SCIENTIFIC Publishing Limited

Digital Technologies Research and Applications

http://ojs.ukscip.com/index.php/dtra

Article

A Blockchain-Enhanced Deep Learning Approach for Intrusion Detection in Trusted Execution Environments

Ahmed Abubakar Aliyu [1,*], Mohammed Ibrahim [1] and Sa'adatu Abdulkadir [1,2]

[1] Department of Secure Computing, Faculty of Computing, Kaduna State University, Kaduna 800283, Nigeria

[2] Department of Informatics, Faculty of Computing, Kaduna State University, Kaduna 800283, Nigeria

[*] Correspondence: ahmed.aliyu@kasu.edu.ng

Received: 9 January 2025; **Revised:** 21 February 2025; **Accepted:** 1 March 2025; **Published:** 8 March 2025

Abstract: Traditional Intrusion Detection Systems (IDSs) face significant challenges in keeping pace with the rapidly evolving landscape of cyber threats, primarily due to limitations in continuous learning and the accuracy of data classification and analysis. This often results in delayed detection and leaves networks susceptible to severe attacks. This paper introduces an innovative IDS empowered by blockchain technology to mitigate these shortcomings, leveraging continuous learning and self-adaptive neural networks. The proposed system adopts a proactive approach by continuously assimilating intrusion logs, utilizing a Long Short-Term Memory (LSTM) core to discern patterns and enhance its real-time threat detection capabilities, removing a major bottleneck in traditional IDS models by eliminating the need for manual tagging. To further strengthen the security measures, self-updating neural networks are embedded in each block of the blockchain, forming a decentralized "brain" that evolves defences against even the most sophisticated adversaries. These networks are securely housed in Trusted Execution Environments (TEEs) to maintain operational integrity, enabling tamper-proof operation and effective threat detection. Real-world evaluations conducted on the Binance Smart Chain and Ethereum Classic datasets demonstrate the system's superior performance. With an impressive accuracy rate of 98.50% and a minimal false positive rate of 1.50%, the model demonstrates a remarkable ability to distinguish legitimate network activity from malicious intrusions.

Keywords: Neural Network; Intrusion Detection System; Blockchain; Deep Learning

1. Introduction

In the wake of the digital revolution, automation, and interconnected systems have become integral parts of modern infrastructure, necessitating robust security measures to safeguard against cyber threats. Despite the numerous benefits brought forth by these advancements, cybercriminals are continuously evolving their intrusion techniques, posing significant risks to organizations and individuals alike [1]. The prevalence of cybersecurity threats, ranging from unauthorized access to data breaches and network intrusions, underscores the critical need for effective Intrusion Detection Systems (IDS) to maintain security [2]. In response to these challenges, researchers and practitioners have been exploring innovative approaches to enhance the detection and prevention of intrusions [3].

Recent studies have proposed novel techniques, such as Min-Max Game Theory Optimized Artificial Neural Networks and Distributed Multi-Agent Intrusion Detection and Prevention Systems, to address the limitations of traditional IDS [4, 5]. However, one emerging technology that holds immense promise in bolstering cybersecu-

rity measures is blockchain. Initially introduced as the underlying technology for cryptocurrencies, blockchain has evolved to offer much more than just financial transactions [6]. Its decentralized and immutable nature makes it well-suited for securing various domains, including IDS. For instance, recent research has introduced blockchain-based IDS systems, such as the African Buffalo system, which utilizes Recurrent Neural Networks (RNNs) trained on both regular and malicious user data to enhance security [7]. These systems ensure data privacy through identity-based encryption and securely store encrypted data on a cloud-based blockchain. The integration of RNNs enables the detection of security breaches within cloud environments, while optimization techniques continuously monitor for potential intrusions, adding an extra layer of protection.

This study explores the potential of deep learning and ensemble methods to further enhance IDS capabilities [8]. Although traditional methods struggle with novel attacks, deep learning models, particularly RNNs and Convolutional Neural Networks (CNNs), excel at analysing raw network traffic and identifying complex patterns indicative of malicious activity. However, challenges such as computational complexity and overfitting persist. Ensemble methods offer a solution by combining different algorithms, achieving improved accuracy and robustness, especially when incorporating CNNs for spatial feature extraction and RNNs for temporal analysis. Nevertheless, challenges remain in interpreting the decision-making processes of deep learning models and ensuring continuous adaptation to evolving cyber threats. In this paper, we propose a novel approach that harnesses the power of deep learning while leveraging the inherent security features of blockchain technology. Our goal is to create a robust IDS that can detect and mitigate network intrusions in real-time by integrating these technologies.

1.1. Contributions of the Study

Our study significantly advances traditional IDS by proposing a novel continuous learning model designed to enhance the detection of normal, malicious, and suspicious activities. This approach not only facilitates early intrusion detection but also minimizes the impact of potential threats, overcoming the limitations of static IDS solutions [9]. The study also ensures robust privacy and security, safeguarding sensitive data against evolving cyber threats by leveraging TEE.

A key innovation of our model lies in its adaptive nature - it continuously learns from historical intrusion data, updating the neural network nodes in each blockchain block through incremental training. This continuous learning mechanism enables our system to stay ahead of emerging threats, ensuring its effectiveness over time.

Our model provides several critical advantages:

- Ensures sensitive data remains confidential and protected against unauthorized access.
- Strengthens defense mechanisms, offering robust protection against a wide range of cyber threats.
- Boosts data processing capabilities and improves the overall performance of the IDS.
- Designed to seamlessly scale, enabling deployment across large, distributed networks without compromising performance.

These benefits are realized through a combination of LSTM networks (RNN-CNN hybrid) for efficient information retention and a distributed consensus mechanism facilitated by blockchain for scalability. The integration of these cutting-edge technologies ensures that the system not only detects intrusions with high accuracy but also maintains efficiency and security in large-scale environments.

In this paper, we present the methodology, architecture, and implementation of our proposed model, along with experimental results that validate its effectiveness. We will also discuss potential challenges and limitations of our approach. Through this work, we aim to make a significant contribution to the ongoing efforts to reinforce cybersecurity in the face of rapidly evolving threats by combining the strengths of deep learning and blockchain technologies in a novel and impactful way.

2. Related Literature

Past researchers in the field have explored various strategies to develop smart IDS. One such strategy that has been adopted is the application of Machine/Deep learning on Smart Grid systems [10]. In this approach, the intrusion detection mechanism operates within a software-defined network, which decouples data planes to monitor and manage the communication network autonomously. However, a significant drawback of relying solely on software detection systems is their susceptibility to high variance and bias in detection [11]. Therefore, an ideal

detection system should exhibit flexibility to accommodate a wide range of anomalies and minimize variance in its results.

Furthermore, to address cybersecurity concerns, the Multi-Zone-Wise Blockchain model (MZWB) has emerged as a viable solution [12]. This method capitalizes on blockchain's capability to integrate seamlessly with the Internet of Things (IoT). The intrusion detection process in MZWB involves two steps: firstly, an analysis of data using a Deep Convolutional Neural Network to classify information as normal, suspicious, or malicious; secondly, the use of Generative Adversarial Networks to classify data as either normal or malicious, facilitating the reconstruction and mitigation of severe attacks. Additionally, the Improved Monkey Optimization technique is employed to recover lost data.

The exploration of information sharing among various IoT nodes to improve malware detection emerges as another significant theme in related research. A study by Putra et al. [13] introduced Collaborative-IDS (CIDS), wherein blockchain serves as a decentralized platform enabling CIDS nodes to exchange malware information and trigger alarms within the system. A critical challenge in such endeavours lies in ensuring the trustworthiness of shared information, particularly in sensitive sectors like medical smartphones [14]. Leveraging blockchain as a distributed ledger technology addresses this challenge by offering unique features such as immutability, ensuring that once data is added to a blockchain, it cannot be altered or deleted without consensus from the majority of network participants [15]. This characteristic renders blockchain an ideal platform for storing and sharing tamper-proof information. Additionally, blockchain's transparency, wherein all transactions are publicly visible, mitigates the risk of fraud or collusion, fostering trust among CIDS nodes even in the absence of direct familiarity or trust between them. Furthermore, blockchain's decentralized nature, not controlled by a single entity, enhances resistance to attack and manipulation. They also facilitate the implementation of specific mechanisms within CIDS to ensure information trustworthiness, including node identity verification, signature verification for intrusion detection alerts, and maintenance of a reputation system for nodes to identify and avoid those with a history of sharing false information [16]. Consequently, the imperative for new developers lies in guaranteeing the reliability of shared data.

In a separate study [17], researchers proposed an Artificial Intelligence (AI)-aligned advanced persistent threat detection system, yielding a significant increase in trust. However, concerns regarding the sustainability and cost of implementing such systems for small enterprises may arise. Similarly, considerable research has been undertaken recently on the integration of IDS with neural networks and blockchain technologies [18]. For instance, a recent study [19] introduced the Blockchain-based Hybrid IDS (BC-HyIDS), which employs blockchain technology for signature exchange among nodes in distributed IDS. Operating in three stages, BC-HyIDS utilizes both detection techniques in the initial phases before incorporating blockchain in the final stage, thereby enhancing security through data encryption within blocks using a cryptosystem. Implemented using Hyperledger Fabric v2.0 and Hyperledger Sawtooth, BC-HyIDS features a prototype blockchain framework built on distributed ledger technology to facilitate secure signature exchange. Additionally, researchers [20] have proposed an IDS leveraging blockchain technology, indirect trust, and the Viterbi algorithm to bolster security standards for the Industrial Internet of Things (IIoT). Integrating blockchain with Viterbi and indirect methods ensures system transparency, enabling assessment of malicious activity probability throughout IIoT product creation, recording, and delivery. Similarly, other researchers [21] have introduced a blockchain-based radial basis function neural network model to enhance Internet of Drones (IoD) network performance. This approach targets improved data storage and integrity for informed decision-making across various IoD contexts. Furthermore, discussions encompass efficient implementation and sharing of decentralized deep learning techniques, along with blockchain's role in facilitating decentralized predictive analytics.

