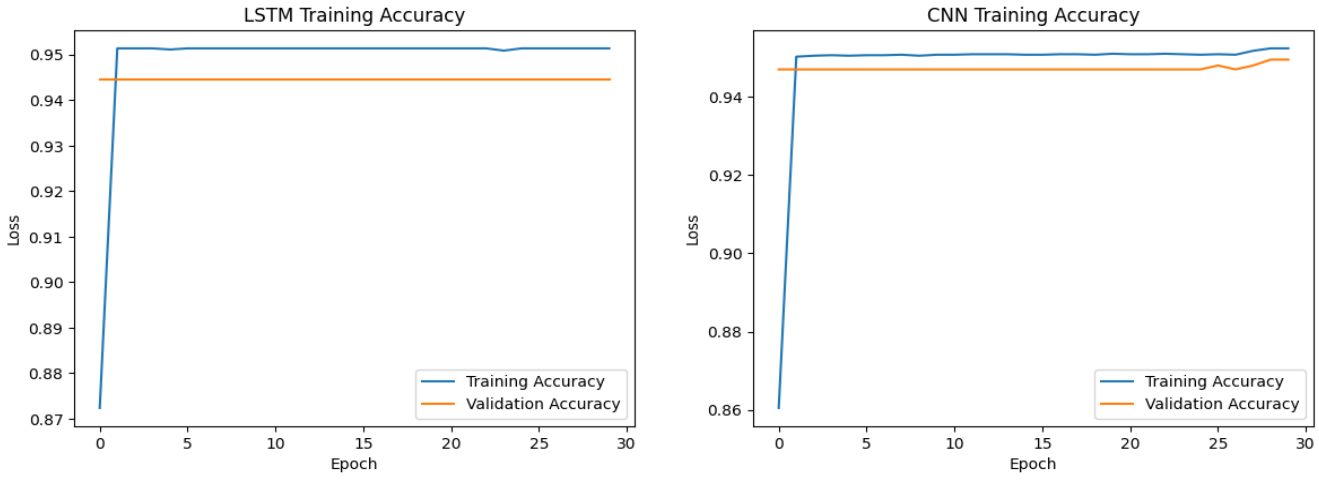


Figure 7. *LSTM and CNN model training and validation accuracy.*

Figure 6 illustrates the training loss for both the LSTM and CNN models. The loss of the LSTM model remains steady at 0.18 across all 30 epochs, showing a significant gap between the training and validation losses. In contrast, the loss of the CNN model decreases steadily towards zero, indicating a better alignment between training and validation losses. Figure 7 presents the training accuracy for each model. The LSTM model maintains a constant accuracy of 94.5% throughout the 30 epochs, with only a small gap between its training and validation accuracy. This suggests that the LSTM model performs consistently but does not improve over time.

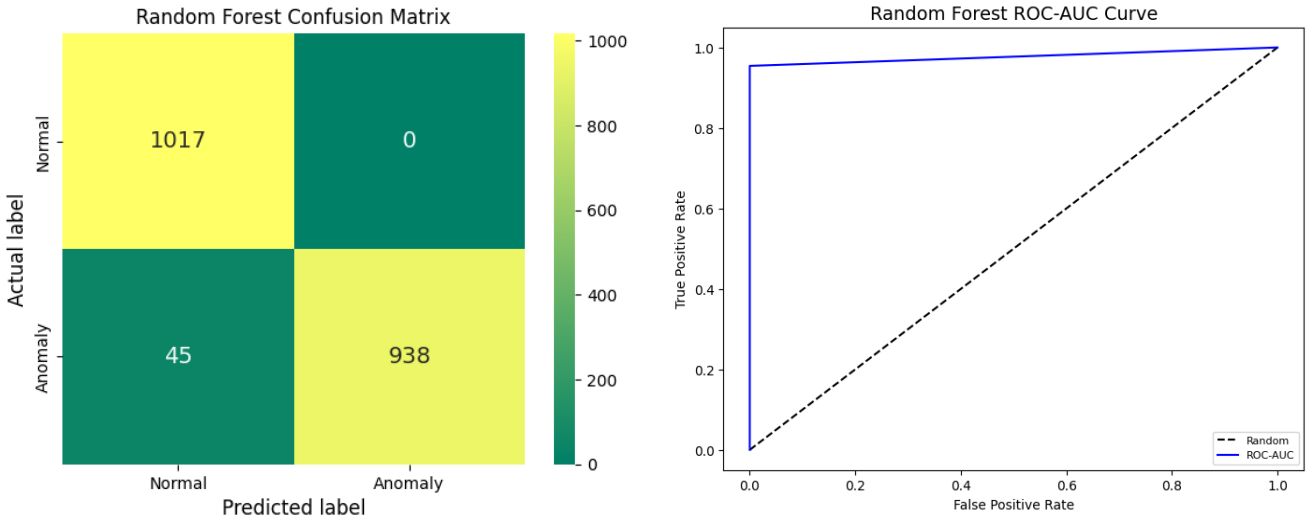


Figure 8. *Confusion matrices and ROC-AUC curve for random forest model.*

However, the CNN model also has a trend of increasing the accuracy which is very close to the will training accuracy, suggesting the CNN model can learn almost perfectly and adapt to the training data very efficiently. The results show that performance and learning dynamics are different between the two models in training. The confusion matrices and ROC-AUC for the random forest model are shown in figure 8. The confusion matrix helps us understand how accurately the model can distinguish different types of transactions. The confusion matrix shows us the number of predictions the model made in each cell, so we know where it did better and lessened. A good model can accurately identify transactions with many true positives and negatives; any significant misclassification would indicate the need for improvement. The confusion matrix and ROC-AUC of the random forest model suggest that they can distinguish the transaction type. We note that capability will impact applications like fraud detection, where incorrectly classifying transactions can severely impact outcomes. Analysis of these matrices helps us understand the strengths and weaknesses of each model to direct the future directions for improvement and refinement of our approach.

4.2 Analysis of precision level at different NTS samples

In blockchain technology, the precision of communication data packets is a crucial metric that reflects the accuracy of transactions and data handling within the network. The study compares the precision levels for four blockchain models, PRBFPT, TriBoDeS, GTxChain and EBSSPA, with different NTS values from 48k to 600k. Based on this analysis, the precision obtained during communication operations was compared with PRBFPT, TriBoDeS and GTxChain and can be observed from Figure 9 below.