A recent study [22] introduces an IDS for IoT urban data based on blockchain technology, designed to safeguard devices from Distributed Denial of Service (DDoS) attacks. Utilizing lightweight technology, it secures key pairs of IoT devices using the Arbiter PUF architecture. Initially, a machine learning-based ensemble technique is employed by the collaborative detection system to identify DDoS attacks on IoT devices, boasting a lower false positive rate and higher detection rate compared to alternative classification techniques. Subsequently, a blockchain system is integrated to securely distribute alert notifications to each node within the IoT network. Similarly, another study [23] proposes PRO-DLBIDCPS, a novel approach for intrusion detection in cyber-physical system environments, leveraging blockchain technology and deep learning. PRO-DLBIDCPS utilizes the Adaptive Harmony Search Algorithm to select crucial features for intrusion detection and employs an attention-based bidirectional gated recurrent neural

network (ABi-GRNN) model to classify features and detect intrusions. Further enhancing detection performance, a hyperparameter optimizer based on the Poor and Rich Optimization algorithm is utilized. Blockchain technology is then leveraged to enhance the security of the cyber-physical system environment. Additionally, researchers have proposed a blockchain-assisted framework to enhance intrusion detection and prevention for IoT smart farms, utilizing the AWS Lambda mechanism and blockchain technology smart contracts to deliver intrusion alerts to farmers in real-time [24].

In another recent study [25], a blockchain-assisted deep learning framework is proposed for privacy-protected cooperative intelligent transport systems. This framework incorporates LSTM, Autoencoder, Attention-based RNN, and Truncated Backpropagation through Time algorithms to ensure data security. A dedicated blockchain module is developed to securely transport data across the system, employing an enhanced Proof of Work (PoW) approach based on smart contracts to verify data integrity and mitigate the risk of data poisoning.

Our study is distinguished from previous research in several key respects. For instance, while previous studies have examined various strategies for developing IDS, such as applying machine/deep learning to smart grid systems or utilizing multi-zone-wise blockchain models, our study introduces an innovative IDS empowered by blockchain technology to address the limitations of traditional IDSs. In contrast to other approaches, our IDS employs continuous learning and self-adaptive neural networks, enabling real-time threat detection without the necessity for manual tagging. Furthermore, our system integrates self-updating neural networks, securely housed in Trusted Execution Environments within each block of the blockchain, forming a decentralized "brain" to evolve defences against sophisticated adversaries while maintaining operational integrity. **Table 1** provides a summary of the findings from related research.

Table 1. Summary of the related work.

Year	Author(s)	Aim of the Paper/Contribution	NN-Based	Classification Approach/Algorithm	Blockchain-Based	Datasets
2023	Abubakar et al. [9]	A novel blockchain-based technique that improves the accuracy of IDS	√	Ensemble Learning Algorithms	√	DARPA99 and MIT Lincoln Lab
2022	Houda et al. [10]	A novel framework that leverages ensemble learning to efficiently detect and mitigate security threats in SDN-based systems.	√	Boosting Feature Selection,	X	NSL-KDD and UNSW-NB15
2022	Janani et al. [26]	IoT routing attack detection and classification model	√	LSTM, Adaptive Mayfly Optimization Algorithm	X	
2023	Kably et al. [12]	A Multi-Zone-Wise Blockchain model.	√		√	
2021	Putra et al. [13]	A decentralized CIDS that emphasizes the importance of building trust between CIDS nodes.	X	Weighted Majority	√	Private
2022	Zheng et al. [27]	Blockchain-based IoT key agreement and authentication schemes using multi-TA network model.	X	Elliptic Curve Encryption Algorithm	√	None
2023	Rahman et al. [17]	An APT detection system based on blockchain and artificial intelligence.	√	DTL-ResNet	√	Private
2022	Khonde et al. [19]	A novel blockchain framework for inter-node signature exchange in distributed IDS.	X	Isolation Random Forest, XGBoost	√	CIC-IDS 2017
2022	Rathee et al. [20]	An IDS that uses the Viterbi algorithm, indirect trust, and blockchain mechanism for Industrial IoT.	X	Viterbi	√	Private
2023	Heidari et al. [21]	A blockchain-based radial basis function neural network model.	√	Radial Basis Function	√	UNSW-NB15, NSL-KDD, CICDDOS2019,CICIDS2017 and AWID
2022	Babu et al. [22]	A permission-based blockchain system that uses the arbiter PUF model to secure the key pairs of IoT devices using lightweight technology.	X	Decision Tree, Random Forest, SVM	√	CICDDoS2019
2022	Kumar et al. [28]	A secure data dissemination system for IoT-based e-health systems using AI and blockchain.	√	LSTM, Multi-Layer Perceptrons	√	ToN-IoT dataset

Table 1. *Cont.*

Year	Author(s)	Aim of the Paper/Contribution	NN-Based	Classification Approach/Algorithm	Blockchain-Based	Datasets
2023	Aljabri et al. [29]	A blockchain-based IDS model based on CNN that protects network traffic data	√	SHA-256 hashing algorithm, Greedy-based genetic algorithm	√	Private
2021	Kumar et al. [30]	A hybrid feature-reduced intelligent cyber-attack detection system for IoT networks.	X	RandomForest,	X	NSL-KDD, BoT-IoT and DS2OS
2022	Mansour et al. [23]	A deep learning model for blockchain-enabled intrusion detection in CPS environment.	√	Attention-based Bi-Directional Gated RNN, Poor and rich optimization	√	NSL-KDD 2015 and CICIDS 2017
2023	Aliyu et al. [24]	A blockchain-based smart farm security framework for IoT.	X	SVM	√	Private
2021	Kumar et al. [25]	A secure framework based on privacy protection using blockchain-enabled deep learning in a cooperative intelligent transport system.	√	LSTM, Autoencoder, A-RNN, BPTT	√	ToN-IoT and CICIDS-2017
2022	Kumar et al. [31]	An integrated framework for decentralized data processing and learning in IIoT networks, using blockchain and deep learning.	√	LSTM-Sparse AutoEncoder, Multi-Head Self-Attention-based Bidirectional Gated Recurrent Unit	√	CICIDS-2017 and ToN-IoT
2023	Kumar et al. [32]	A deep learning technique using blockchain for secure data transfer in an IoT-enabled healthcare system.	√	Autoencoder, Bidirectional LSTM	√	CICIDS-2017 and ToN-IoT
2023	Kumar et al. [33]	A new variational autoencoder and attention-based gated recurrent unit-based IDS for zero-touch networks.	√	Variational Autoencoder, Attention-Based Gated Recurrent Units	√	ToN-IoT and IoJ-Botnct
2022	Kumar et al. [34]	A secure communication framework for the network of unmanned aerial vehicles using blockchain.	X	Proof-of-Authority, Round-based Aura	√	None
2023	Our proposal	A blockchain-based IDS model to increase the accuracy of malicious attack detection using deep learning.	√	LSTM, RNN, Autoencoder,	√	Binance Smart Chain (BSC) and Ethereum Classic (ETC)

Prior research in this domain has pursued diverse objectives, all with a shared emphasis on pioneering novel and innovative IDS solutions. Some studies endeavour to create neural network-based IDS models capable of discerning malicious attacks with heightened accuracy, efficiency, security, and reliability compared to conventional IDS models. Others centre on crafting hybrid IDS models that harness the combined strengths of neural networks and blockchain technologies. While the majority of cited works concentrate on tailoring IDS models to specific network types and applications, such as cloud computing networks, smart grid networks, and IIoT networks, none have delved into the realm of incremental training for blockchain-based IDSs. Additionally, none of the proposed solutions undergo evaluation using blockchain-based datasets such as the BSC and ETC.

3. Proposed Method

To enhance the accuracy of blockchain-based IDS, the current study proposes combining machine learning and a secure distributed ledger implemented by blockchain to safeguard the communications between nodes. The raw alert data generated by monitors is then kept in the blockchain. The data is then replicated among all the connected nodes of the network displaying the nature of the actual data such as bloom filters or alert hashes. Consecutively, there is pre-processing of the logs and classification as either normal or malicious. Moreover, the nodes run a validity test to ensure that the transactions are credible before addition to the next block. The harvested datasets are then compared and summarized using a specific criterion to evaluate consistency. The information is then memorized by the machine to aid in future detection systems. Notably, the collection and processing of data is decentralized to achieve better scalability. Here is more detail on the methodology and architecture of our approach:

Data Collection: The first step in building the IDS is to collect and pre-process network data. This data can include network traffic logs, packet captures, and other relevant information. The dataset should include both normal and malicious network behaviour to effectively train the neural network.

Train the neural network: A neural network is trained using the collected dataset to learn patterns and characteristics of normal network behaviour. Various deep learning architectures, such as CNNs or RNNs, can be used to analyse the network data and extract meaningful features.

Anomaly detection: Once the neural network is trained, it can be used to detect anomalies in network traffic. During the inference phase, the network analyses incoming data and identifies deviations from normal behaviour. Anomalies can indicate potential network intrusions or security breaches.

Intrusion reporting: Detected anomalies are reported to the blockchain network. Each reported intrusion is recorded as a transaction on the blockchain, providing an immutable and transparent history of detected security incidents. The transaction can include relevant information such as the type of intrusion, timestamp, and any additional metadata.

Consensus and validation: The blockchain network's consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensures agreement among network participants on the validity of reported intrusions. Consensus algorithms prevent malicious actors from tampering with the blockchain and provide a trust mechanism for the recorded data. In this experiment, we used a hybrid of Delegated PoS (DPoS) and PoS consensus mechanisms to achieve improved decentralization while reducing the risk of collusion by allowing users to delegate their participation to multiple delegates.