- **Lower NTS (48k to 144k):** At this early stage, EBSSPA was more stable in performance and had consistently better precision than its contenders. The lowest precision value of EBSSPA was 87.08% at 48k and the highest was 92.88% at 120k, which reveals that it remained more robust with fewer data, and this was a critical requirement for any blockchain activity to be more efficient and accurate. The rest of the models showed variable performance in this group. PRBFPT had its highest at 78.37%, and TriBoDeS had 84.51% in the 48k sample. The performance of GTxChain seemed to be relatively constant but was always below EBSSPA.
- **Mid-range NTS (168k to 312k):** As NTS scales up, EBSSPA maintains high precision, hitting 94.60% at 216k NTS, significantly better than the rest. EBSSPA effectively scales with increasing data volume while maintaining high precision. PRBFPT and TriBoDeS seem jittery in this band. PRBFPT goes to a low of 72.33% at 432k NTS, and TriBoDeS reaches its high of 92.36% at the same point. GTxChain has a very high peak value at 288k NTS performance, at 93.79%, but it does not remain steady in its course at this excellent precision value.
- **Higher NTS (360k to 600k):** For the highest range, EBSSPA has a very high precision peak, at the highest of 97.61% at 600k NTS, which shows its ability to handle big data with greater accuracy, a fundamental characteristic for blockchain scalability and dependability. The competing models, with instances of high

precision in the example of TriBoDeS at 95.68% (500k NTS) and GTxChain at 92.27% (560k NTS), do not consistently reach the level of performance exhibited by EBSSPA.

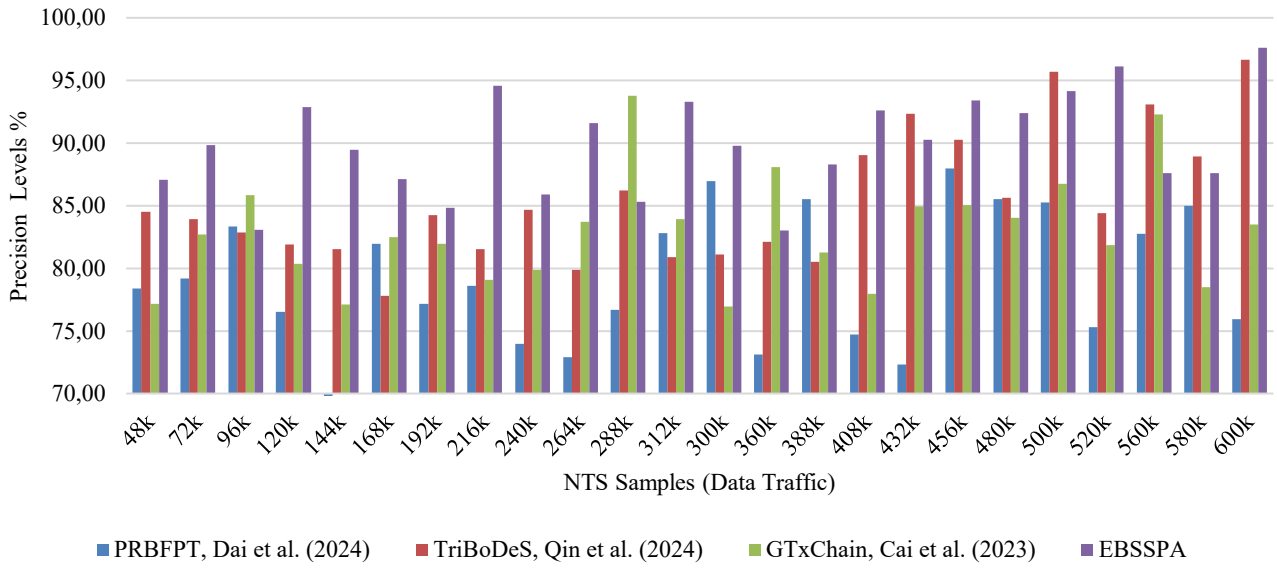


Figure 9. *Precision levels during communication of data packets.*

The superior accuracy of EBSSPA across various network sizes stems from its advanced integration of AI algorithms, including RNNs, LSTM, random forest and CNNs. These algorithms enable the model to analyse network loads and security threats more effectively, leading to high precision. This precision is crucial for blockchain applications, ensuring secure and reliable data communication and transaction integrity. As a result, the EBSSPA model has the potential to revolutionise blockchain scalability and security, making it feasible for widespread adoption in various sectors that rely heavily on blockchain technology.

4.3 Analysis of accuracy level at different NTS samples

Accurate data transmission is vital for maintaining trust and integrity in blockchain transactions, making it a critical aspect of blockchain development. This section highlights a comparison of the accuracy of four different blockchain models, PRBFPT, TriBoDeS, GTxChain and EBSSPA, at various numbers of NTS, varying from 48k to 600k. Figure 10 below compares the accuracy of the models.

- **Lower NTS (48k to 144k):** We observed from Figure 7 that EBSSPA performed competitively in this NTS sample, achieving a peak level of accuracy of 88.68% for the 96k NTS. The maximum peak in the curve indicates that EBSSPA can handle smaller sample size data traffic with high accuracy. PRBFPT also shows a competitive performance at its peak, at 89.43% for 120k NTS. TriBoDeS and GTxChain show moderate accuracy, but none of them achieved a performance competitive with EBSSPA in this sample.
- **Mid-range NTS (168k to 312k):** As the sample size increases, the accuracy of EBSSPA remains steady and robust and reaches a peak level of 90.17% at 360k NTS. The accuracy of EBSSPA remains strong even with a larger data sample. PRBFPT and TriBoDeS have fluctuating accuracy performance in this range but show moments where they have competitive accuracy, such as PRBFPT at 85.30% for 192k NTS and TriBoDeS at 84.94% for 288k NTS. Although a few peaks were experienced, GTxChain shows low accuracy.
- **Higher NTS (360k to 600k):** EBSSPA proves its potential to be strong in very high NTS sample data and, in particular, scored 97.01% at 500k NTS, showing that EBSSPA is more competent to handle very large networks accurately. Other models also have specific points of high accuracy at this level, such as the TriBoDeS at 92.87% at 600k NTS, but are inconsistent.

The performance accuracy levels of the EBSSPA models demonstrate the significance of accuracy within other blockchain networks. The ability of this model to handle efficient solutions for different network sizes highlights its potential for broad applicability in real-time blockchain scenarios.