Distributed storage and auditing: The blockchain network stores intrusion data in a decentralized manner across multiple nodes. This distributed storage provides redundancy and eliminates a single point of failure. Security analysts and auditors can access the blockchain to review and analyse recorded intrusions, aiding in forensic investigations and attribution. **Figure 1** illustrates the techniques employed in the proposed model's activity flow, while **Figure 2** presents the architecture, which primarily comprises blockchain-based system components.

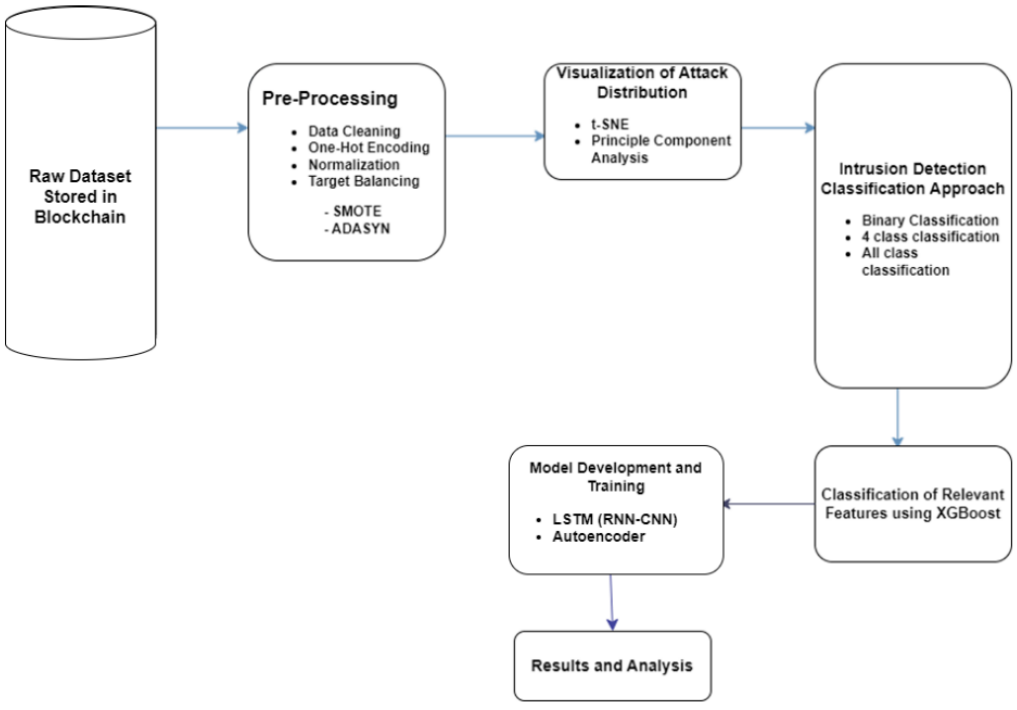

Figure 1. Our blockchain-based model.

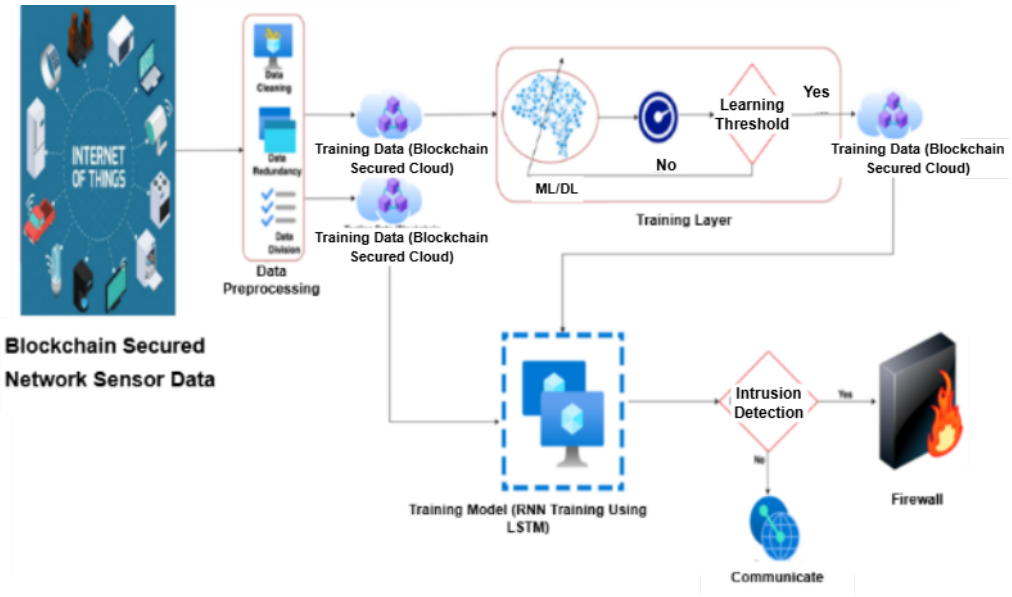

Figure 2. The blockchain-based system architecture.

Data Collection Module

This is responsible for collecting network data from various network sensors and saving it in the blockchain. The collected data is then pre-processed and prepared for input to the neural network. Some of the common pre-processing techniques used in this module include data filtering or data cleaning, feature extraction which is done using machine learning algorithms, and normalization as seen in **Figure 1**.

Neural Network Module

This contains the trained neural network responsible for analysing the network data and detecting anomalies. It extracts relevant features, applies machine learning algorithms, and classifies network behaviour as normal or malicious. The neural network is trained on a dataset of labelled network traffic data containing both normal and malicious traffic. The neural network learns to identify the patterns in the data that are associated with malicious traffic. Once trained, it can be used to analyse new network traffic data and detect anomalies. The neural network also outputs a probability score for each network packet, indicating the probability that the packet is malicious.

Intrusion reporting module

When an anomaly is detected, this module reports the intrusion to the blockchain network. It creates a transaction with relevant intrusion details and sends it to the blockchain network for validation and recording. The intrusion report includes the following information:

- Time and date of the intrusion
- Source and destination IP addresses
- Port numbers
- Type of attack
- Severity of the attack
- Blockchain Network

The blockchain network consists of multiple nodes that maintain a distributed ledger of intrusion records, using DPoS-PoS to validate and reconcile reported intrusions. The blockchain network ensures immutability, transparency, and tamper-proof storage of intrusion data. When an intrusion report is submitted to the blockchain network, each node validates the report. If the report is valid, it is added to the blockchain ledger. Once an intrusion report is added to the blockchain ledger, it cannot be modified or deleted. This ensures the immutability of the

data.

Audit and Analysis Module

The Audit and Analysis Module allows authorized users, such as security analysts or auditors, to access the blockchain network and review recorded intrusion data through an API. It provides tools for pattern analysis, incident investigation, and forensic analysis. Security analysts can use the audit and analysis module to identify trends in intrusion data which can be used to improve the organization's security posture. In addition, auditors can use this module to ensure that the organization is compliant with security regulations while forensic analysts can use it to investigate security incidents, identify the root cause of the incident, and recommend remediation. These elements work together to create an architecture that combines the security and transparency of blockchain technology with neural network-based anomaly detection. The blockchain serves as a secure and immutable record-keeping mechanism for identified intrusions, with the neural network serving as the primary detection engine as shown in **Figure 2**.

The competence evaluation of an IDS is complexly tied to the challenge of sourcing relevant data for analysis. Despite the fact that network monitoring provides indispensable insights, obtaining suitable datasets for experimentation presents a formidable obstacle due to the prohibitive costs associated with data collection [35], forcing developers to observe their network systems often resort to utilizing available datasets to expedite model development. One common approach involves monitoring network traffic on a production network using tools like packet sniffers and network flow analysers. This gathered data forms the basis for constructing a profile of normal network behaviour, which is then utilized to train the IDS model to detect anomalous activity. Alternatively, synthetic network traffic datasets offer another avenue for experimentation. In our case, we employed such datasets in our experiment, training our proposed model on typical network traffic patterns extracted from the BSC and ETC networks. ETC, being a distributed computing platform built on a free blockchain, provides valuable insights into network system assaults, making it an ideal candidate for our study [36]. On the other hand, the BSC dataset offers a comprehensive and rapidly growing record of transactions on the Binance platform, making it suitable for training an IDS capable of detecting a wide range of attacks in real time.

The integration of the LSTM models within the IDS architecture is pivotal for capturing long-term dependencies in sequential data. The LSTM layer, serving as the core component of the model, employs specialized gates (input, output, forget) to regulate information flow and memory retention [37]. Activation functions, such as the hyperbolic tangent (tanh), introduce non-linearity and control information flow within each LSTM unit. The formula for the hyperbolic tangent function is:

$$\tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} \tag{1}$$

Where:

- e is the base of the natural logarithm, approximately equal to 2.71828.
- x is the input value to the tanh function.

This equation represents the ratio of the difference of two exponential values to their sum. When x is positive, e^{x} dominates the expression, leading to a value close to 1. When x is negative, e^{-x} dominates, resulting in a value close to –1. Therefore, the tanh function outputs values between –1 and 1, mapping any real-valued input to the range (–1, 1). The output layer, receiving processed features from the LSTM layer, generates final classifications or predictions using techniques like softmax or sigmoid activation functions. To update the cell state in the LSTM cell, we use:

$$s_t = f_t \odot s_t{-}1 + i_t \odot tanh(W_{xi}x_t + W_{hi}h_{t-1} + b_i) \tag{2}$$

Where:

s_t is the cell state at time step *t.*
f_t is the forget gate output at time step *t.*
i_t is the input gate output at time step *t.*
x_t is the input at time step t
h_{t-1} is the hidden state of the previous time step.

W_{xi} and W_{hi} are weight matrices for the input and hidden state, respectively.
b_i is the bias vector.
The calculation of the output gate activation in an LSTM cell at time step t is:

$$o_t = tanh\,(s_t) \tag{3}$$

Where o_t is the output gate activation at time step t and *tanh* is the hyperbolic tangent function, which squashes the input values between –1 and 1. **Figure 3** shows the neural network attack structure [38].

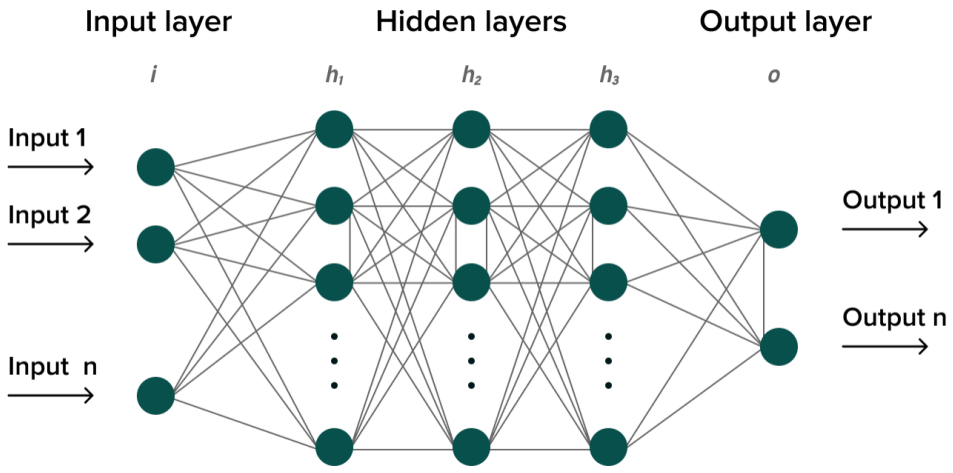

Figure 3. Neural networks attack structure.

Blockchain technology plays a crucial role in facilitating decentralized storage, tamper-proof audit trails, and validation mechanisms for intrusion reports within the IDS architecture. Blockchain nodes store and validate intrusion reports submitted by the IDS system, ensuring transparent and immutable records of security incidents. However, integration introduces latency due to consensus processes, impacting real-time intrusion detection and response. Optimization techniques, including efficient block validation algorithms and distributed storage mechanisms such as Distributed Hash Tables (DHT), can mitigate latency issues [39].

Despite the effectiveness of LSTM models, challenges such as vanishing gradients and computational expense persist [40]. To address these challenges, simpler Autoencoder architectures have been developed, offering faster training and recalling long sequence connections with minimal memory overhead. This underscores the importance of considering computational costs, data pre-processing, and hyper-parameter tuning in designing effective IDS architectures.

3.1. Preliminary Processing

The preliminary processing phase encompasses planning, training, and expert testing to effectively reduce the volume of data without compromising critical information. This step is essential for optimizing subsequent analysis. The objectives of this pre-processing phase include:

1. Providing more accurate and reliable computing data for the IDS.
2. Minimizing the occurrence of error messages and false alarms while enhancing the system's detection capabilities.
3. Identifying patterns of attack and offering administrators relevant data types to facilitate informed decision-making.

During the initial stages of pre-processing, several key features are often generated, including average block size, average gas consumption, number of block transactions, average transaction characteristics, total gas expen-

diture, and transaction value. These features contribute significantly to the effectiveness of intrusion detection processes. For instance, they enable the IDS to discern abnormal patterns in network activity and identify potential security threats promptly. Additionally, **Tables 2** and **3** provide a detailed breakdown of the information contained within each intrusion transaction recorded on the blockchain, including associated metadata. This information is instrumental in understanding the nature and context of security incidents, further enhancing the IDS's ability to detect and respond to threats effectively. Overall, this pre-processing methodology aims to optimize the IDS's performance by streamlining data processing and extracting meaningful insights from the available information.

Table 2. Processes of some intrusion detection features.

Feature	Normal	Potential Attack	Description
Block size	Normal size	DoS attack (large data or complex transactions)	A sudden increase in block size could indicate a DoS attack designed to overwhelm the network with large amounts of data or hide malicious activity within complex transactions. Attackers can also spam the network with small transactions to inflate the block size and slow down processing.
Gas supply	Increased network activity (normal or attack)	DoS attack (high gas prices)	A high gas supply can indicate increased network activity, which may be normal or a sign of an attack. Hackers can manipulate the gas supply to drive up prices and make it expensive for legitimate users to conduct transactions.
Block complexity	Normal	Overload attack (complex smart contracts or mining)	Sudden increases in block complexity could indicate an attack designed to overload the network with complex smart contracts or resource-intensive mining.
Average transactions per block	Normal	Network partitioning (isolated nodes)	A significant drop in this value could indicate network partitioning, where parts of the network are no longer communicating with each other. This can allow attackers to exploit isolated groups of nodes.
Gas consumption and transaction volume	Normal	Money laundering or other financial crimes	High gas usage and large transaction amounts can be indicators of money laundering or other financial crimes.

Table 3. Intrusion transaction and associated metadata.

Metadata Field	Description
Transaction Hash	Unique identifier for transaction
Timestamp	Transaction time
Source Address	Originating account address
Destination Address	Targeted account address
Transaction Amount	Amount of cryptocurrency involved
Attack Type	Intrusion type (DoS, account compromise, etc.)
Attack Vector	Intrusion execution method
Attacker Signature	Attacker's unique pattern
Attack Payload	Data or code used to carry out intrusion
Forensic Evidence	Logs and traces generated during intrusion

In neural modelling, a series of standardized procedures is implemented to ensure data stability and reduce variability. These steps are essential for eliminating the influence of seasonal, periodic, and statistical trends, which can distort the analysis. Data standardization plays a pivotal role in preparing datasets for neural networks, as these models are highly sensitive to the scale of input data. Failure to standardize input data can lead to issues such as overfitting or the learning of irrelevant features by the neural network. *Z-score* normalization is a commonly employed technique for standardization, as it centres the data by subtracting the mean and scales it by dividing it by the standard deviation. Within the context of neural modelling, a division motion ratio is utilized during data normalization. This ratio quantifies the difference between the current data point and the mean of the dataset, which is then divided by the standard deviation. These standardized approaches ensure that input data is appropriately

scaled and centred, facilitating effective neural network training and analysis. The *Z-score* is given:

$$Z = \frac{(X - \mu)}{\sigma} \tag{4}$$

Where:

Z is the normalized data point.
X is the current data point.
μ is the mean of the data.
σ is the standard deviation of the data.

4. Test and Results Analysis

The model systematically categorized incoming system logs as malicious, suspicious, or normal, ensuring continuous classification to maintain a comprehensive memory of various system attacks. Leveraging advanced IDS capabilities as noted in Maseno, Wang and Xing's study [41], the model's effectiveness is inherently tied to the volume and accuracy of data collected and classified. Utilizing the immutable BSC and ETC datasets processed with PyTorch, 80% of the data was dedicated to training the model, with the remaining 20% allocated for testing to assess its generalization capacity beyond the training data. Using pre-processed data, the IDS effectively discerned unusual blockchain network activity, distinguishing between benign and malicious data. Experimental findings on historical logs demonstrated the model's efficacy in identifying a spectrum of intrusions, encompassing DoS attacks, account compromises, and smart contract exploits [42].

The initial stages of data pre-processing generated a subset of key daily characteristics, such as average block size, gas supply, block complexity, transactions per block, total gas consumption, and transaction amount, crucial for gauging network activity. Notably, anomalies in these metrics, like sudden fluctuations, signalled potential threats, enabling the model to flag instances of suspicious behaviour. Access to blockchain data through APIs facilitated forensic analysis, empowering security analysts to trace attack origins, assess impacts, and recover assets. Utilizing Rectified Linear Unit (ReLU) optimization for prediction time, the model harnessed computational efficiency, characterized by a single comparison operation, thus accelerating computations compared to traditional activation functions like sigmoid or tanh [43]. This computational efficiency is paramount for real-time prediction, especially within the demanding context of a blockchain-based neural network-integrated IDS. Additionally, ReLU's introduction of sparsity and non-negative outputs enhances its suitability for tasks like anomaly detection and intrusion scoring in neural network-integrated IDS environments [44]. It can be calculated:

$$f\,(x) = max(0, x) \tag{5}$$

Where:

x is the input of the activation function.
$f(x)$ is the output of the activation function.

The model's ability to learn from historical logs signifies a significant advantage, eliminating the need for manual labelling of vast datasets - a common challenge in traditional machine learning-based IDS. Consequently, the presented results underscore the potential of the proposed blockchain-based intrusion detection model as a valuable asset for safeguarding blockchain networks against diverse attacks. Upon examining **Figures 4–9**, it becomes evident that the 51 percent attack led to numerous ETC-related companies suspending their operations [45]. Our analysis suggests that the current block size and associated characteristics may not be adequate for detecting certain types of blockchain attacks promptly. However, we posit that integrating data from additional sources, such as the server operating system and application, could enhance the efficacy of our detection method. Consequently, the blockchain experienced a decrease in recorded transactions during the attack.