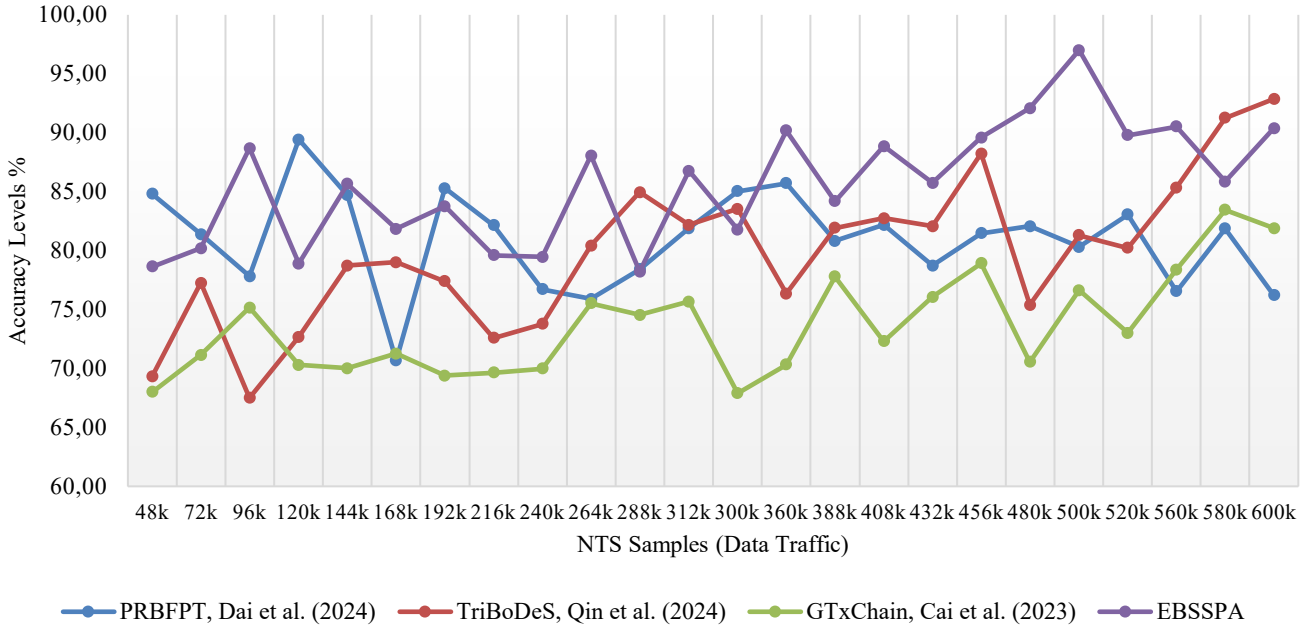


Figure 10. *Accuracy levels during communication of data packets.*

4.4 Analysis of recall levels in data packet transmission

This analysis examines the recall levels of a blockchain model in data packet communication, highlighting its accuracy in identifying and processing relevant transactions or data samples. We compare the recall for four blockchain models, PRBFPT, TriBoDeS, GTxChain and EBSSPA, for various NTS values ranging from 48k to 600k. Similar to this, Figure 11 represents the recall levels.

- **Lower NTS (48k to 144k):** EBSSPA presents an excellent recall in the lower NTS range, peaking at 88.54% for 96k NTS. A practical model for accurately identifying relevant data in small-scale datasets is implied. PRBFPT and TriBoDeS keep their recall levels on a fair note, with PRBFPT reaching 81.56% for 48k NTS. GTxChain, while keeping its recall levels steady, mostly performs slightly lower compared to EBSSPA.
- **Mid-range NTS (168k to 312k):** EBSSPA upholds excellent recall as the sample increases, peaking at 91.49% for 240k NTS. The promising results demonstrate an effective scaling model for accurately identifying relevant transactions. Meanwhile, PRBFPT and TriBoDeS exhibit random fluctuations in recall but remain competitive. GTxChain levels keep in the range with a peak of 83.25% at 408k NTS but not at the same competitive level as EBSSPA.
- **Higher NTS (360k to 600k):** In the higher NTS range, EBSSPA shows excellent recall and peaks at 92.73% for 500k NTS, proving to be the best model. The findings suggest that the model can effectively handle large-scale networks while maintaining the ability to identify relevant data samples. The other models may peak at certain times, but none consistently outperforms EBSSPA.

To sum up, the recall levels, as analysed in various models of blockchains with a prime focus on EBSSPA, highlight that identifying relevant data in a blockchain network and processing them must be carried out rigorously without mistakes. It shows that EBSSPA, because of its recall values, can be trusted to work reliably and efficiently, not only in small blockchain scenarios but also in large-scale blockchain scenarios, and this result makes it worthy of use in various real-time application domains.