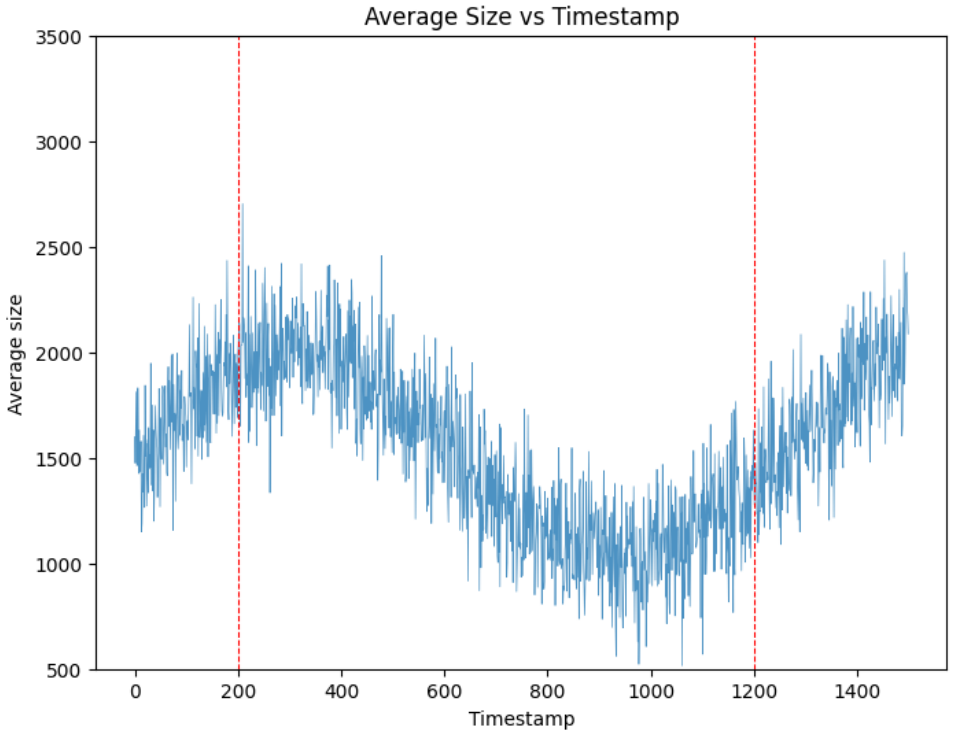

Figure 4. Block average size.

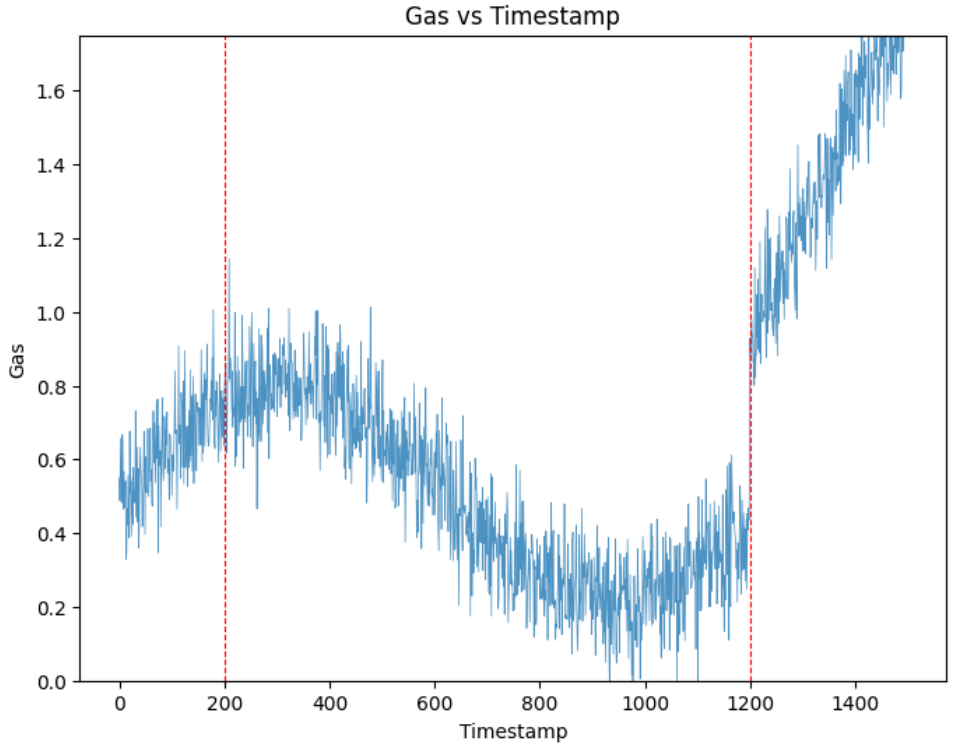

Figure 5. Supplied gas average.

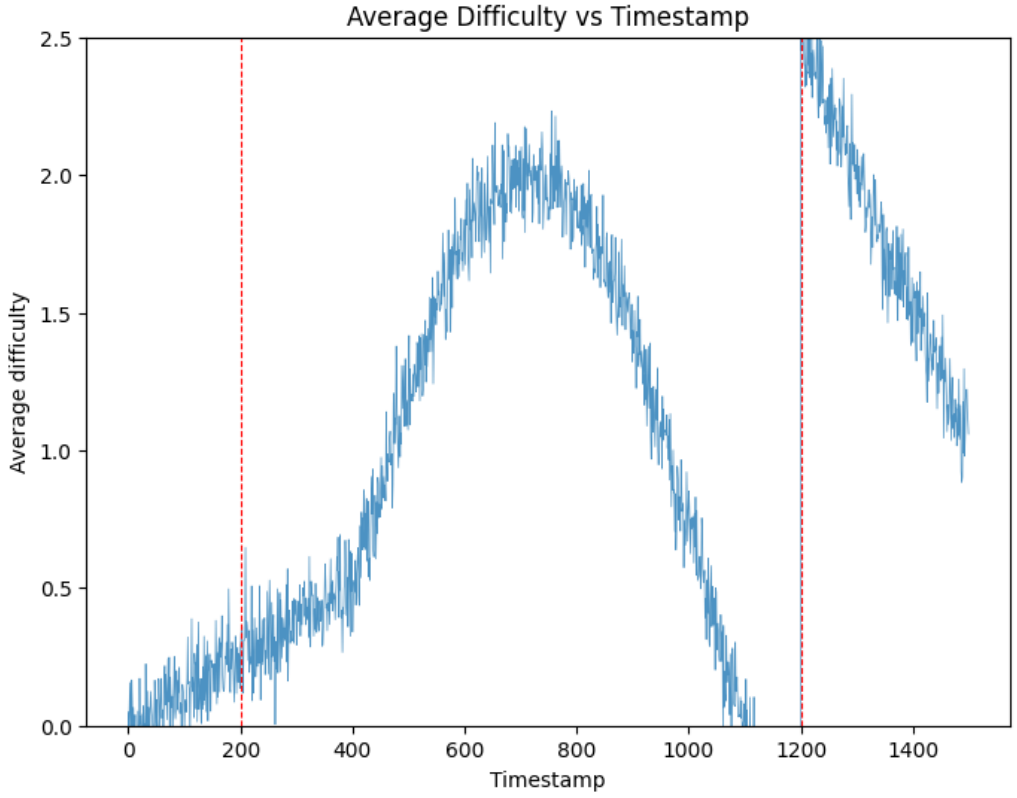

Figure 6. Average block difficulty.

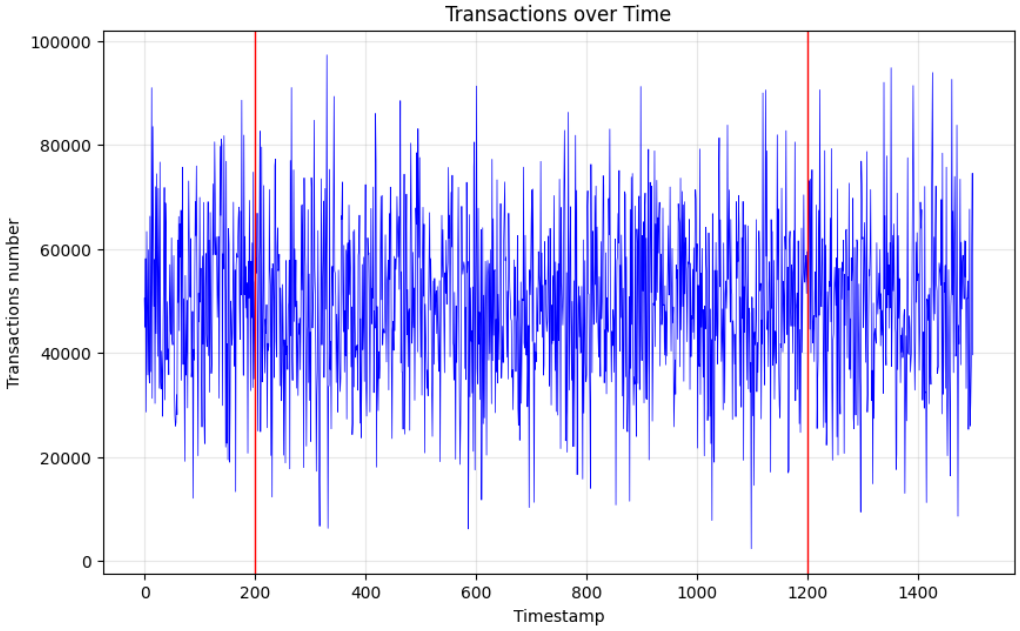

Figure 7. Number of transactions.