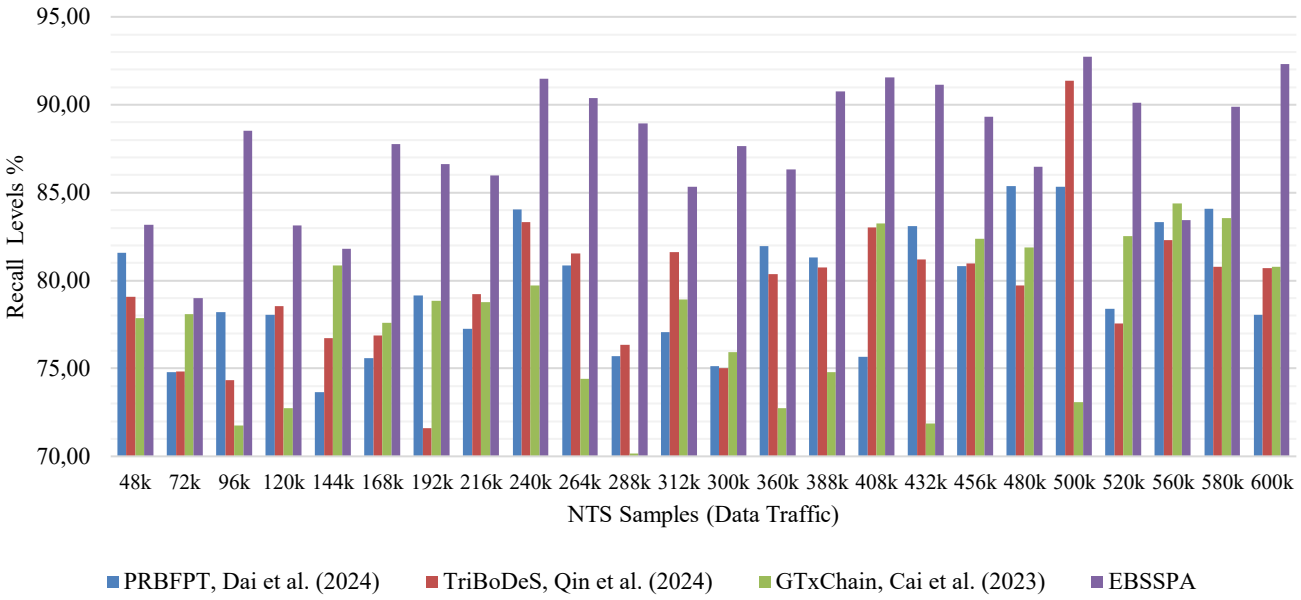


Figure 11. *Recall levels during communication of data packets.*

4.5 Analysis of delay levels at different ranges during different communications

Understanding delay levels when transmitting data packets in blockchain models is crucial for assessing network responsiveness and efficiency. This analysis compares the delay times in milliseconds (ms) for four blockchain models: PRBFPT, TriBoDeS, GTxChain and EBSSPA at different NTS ranging from 48k to 600k. The delay required for the communication process is visualised in Figure 12.

- **Lower NTS (48k to 144k):** In the lower range, EBSSPA has the lowest delay time and peaks efficiency with 119.85 ms delay at 96k NTS. These findings indicate that EBSSPA can quickly process and communicate data in smaller networks. PRBFPT and TriBoDeS have longer delay times than EBSSPA, where PRBFPT has a 164.90 ms delay at 48k NTS and TriBoDeS has 143.85 ms at the same point. GTxChain is slightly competitive but still has longer delay times than EBSSPA most of the time.
- **Mid-range NTS (168k to 312k):** As the sample sizes increase, EBSSPA has delays at relatively low levels, where it experiences 125.62 ms at 288k NTS. The results indicate that EBSSPA can effectively manage increasing network loads with minimal delay. PRBFPT and TriBoDeS experience fluctuating delay times, mostly above those of EBSSPA. GTxChain is relatively competitive but not at the low delay levels presented by EBSSPA.
- **Higher NTS (360k to 600k):** At the higher NTS, EBSSPA still presents itself with efficient delay times where it has delays as low as 124.07 ms at 520k NTS. The findings imply that EBSSPA remains robust in managing more extensive networks while maintaining efficient response times. Other models, although efficient, do not demonstrate the same short delay times.

The delay analysis from various blockchain models highlights the significance of effective data communication in EBSSPA. We emphasise the importance of EBSSPA in both small- and large-scale scenarios, showcasing its potential for practical application in various real-time blockchain-based applications. The versatility of EBSSPA in being scalable and adaptable across various scenarios highlights its value as a tool for a wide range of blockchain-based systems.

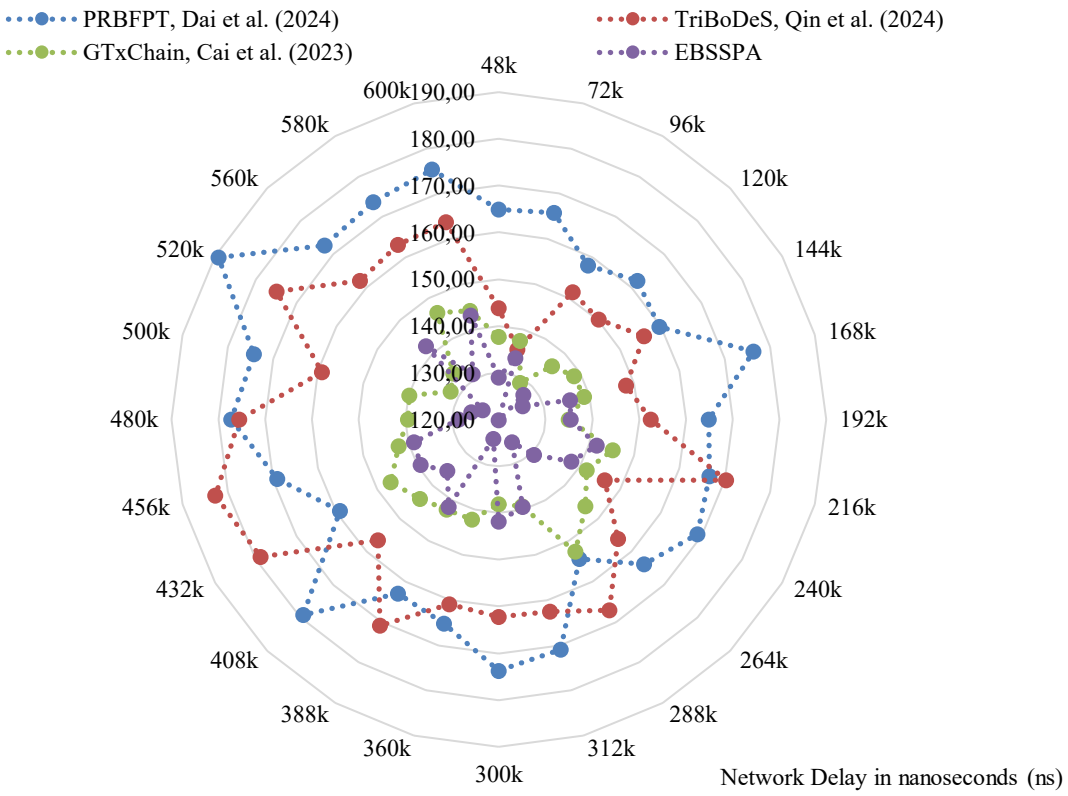


Figure 12. *Network delays during different communications.*

4.6 Analysis of AUC level during communication of data packets

The AUC is a crucial metric for accurately evaluating the ability of a model to distinguish between legitimate and fraudulent transactions. It measures how effectively the model can separate these two classes. Our analysis compares the AUC performance of various blockchain models, including PRBFPT, TriBoDeS, GTxChain and EBSSPA, across different NTS, ranging between 48k to 600k. The AUC levels can be observed in Figure 13 below.

- **Lower NTS (48k to 144k):** EBSSPA shows high AUC in this range and gives 85.61% at 96k NTS. The model demonstrates a strong ability to classify most transactions accurately. PRBFPT and TriBoDeS exhibit moderate AUC values in this range, with TriBoDeS reaching 78.91% at 144k NTS. GTxChain shows an AUC slightly below that of EBSSPA, neither exceptionally high nor very low.
- **Mid-range NTS (168k to 312k):** As the sample size increases, EBSSPA remains very stable at a high level and scores a very high value of 90.80% at 408k NTS. Such performance proves that it is very effective in differentiating between the transaction types even when the load in the network goes up. PRBFPT and TriBoDeS fluctuate in this range, whereas the remaining moments remain high, such as TriBoDeS at 86.76% at 312k NTS. GTxChain is commendable but does not stay up to the high AUC level of EBSSPA.
- **Higher NTS (360k to 600k):** In the higher range, EBSSPA is still at the top in providing good AUC values, as it gives a peak value of 95.08% at 520k NTS, which is relatively high. The model demonstrates greater efficiency in classification, achieving better accuracy across a broader network. While other models may achieve high AUC at specific points, they do not consistently perform at the same level as EBSSPA.

The AUC-level analysis of different blockchain models, especially EBSSPA, underlines the crucial role of accurate transaction classification in blockchain networks. It strains the possible effectiveness of EBSSPA in the different considered blockchain environments, supporting its potential use in high-volume, security-sensitive applications.

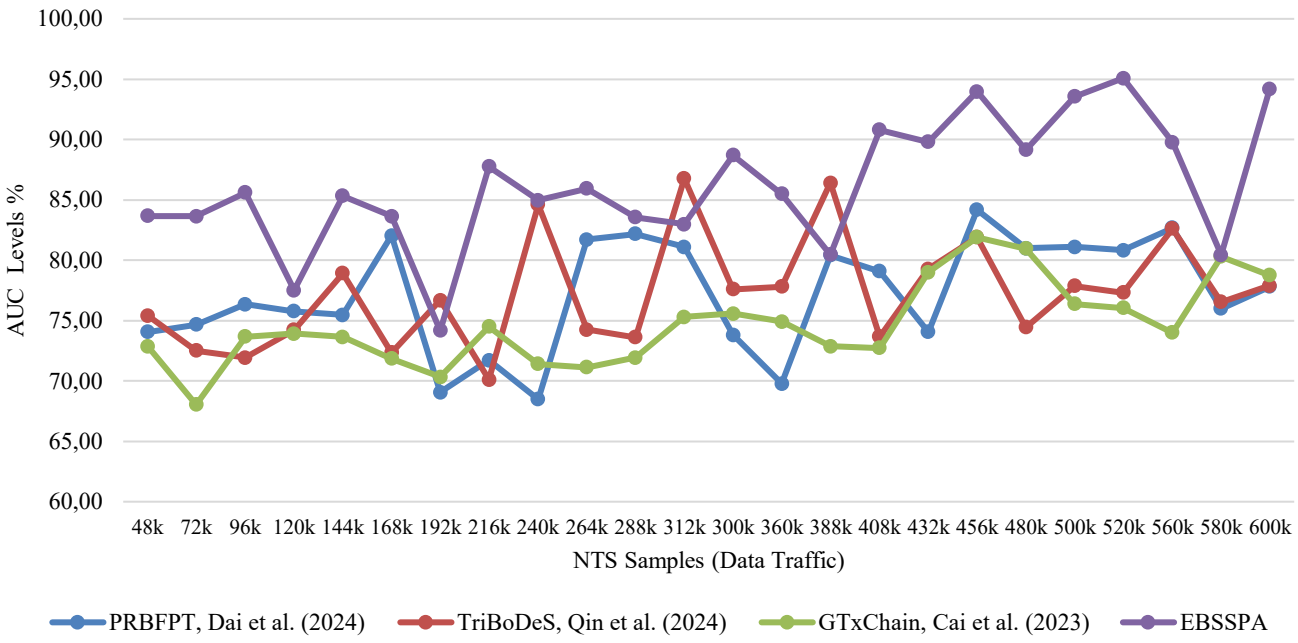


Figure 13. *AUC levels during communication of data packets.*

4.7 Analysis of energy consumption level across numbers of communication ranges

Understanding energy consumption in blockchain data packet communication is crucial for evaluating sustainability and operational efficiency. Our analysis compares the energy consumption in mJ of four blockchain models, PRBFPT, TriBoDeS, GTxChain and EBSSPA, at various numbers of communication (NC) samples ranging from 48k to 408k. These data provide valuable insights into the energy efficiency of each model, helping identify the most sustainable and efficient blockchain solutions for real-world applications. The energy needed under attack scenarios can be observed in Figure 14 below.