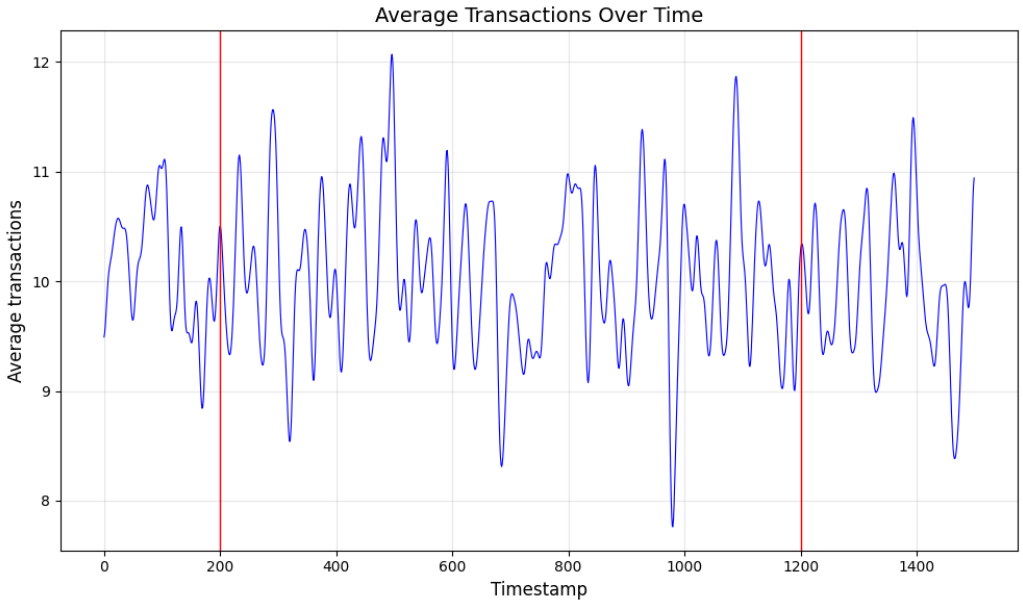

Figure 8. Average transactions per block.

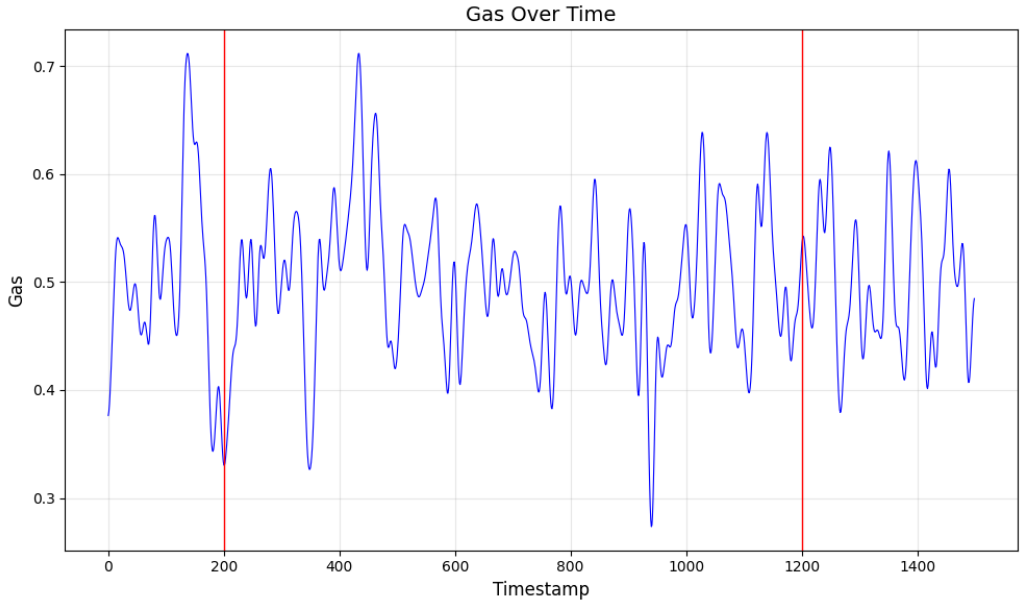

Figure 9. The sum of gas consumed.

Moreover, the reduction in prediction time correlates with the increasing accuracy levels, attributed to the LSTM's information storage design. As previously elucidated, the model's algorithm continuously updates neural network nodes with each block, facilitating timely intrusion detection to mitigate potential damage. Consequently, the system exhibits heightened accuracy and expansive memory, enabling efficient classification and resolution of similar threats. Accuracy, a pivotal metric in evaluating model efficacy [46], is quantified using the accuracy formula, which measures the model's ability to detect anomalies within a given dataset and predict whether each data point constitutes an anomaly. Precision, recall, F1 score, Area Under the Curve (AUC), and false positive rates (FPR) in **Table 4** are additional metrics employed to gauge model performance. These metrics, encompassing various aspects of classification accuracy and error rates, offer a comprehensive evaluation of the model's effectiveness.

Precision delineates the proportion of true positives among all predicted positives, while recall denotes the fraction of true positives among all actual positives. The false positive rate quantifies the ratio of false positives to the sum of false positives and true negatives, providing insights into the model's propensity for misclassification. The F1 score, a harmonic mean of precision and recall, offers a balanced assessment of the model's performance. Additionally, the AUC metric, computed as the integral of True Positive Rate (TPR) against FPR, provides a consolidated measure of the model's ability to discriminate between positive and negative instances. **Figures 10–12** display the performance metrics. Collectively, these metrics furnish a robust framework for evaluating the model's accuracy and effectiveness in intrusion detection.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

Where

TP = True Positive
TN = True Negative
FP = False Positive
FN = False Negative

$$\text{Precision} = \frac{TP}{TP + FP} \tag{7}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{8}$$

$$\text{F1 Score} = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{9}$$

For the true positive value and calculating the AUC, we say
Given:

$$TP = 1 - FN = 1 - 0.015 = 0.985$$

Now, we can compute the AUC using the ROC curve formula:

$$AUC = \frac{1}{2} \times \text{TPR}_1 \times \text{FPR}_2 + \text{FPR}_3 + \ldots \tag{10}$$

Assuming the False Positive Rate (FPR) varies from 0 to 1:

$$\text{FPR}_1 = 0, \text{FPR}_2 = 0.009, \text{FPR}_3 = 1$$

And the True Positive Rate (TPR) varies from 0 to 1:

$$\text{TPR}_1 = 0,\ \text{TPR}_2 = 0.985,\ \text{TPR}_3 = 1$$

$$\text{AUC} = \tfrac{1}{2} \times (0 \times 0.009 + 0.985 \times 0.009 + 1 \times 1)$$

$$\text{AUC} = \tfrac{1}{2} \times (0 + 0.008865 + 1) = \tfrac{1}{2} \times 1.008865 = 0.5044325$$

Table 4. Evaluation results.

Metric	BSC Dataset	ETC Dataset
Accuracy	98.5%	97.2%
Recall	99.2%	98.1%
Precision	98.7%	97.6%
F1 score	98.9%	97.8%
FPR	1.5%	2.8%
AUC	0.993	0.989

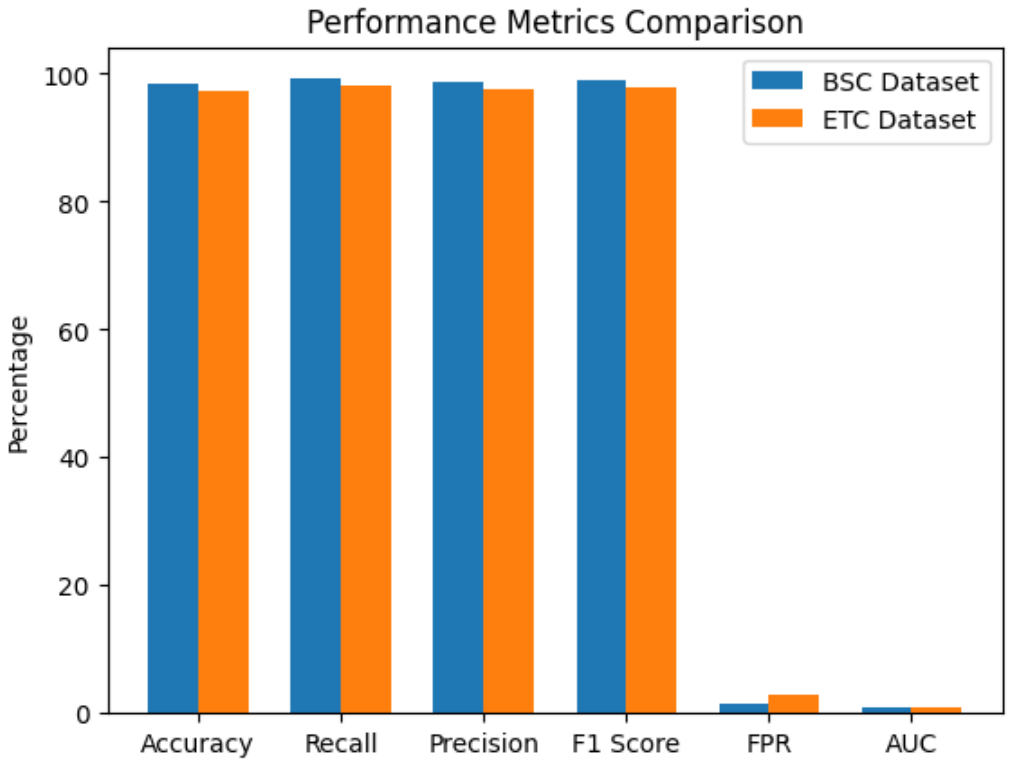

Figure 10. Performance metrics.