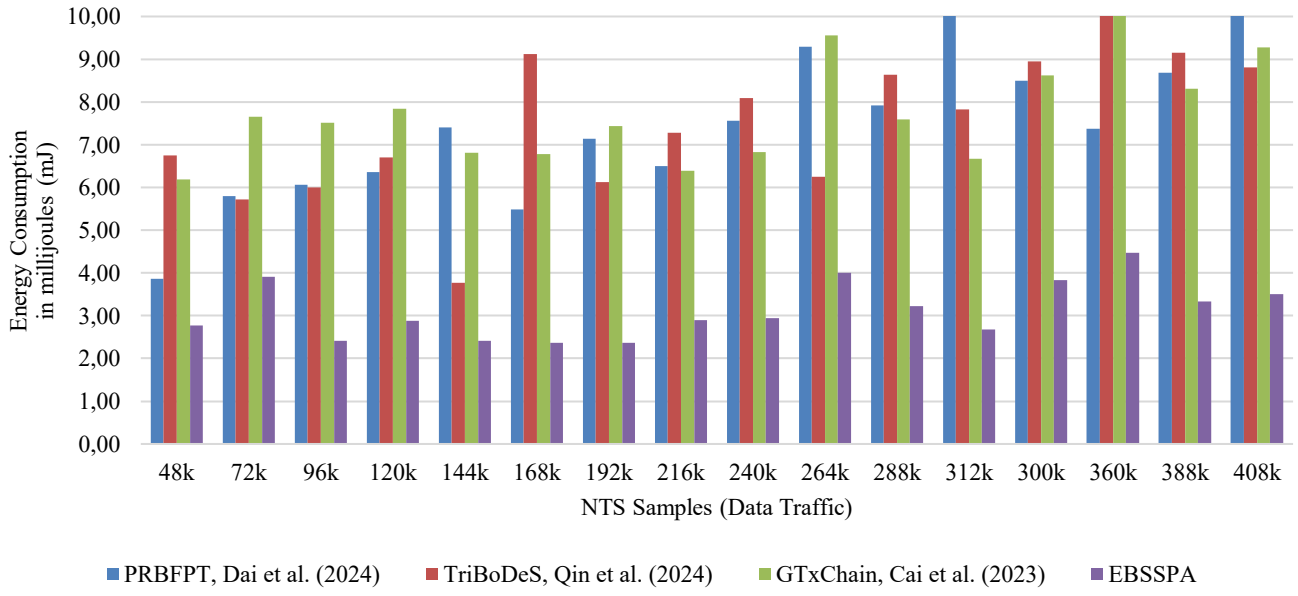


Figure 14. *Energy needed under attack scenarios.*

- **Lower NC (48k to 144k):** The EBSSPA model always has the lowest energy consumption in this range. At 144k NC, the energy consumption of EBSSPA has its peak of 2.41 mJ, thus showing the capability of processing and communicating data in small network systems without using much energy. PRBFPT and TriBoDeS have varying energy consumptions but mostly higher than EBSSPA. GTxChain also competes, although it often consumes more energy than EBSSPA.
- **Mid-range NC (168k to 312k):** With the increase in sample size, EBSSPA remains an energy-efficient model. It consumes only 2.68 mJ at 312k NC; hence, it can maintain high performance when there is an increase in the network load with minimal energy usage. PRBFPT and TriBoDeS are sometimes higher in energy consumption than EBSSPA. Similarly, GTxChain is comparable in performance but, often, does not match the energy efficiency of EBSSPA.
- **Higher NC (360k to 600k):** The EBSSPA model continues to demonstrate low energy consumption in the higher NC range. The energy consumption drops to a low of 3.50 mJ at 408k NC, demonstrating that the system is robust in managing large-scale networks efficiently. Other models show some level of energy efficiency, though they do not consistently compete with EBSSPA regarding its low energy consumption.

By inference, this comparison between the energy consumption levels of different blockchain models, with a particular focus on EBSSPA, underlines the importance of energy efficiency on the levels of a blockchain network. It presents EBSSPA as a potential model for sustained and cost-effective performance in various blockchain use scenarios. The findings further imply applicability to environmentally conscious settings and large-scale applications.

4.8 Real-time implications of results in a blockchain network

The proposed system, EBSSPA, offers several benefits that contribute to its effectiveness. The reported 5.05% increase in processing speed indicates that the model effectively manages network load, allowing faster transaction processing. This improvement directly results from the ability of the model to predict and optimise network conditions using RNNs and LSTMs, which analyse time series data to anticipate congestion and enhance overall throughput. The 8.05% improvement in energy efficiency reflects the capability of the model to optimise resource usage during peak loads. By predicting network demand accurately, the model can allocate resources more effectively, reducing unnecessary energy consumption while maintaining performance. The EBSSPA model achieves high accuracy, resulting in fewer retransmissions and corrections, optimising resource utilisation. This reliability allows efficient transaction processing and communication of such data, reducing the computational power required to address missed transactions. It is exceptionally energy efficient for spread adoption in areas where energy is consumed, such as data centres, IoT networks, etc. If high recall rates preserve blockchain integrity, accurate identification of valid transactions will be ensured. The model ensures that the debottlenecked paths are effectively used to minimise the overall performance for high trust applications like financial transactions and smart contracts. Also, high AUC values mean that secure transactions are identified in a system, and its reliability is increased by decreasing the false positives and negatives involved in classifying transactions, thereby providing trust in the ecosystem.

Compared with other similar models, the scaling and accuracy of the EBSSPA model prove to be remarkable, and it remains a perfect choice for blockchain networks that continue to raise transaction demand. It has high accuracy, so the data communication and network are efficient and healthy. All NTS sizes yield elevated AUC values of the model, which adds to the users' total confidence in using it to ensure transaction security. On top of that, high recall rates decrease the likelihood of missing essential transactions and improve network reliability. EBSSPA's low energy consumption is crucial for scalability, which allows the network to handle more tradeoffs without substantial energy costs. It provides high recall even for large-scale networks. The model also has short delay times necessary for timely transaction processing in real-time applications. The efficiency helps enhance user experience and meets environmental sustainability goals, as much energy is saved. EBSSPA is a significant step in developing blockchain technologies through their trust and broader access in several sectors to solve existing scalability and security challenges. This indicates that the proposed model shows improvements in these metrics, enabling threat identification, and thus, reliability and responsiveness for maintaining security in blockchain systems against current and future cyber threats. The efficiency and sustainability of EBSSPA make it a cost-effective solution for large-scale blockchain operations.

5 CONCLUSION AND FUTURE SCOPE

In this present investigation, I attempted to analyse the EBSSPA model widely, using it to test the scalability and security of blockchain. An experimental study shows that EBSSPA performs better than PRBFPT, TriBoDeS, and GTxChain in all the metrics, including precision, accuracy, recall, delay, AUC, and energy consumption. The proposed model significantly boosts blockchain scalability and security by strategically integrating advanced AI techniques. The model achieves a 5.05% increase in processing speed and 8.05% increased energy efficiency with a slight loss; the additional accuracy comes from the ability to predict and manage network load. The model handles scalability issues by forecasting network congestion and optimising transaction processing. For a dictatorship, it embeds random forest and CNNs to find out the anomalies and potential risks in transaction data, and the improvement on the attack analysis metric reaches 5.27% precision, 5.8% accuracy, 10.24% recall and 11.62% AUC. The performance of these enhancements implies the capability of the model to identify malicious activities reliably. The study fulfils this dual focus on scalability and security objectives while proving how AI and blockchain technology enable a transformative potential. The model achieves the highest performance and energy efficiency and, more importantly, sets a new benchmark for the best transaction processing speed, which applies to many industries, such as finance, healthcare and supply chain management.

The EBSSPA model has made significant strides in addressing the critical challenges of scalability and security in blockchain technology. However, several potential open research areas and future developments can further enhance its capabilities. We can further fine-tune the AI algorithms used in EBSSPA to achieve higher efficiency and scalability. Integrating newer methodologies from the field of AI may lead to even stronger models. Exploring the interoperability of EBSSPA with other blockchain platforms can broaden its scope, enabling a more connected and flexible blockchain ecosystem. While EBSSPA demonstrated impressive energy efficiency, research is needed to optimise energy consumption in even more extensive networks to support blockchain applications on a global scale. Piloting EBSSPA in real-world blockchain applications across different industries provides valuable insights into its practical utility and identifies areas for further improvement. Ongoing research for enhancing the security features of the EBSSPA model is crucial, as cybersecurity threats are constantly evolving, and the model must adapt to more sophisticated attacks. As blockchain technology intersects with emerging regulatory frameworks, future research may assess how EBSSPA can be adapted to satisfy various legal requirements in different jurisdictions. These open research areas and future developments present exciting opportunities to build upon the groundbreaking contributions of the EBSSPA model, further advancing the field of blockchain technology and enabling its widespread adoption in diverse scenarios.

ADDITIONAL INFORMATION AND DECLARATIONS

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: A.H.: Methodology, Software, Validation, Visualization. A.P.: Validation, Writing - review & editing, Supervision, Project administration. B.D.: Formal Analysis, Resources, Writing – original draft. N.T.: Conceptualization, Methodology, Validation, Writing – original draft. S.J.: Formal analysis, Investigation, Resources, Data curation. T.M.: Formal Analysis, Writing – original draft.

Statement on the Use of Artificial Intelligence Tools: The authors declare that they didn't use artificial intelligence tools for text or other media generation in this article.

Data Availability: The data that support the findings of this study are openly available at https://www.kaggle.com/datasets/amitpimpalkar/blockchain-nts-transactions/

REFERENCES

Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, TT, Assam, M., Ghadi, Y.Y., & Muhammad, H.G. (2023). Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. *Sensors*, 23, 7740. https://doi.org/10.3390/s23187740

Alsamhi, S. H., Hawbani, A., Sahal, R., Srivastava, S., Kumar, S., Zhao, L., Al-Qaness, M. A., Hassan, J., Guizani, M., & Curry, E. (2024). Towards sustainable industry 4.0: A survey on greening IoE in 6G networks. *Ad Hoc Networks*, 165, 103610. https://doi.org/10.1016/j.adhoc.2024.103610

Alsamhi, H., Shvetsov, V., Shvetsova, V., Hawbani, A., Guizani, M., Alhartomi, A. & Ma, O. (2023). Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. *IEEE Transactions on Green Communications and Networking*, 7(1), 328–338. https://doi.org/10.1109/TGCN.2022.3195479

Arabsorkhi, A., & Ebrahimi, S. (2022). Blockchain Applications for the Police Task Force of IRI: A Conceptual Framework Using Fuzzy Delphi Method. *Journal of Information Technology Management*, 14, 36-61. https://doi.org/10.22059/jitm.2022.87840

Bagchi, P., Maheshwari, R., Bera, B., Das, A. K., Park, Y., Lorenz, P., & Yau, D. K. Y. (2023). Public Blockchain-Envisioned Security Scheme using post Quantum Lattice-Based aggregate signature for internet of Drones applications. *IEEE Transactions on Vehicular Technology*, 72(8), 10393–10408. https://doi.org/10.1109/tvt.2023.3260579

Bathula, A., Gupta, S. K., Merugu, S., Saba, L., Khanna, N. N., Laird, J. R., Sanagala, S. S., Singh, R., Garg, D., Fouda, M. M., & Suri, J. S. (2024). Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. *Artificial Intelligence Review*, 57(9), 238. https://doi.org/10.1007/s10462-024-10873-5

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N. & Shiaeles, S. (2023). Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 24(4), 3614–3637. https://doi.org/10.1109/TITS.2023.3236274

Bukola F. B., Khushboo T., Shrikant T., Shyam M. S., & Amit K. T. (2024). A blockchain-based deep learning approach for cyber security in next-generation medical cyber-physical systems. *Journal of Autonomous Intelligence*, 7(5), 1–18. https://doi.org/10.32629/jai.v7i5.1478

Cai, J., Liang, W., Li, X., Li, K., Gui, Z., & Khan, M. K. (2023). GTxChain: A Secure IoT Smart Blockchain Architecture Based on Graph Neural Network. *IEEE Internet of Things Journal*, 10(24), 21502–21514. https://doi.org/10.1109/JIOT.2023.3296469

Chen, X., Yang, A., Weng, J., Tong, Y., Huang, C., & Li, T. (2023). A Blockchain-Based Copyright Protection Scheme With Proactive Defense. *IEEE Transactions on Services Computing*, 16(4), 2316–2329. https://doi.org/10.1109/TSC.2023.3246476

Costa, L. D., Pinheiro, B., Cordeiro, W., Araújo R., & Abelém, A. (2023). Sec-Health: A Blockchain-Based Protocol for Securing Health Records. *IEEE Access*, 11, 16605–16620. https://doi.org/10.1109/ACCESS.2023.3245046

Dai, W., Liu, J., Zhou, Y., Choo, K. R., Xie, X., Zou, D., & Jin, H. (2024). PRBFPT: A Practical Redactable Blockchain Framework With a Public Trapdoor. *IEEE Transactions on Information Forensics and Security*, 19, 2425–2437. https://doi.org/10.1109/TIFS.2024.3349855

Das, D., Banerjee, S., Chatterjee, P., Ghosh U., & Biswas, U. (2023). A Secure Blockchain Enabled V2V Communication System Using Smart Contracts. *IEEE Transactions on Intelligent Transportation Systems*, 24(4), 4651–4660. https://doi.org/10.1109/TITS.2022.3226626

Duan, L., Sun, Y., Ni, W., Ding, W., Liu, J., & Wang, W. (2023). Attacks Against Cross-Chain Systems and Defense Approaches: A Contemporary Survey. *CAA Journal of Automatica Sinica*, 10(8), 1647–1667. https://doi.org/10.1109/JAS.2023.123642

Echikr, A., Yachir, A., Kerrache, C. A., Oudjida, A. K., & Sahraoui, Z. (2024). Interoperable IoRT for Healthcare: Securing Intelligent Systems with Decentralized Blockchain. *Acta Informatica Pragensia*, 13(2), 168–192. https://doi.org/10.18267/j.aip.233

Feng, Q., Yang, K., Ma, M., & He, D. (2023). Efficient Multi-Party EdDSA Signature With Identifiable Aborts and its Applications to Blockchain. *IEEE Transactions on Information Forensics and Security*, 18, 1937–1950. https://doi.org/10.1109/TIFS.2023.3256710

Haritha, T., & Anitha, A. (2023). Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System. *IEEE Access*, 11, 114322–114340. https://doi.org/10.1109/ACCESS.2023.3324740

Jiaxing, L., Jigang, W., Lin J., & Jin L. (2024). Blockchain-based public auditing with deep reinforcement learning for cloud storage. *Expert Systems With Applications*, 242, 122764. https://doi.org/10.1016/j.eswa.2023.122764

Jie, W., Qiu, W., Voundi Koe A., Li, J., Wang, Y., Wu, Y., Li, J., Zheng Z. (2024). A Secure and Flexible Blockchain-Based Offline Payment Protocol. *IEEE Transactions on Computers*, 73(2), 408–421. https://doi.org/10.1109/TC.2023.3331823

Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. *IEEE Access*, 12, 3881–3897. https://doi.org/10.1109/ACCESS.2023.3349019.