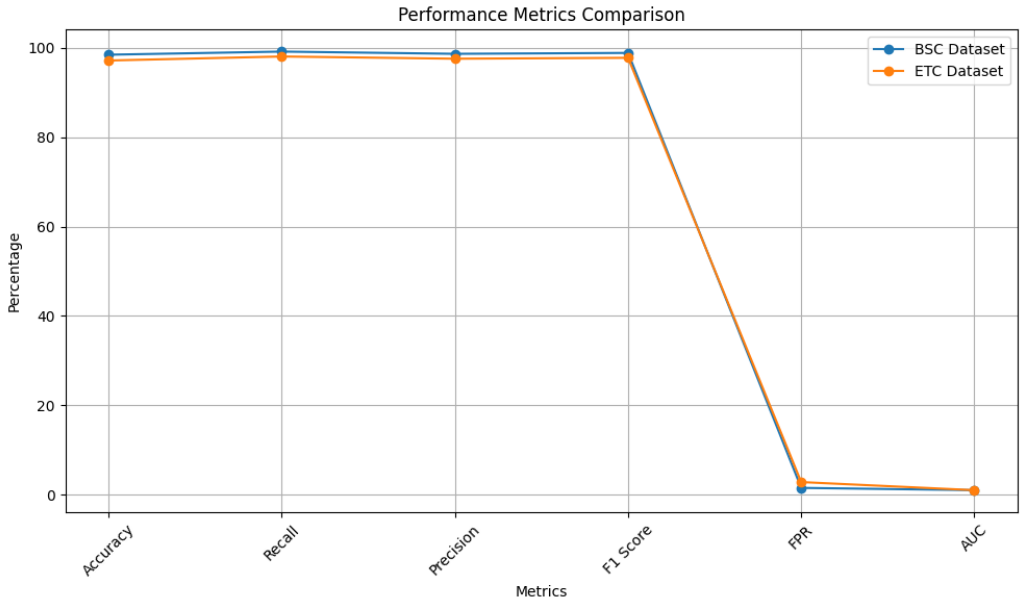

Figure 11. Performance metrics display.

For the ROC curve plot:
BSC Dataset:

- TPR = 0.992
- FPR = 0.015

ETC Dataset:

- TPR = 0.981
- FPR = 0.028

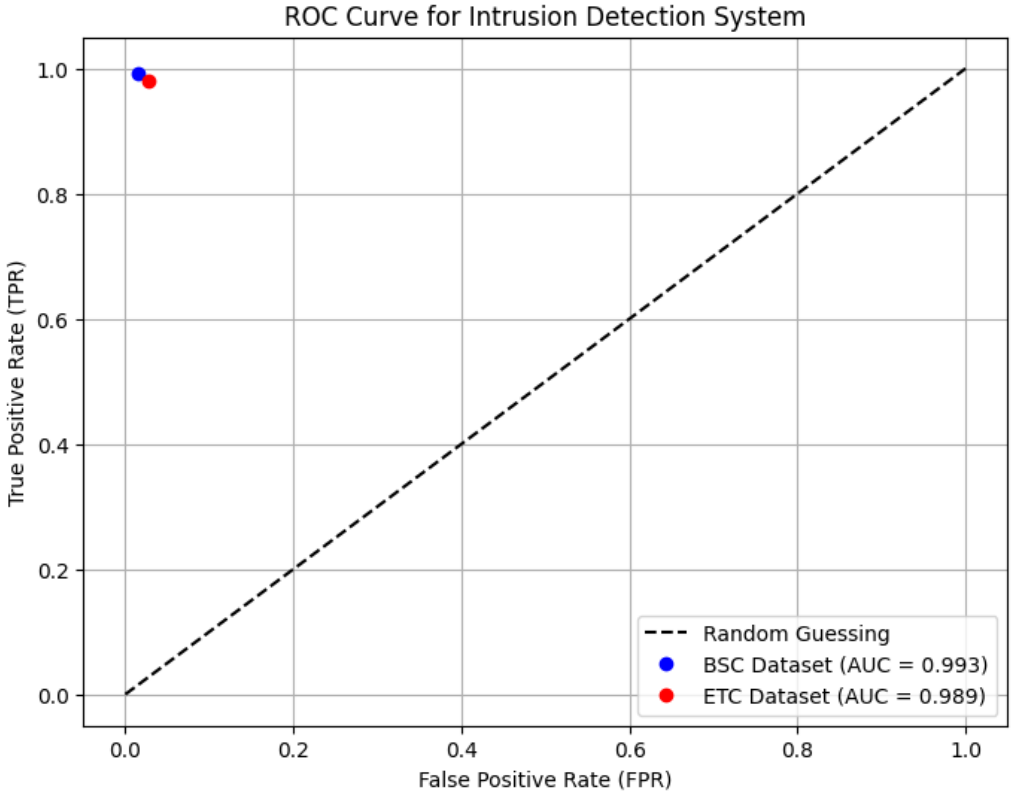

Figure 12. ROC curve.

5. Discussion

The Receiver Operating Characteristic (ROC) curve plays a crucial role in setting thresholds, offering a graphical depiction of a model's sensitivity and specificity across various thresholds [47]. A higher ROC curve signifies superior performance in distinguishing between normal and malicious traffic. Leveraging a decentralized data structure ensures the resilience of storing information across numerous nodes, mitigating risks of tampering or deletion. Data distribution enables access to intrusion data by any node in the network by employing DHT, bolstering defence against potential attacks. To address data loss risks, replication across multiple nodes using DHT ensures redundancy and fault tolerance. Additionally, Principal Component Analysis application is to reduce data dimensionality and streamline processing and also model training. Through transfer learning, pre-trained models are adapted to detect anomalies in blockchain data, optimizing labelling processes. Despite potential vulnerabilities associated with hardware and software from major vendors like Intel and AMD, TEE safeguards sensitive data within a protected enclave, ensuring confidential handling and examination of private information, such as transaction files and private keys, while effectively detecting anomalous behaviour in blockchain data.

The intrusion detection results underscore a promising future for cybersecurity, showcasing exceptional accuracy (97.2%–98.5%), precision in identifying true threats (97.6%–98.7%), and the ability to recall true attacks (98.1%–99.2%) across two independent datasets (BSC and ETC). Additionally, high F1 scores (97.8%–98.9%), minimal false positive rates (1.5%–2.8%), and strong AUC values (0.989–0.993) demonstrate minimal misidentification of normal activity, maximizing effectiveness in real-world applications. It is of paramount importance for an IDS to achieve a balance between high accuracy and low false alarm rates. The proposed methodology has been demon-

strated to greatly reduce false-positive rates while enhancing accuracy, outperforming benchmark models such as those of Abubakar, Liu and Gilliard [9] and Abbas et al. [48], as well as achieving the same result as those of Khonde and Ulagamuthalvi [49]. However, Khonde and Ulagamuthalvi [19] employ the CICIDS17 dataset, which is a synthetic dataset that simulates network traffic data. Real-time classification of incoming protocols, continuous monitoring and learning, improved accuracy, fewer false positives, scalability, adaptability, and enhanced forensic capabilities are among the key findings of this study. However, challenges such as data volume and complexity, data labelling, and privacy considerations associated with using BSC and ETC datasets remain, underscoring the need for ongoing research and development in IDS based on neural networks.

Furthermore, updating the model in a decentralized framework involves several complex processes that are essential to maintaining the integrity and efficiency of the system. First and foremost, any updates to the model must go through a consensus mechanism agreed upon by the network participants to ensure that all nodes agree on the validity of the changes. This often involves a consensus algorithm such as PoS and D-PoS, where nodes compete or stake resources to validate transactions and changes. Once consensus is reached, the updated model must be propagated through the network to ensure that all nodes have access to the latest version. This propagation process can vary depending on the blockchain protocol used and may involve broadcasting the update to all nodes or following a peer-to-peer distribution mechanism. In addition, adding new nodes to the blockchain network requires a similar consensus process to validate the authenticity and trustworthiness of the new participants. These new nodes may need to undergo verification steps and provide proof of their computational power or stake before they are allowed to join the network. Once admitted, they must synchronize with the existing blockchain ledger to ensure they have an up-to-date copy of the entire transaction history. These processes are critical to maintaining the decentralized nature of the network while ensuring the security and efficiency of model updates and node additions.

5.1. Scalability Analysis and Optimization Strategies

A comprehensive scalability analysis is conducted to evaluate the potential impact of blockchain technology on the real-time detection capabilities of the proposed IDS. The analysis begins with an examination of key factors, including transaction throughput, latency, and potential bottlenecks that may arise due to scalability limitations. Transaction throughput is a critical aspect of blockchain scalability, referring to the number of transactions processed per unit of time. High transaction throughput is essential for ensuring timely intrusion detection, as delays in transaction processing can hinder the system's ability to respond to security threats promptly [50]. Therefore, we analyse the transaction throughput of the underlying blockchain platform to assess its suitability for supporting real-time IDS operations.

Latency, another crucial consideration, refers to the time taken for a transaction to be confirmed and added to the blockchain [51]. Excessive latency can lead to delays in detecting and responding to security incidents, compromising the effectiveness of the IDS. Thus, we evaluate the latency characteristics of the blockchain network and explore potential strategies for reducing latency to meet real-time requirements. Furthermore, we investigate potential bottlenecks that may arise in the blockchain network, such as network congestion, block size limitations, and consensus algorithm inefficiencies. Identifying these bottlenecks is essential for devising effective scalability solutions and ensuring uninterrupted operation of the IDS.

To mitigate scalability issues and ensure timely intrusion detection, we explore various optimization strategies for enhancing blockchain performance. These strategies may include sharding, a technique that partitions the blockchain into smaller shards to parallelize transaction processing and improve throughput. Additionally, off-chain processing mechanisms allow certain transactions to be executed off the main blockchain, reducing congestion and latency. Layer 2 solutions, such as state channels and sidechains, offer further scalability enhancements by enabling off-chain computation and settlement while retaining the security guarantees of the main blockchain [52]. Furthermore, the proposed system could be deployed in different contexts including:

- Enterprise Network Security: In a large corporate network with multiple branches and thousands of devices, the proposed system could be deployed to enhance intrusion detection and prevention. The system could analyse network traffic and detect anomalies or malicious activity in real-time, leveraging the scalability of blockchain technology and the efficiency of deep learning models. Case studies could focus on industries such

as banking, healthcare, or manufacturing, where network security is critical due to regulatory requirements and sensitive data handling.