Li, W., Zhao, Z., Ma, P., Xie, Z., Palade, V., & Liu, H. (2024). Graphical Consensus-Based sharding for efficient and secure sharings in Blockchain-Enabled internet of vehicles. *IEEE Transactions on Vehicular Technology*, 73(2), 1991–2002. https://doi.org/10.1109/tvt.2023.3311445

Liu, J., Jiang, W., Sun, R., Bashir, A. K., Alshehri, M. D., Hua, Q., Yu, K. (2023). Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain. *IEEE Journal of Biomedical and Health Informatics*, 27(5), 2231–2242. https://doi.org/10.1109/JBHI.2022.3183397

Olumide, O. M., Danda, B. R., & Moses, G. (2018). Next-generation cybersecurity through a blockchain-enabled federated cloud framework. *The Journal of Supercomputing*, 74, 10, 5099–5126. https://doi.org/10.5555/3288339.3288359

Peng, G., Zhang, A., & Lin, X. (2023). Patient-Centric Fine-Grained Access Control for Electronic Medical Record Sharing With Security via Dual-Blockchain. *IEEE Transactions on Network Science and Engineering*, 10(6), 3908–3921. https://doi.org/10.1109/TNSE.2023.3276166

Puneeth, R. P., & Parthasarathy, G. (2024). Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control. *Acta Informatica Pragensia*, 13(1), 1–23. https://doi.org/10.18267/j.aip.225

Qin, H., Tan, Y., Chen, Y., Ren W., & Choo, K. (2024). TriBoDeS: A Tri-Blockchain-Based Detection and Sharing Scheme for Dangerous Road Condition Information in Internet of Vehicles. *IEEE Internet of Things Journal*, 11(2), 3563–3577. https://doi.org/10.1109/JIOT.2023.3297259

Rani, S., Babbar, H., Srivastava, G., Gadekallu T. R., & Dhiman, G. (2023). Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain. *IEEE Internet of Things Journal*, 10(7), 6074–6081. https://doi.org/10.1109/JIOT.2022.3223576

Rao, P. M., Jangirala, S., Pedada, S., Das A. K., Park, Y. (2023). Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges. *IEEE Access*, 11, 54476–54494. https://doi.org/10.1109/ACCESS.2023.3281844

Samuel, O., Omojo, A.B., Onuja, A.M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez. G., Yahaya, A.S., Fatoba, O.J., & Shamshirband, S. (2023). IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain. *IEEE Journal of Biomed Health Information*, 27(2), 823–834. https://doi.org/10.1109/JBHI.2022.3143576

Saraswat, B. K., Saxena, A., & Vashist, P. C. (2024). Machine learning for effective EHR management in blockchain-cloud integration. *Journal of Autonomous Intelligence*, 7(4), 1–15. https://doi.org/10.32629/jai.v7i4.1274

Tandon, R., Verma, A., & Gupta, P. (2024). D-BLAC: A dual blockchain-based decentralized architecture for authentication and communication in VANET. *Expert Systems With Applications*, 237, 121461. https://doi.org/10.1016/j.eswa.2023.121461

Vidal, F. R., Gouveia, F., & Soares, C. (2022). Analysis of Revocation Mechanisms for Blockchain Applications and a Proposed Model Based in Self-Sovereign Identity. *Journal of Information Technology Management*, 14, 192–210. https://doi.org/10.22059/jitm.2022.87848

Wang, Z., Chen, Q., & Liu, L. (2023). Permissioned Blockchain-Based Secure and Privacy-Preserving Data Sharing Protocol. *IEEE Internet of Things Journal*, 10(12), 10698–10707. https://doi.org/10.1109/jiot.2023.3242959

Xie, H., Zheng, J., He, T., Wei, S., Shan, C., & Hu, C. (2023). B-UAVM: A Blockchain-Supported Secure Multi-UAV Task Management Scheme. *IEEE Internet of Things Journal*, 10(24), 21240–21253. https://doi.org/10.1109/JIOT.2023.3279923

Xu, Y., Xu, G., Liu, Y., Liu, Y., & Shen, M. (2024). A survey of the fusion of traditional data security technology and blockchain. *Expert Systems With Applications,* 252, 124151. https://doi.org/10.1016/j.eswa.2024.124151

Zhang, J., Jiang, Y., Cui, J., He, D., Bolodurina, I. & Zhong, H. (2024). DBCPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 23(2), 1127–1141. https://doi.org/10.1109/TMC.2022.3230853

Zhang, Y., Ma, Z., Luo S., & Duan, P. (2024). Dynamic Trust-Based Redactable Blockchain Supporting Update and Traceability. *IEEE Transactions on Information Forensics and Security*, 19, 821–834. https://doi.org/10.1109/TIFS.2023.3326379

Zhou, Z., Wan, Y., Cui, Q., Yu, K., Mumtaz, S., Yang, C., & Guizani, M. (2024). Blockchain-Based Secure and Efficient Secret Image Sharing With Outsourcing Computation in Wireless Networks. *IEEE Transactions on Wireless Communications*, 23(1), 423–435. https://doi.org/10.1109/TWC.2023.3278108

Zukaib, U., Cui, X., Hassan, M., Harris, S., Hadi, H. J., & Zheng, C. (2023). Blockchain and Machine Learning in EHR Security: A Systematic Review. *IEEE Access*, 11, 130230–130256. https://doi.org/10.1109/ACCESS.2023.3333229

Acta Informatica Pragensia is published by the Prague University of Economics and Business, Czech Republic | eISSN: 1805-4951