- Smart City Infrastructure: In the context of a smart city, where various IoT devices are interconnected to manage utilities, transportation, and public services, the proposed system could play a vital role in securing the infrastructure against cyber threats. Studies could explore scenarios such as traffic management systems, energy grids, or public safety networks, highlighting how the system detects and mitigates attacks while ensuring the reliability and efficiency of essential services.
- Cloud Computing Environments: With the increasing adoption of cloud computing services, there is a growing need for robust security measures to protect cloud-based applications and data. The proposed system could be deployed in cloud environments to monitor network traffic, detect unauthorized access attempts, and safeguard sensitive information. Research could focus on cloud service providers or enterprises migrating their infrastructure to the cloud, illustrating how the system enhances security while minimizing disruptions to business operations.
- Small and Medium-sized Enterprises (SMEs): Despite resource constraints, SMEs also face cybersecurity threats and require effective intrusion detection solutions. The proposed system could be tailored to meet the needs of SMEs by offering cost-effective and scalable security measures. Studies could showcase how SMEs in various industries, such as e-commerce, software development, or hospitality, deploy the system to protect their networks and customer data from cyber-attacks.
- Remote and Rural Areas: In regions with limited internet connectivity or infrastructure, the proposed system could be adapted to operate in offline or low-bandwidth environments. Case studies could explore how the system functions in remote communities, agricultural settings, or developing countries, demonstrating its ability to provide reliable intrusion detection capabilities even under challenging conditions.

5.2. Ethical Implications of Blockchain Use and Data Protection Compliance

When deploying blockchain-based IDS systems, we need to consider various ethical implications, particularly concerning privacy, transparency, and compliance with regulations such as the General Data Protection Regulation. The immutability of blockchain data raises concerns about the permanent storage of sensitive information, potentially violating individuals' privacy rights if personally identifiable information remains accessible indefinitely. In addition, the decentralized nature of blockchain networks poses challenges in ensuring data sovereignty and control, as IDS data can be replicated across multiple nodes, increasing the risk of unauthorized access and disclosure of sensitive information.

To address these ethical implications and protect sensitive information, we should implement several measures. First, data anonymisation techniques can minimize the exposure of PII on the blockchain, preserving individuals' privacy while benefiting from the blockchain's security features. We also advocate for robust access controls, encryption, and cryptographic key management to regulate data access and prevent unauthorized manipulation or disclosure. In addition, privacy impact assessments could be conducted to identify and mitigate privacy risks and ensure compliance with regulations and ethical standards. Transparent governance frameworks, including clear policies and procedures for data management and incident response, should be established to ensure accountability and oversight throughout the system lifecycle. Collectively, these measures promote trust, accountability, and compliance with ethical standards and regulations in the deployment of blockchain-based IDS systems.

6. Conclusions

As the digital revolution leads to automation and internet connectivity, cybercriminals are constantly improving their intrusion techniques, requiring systems to leverage advances in intrusion detection to maintain security. This study introduces a pioneering IDS model, leveraging neural networks, to enhance intrusion detection accuracy by efficiently categorizing system logs as either malicious or normal, facilitated by blockchain technology. Utilizing the immutable datasets of BSC and ETC, the model proactively identifies anomalies and fortifies defences against potential attacks. Employing an 80/20 data split for training and testing ensures rigorous evaluation, while preprocessed blockchain data enables the detection of unusual activity within the network. Additionally, the model's integration with a dedicated blockchain API facilitates data retrieval, transaction submission, and smart contract

interaction, bolstering its versatility and applicability. Furthermore, the utilization of the ReLU activation function optimizes prediction time, enabling efficient learning of complex data patterns. The model's scalability and adaptability render it suitable for deployment in large and intricate networks, capable of processing substantial data volumes and adapting to dynamic network conditions. The incorporation of TEEs ensures secure storage and analysis of network logs, providing invaluable forensic insights for incident analysis and attack attribution.

In summary, the proposed blockchain-based IDS continuously learns from intrusion logs, storing information in LSTM units, and autonomously updating neural network nodes within each block, all safeguarded by TEEs. Demonstrating remarkable accuracy (97.2%–98.5%), precision in identifying true threats (97.6%–98.7%), and the ability to recall true attacks (98.1%–99.2%) across two independent datasets (BSC and ETC), the model surpasses existing systems, promising enhanced reliability, efficiency, and scalability in intrusion detection. Despite its strengths, the model faces challenges such as data dependency and computational complexity, which are mitigated through strategic data analysis and the adoption of a pre-trained model approach. Moreover, innovative measures such as a Dpos/PoS hybrid consensus mechanism and GPU utilization overcome inherent blockchain limitations, ensuring optimal performance in demanding environments. This research lays the foundation for future investigations into novel neural network architectures, diversified data sources, federated learning approaches, and infrastructure optimization techniques, heralding a new era of robust and adaptive network security solutions.

To provide a more comprehensive analysis of the proposed system, further exploration into the overhead introduced by the blockchain and the computational cost of running deep learning models is warranted. Quantitative data on these aspects would enhance the completeness of our study and provide valuable insights into the practical feasibility of implementing the system in real-world scenarios. Moreover, future research endeavours could include conducting experiments to measure the computational resources required for training and inference tasks, as well as evaluating the performance impact of blockchain transactions on system overhead. Furthermore, future researchers could:

1. Develop standardized APIs and middleware for integrating DL models, blockchain layers, and TEEs.
2. Use data anonymization and tokenization to protect PII while maintaining data traceability.
3. Encourage modular system design to allow independent scaling and updating of IDS components.
4. Promote auditable consensus protocols and rigorous TEE attestation mechanisms.

Policy Implications

1. Regulatory bodies should update cybersecurity standards to account for distributed AI-based IDS systems.
2. Organizations adopting blockchain-based IDS should conduct regular compliance assessments, especially concerning immutable logs and personal data.
3. Governments and institutions should fund research into lightweight cryptographic and AI models suitable for edge deployment in TEE environments.

Author Contributions

A.A.A.: Conceptualization, methodology, data curation, investigation, software, validation and writing—original draft. M.I.: Supervision, visualization, funding acquisition. S.A.: Writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding

This research was funded by China National Key R&D Plan 2020YFA0607902.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The datasets could be obtained from the corresponding author upon reasonable request.

Acknowledgment

Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Rullo, A.; Bertino, E.; Ren, K. Guest Editorial Special Issue on Intrusion Detection for the Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 8327–8330. [CrossRef]
2. Aliyu, A.A.; Liu, J.; Gilliard, E. Blockchain-Based Poisoning Attack Prevention in Smart Farming. *Sci. Practi. Cyber Secur. J.* **2023**, *7*, 38–53.
3. Wang, Z.; Han, D.; Li, M.; et al. The Abnormal Traffic Detection Scheme Based on PCA and SSH. *Connect. Sci.* **2022**, *34*, 1201–1220. [CrossRef]
4. Hephzipah, J.J.; Vallem, R.R.; Sheela, M.S.; et al. An Efficient Cyber Security System Based on Flow-Based Anomaly Detection Using Artificial Neural Network. *Mesopotamian J. CyberSecurity* **2023**, 2023, 48–56. [CrossRef]
5. Javadpour, A.; Pinto, P.; Ja'fari, F.; et al. DMAIDPS: A Distributed Multi-Agent Intrusion Detection and Prevention System for Cloud IoT Environments. *Cluster Comput.* **2023**, *26*, 367–384. [CrossRef]
6. Li, N.; Zhang, R.; Zhu, C.; et al. A Data Sharing Method for Remote Medical System Based on Federated Distillation Learning and Consortium Blockchain. *Connect. Sci.* **2023**, *35*, 2186315. [CrossRef]
7. Saravanan, V.; Madiajagan, M.; Rafee, S.M.; et al. IoT-Based Blockchain Intrusion Detection Using Optimized Recurrent Neural Network. *Multimed. Tools Appl.* **2023**, 83, 31505–31526. [CrossRef]
8. Qu, X.; Liu, Z.; Wu, C.Q.; et al. MFGAN: Multimodal Fusion for Industrial Anomaly Detection Using Attention-Based Autoencoder and Generative Adversarial Network. *Sensors* **2024**, *24*, 637. [CrossRef]
9. Abubakar, A.A.; Liu, J.; Gilliard, E. An Efficient Blockchain-Based Approach to Improve the Accuracy of Intrusion Detection Systems. *Electron. Lett.* **2023**, *59*, e12888. [CrossRef]
10. El Houda, Z.A.; Brik, B.; Khoukhi, L. Ensemble Learning for Intrusion Detection in SDN-Based Zero Touch Smart Grid Systems. In Proceedings of the 2022 IEEE 47th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 26–29 September 2022. [CrossRef]
11. Yang, Y.; Peng, S.; Siet, S.; et al. Detecting Susceptible Communities and Individuals in Hospital Contact Networks: A Model Based on Social Network Analysis. *Connect. Sci.* **2023**, *35*, 2236810. [CrossRef]
12. Kably, S.; Benbarrad, T.; Alaoui, N.; et al. Multi-Zone-Wise Blockchain Based Intrusion Detection and Prevention System for IoT Environment. *Comput. Mater. Continu.* **2023**, *74*, 253–278. [CrossRef]
13. Putra, G.D.; Dedeoglu, V.; Pathak, A.; et al. Decentralised Trustworthy Collaborative Intrusion Detection System for IoT. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021. [CrossRef]
14. Cai, S.; Han, D.; Yin, X.; et al. A Hybrid Parallel Deep Learning Model for Efficient Intrusion Detection Based on Metric Learning. *Connect. Sci.* **2022**, *34*, 551–577. [CrossRef]
15. Zhou, P.; Zhang, H.; Liang, W. Research on Hybrid Intrusion Detection Based on Improved Harris Hawk Optimization Algorithm. *Connect. Sci.* **2023**, *35*(1), 2195595. [CrossRef]
16. Chen, J.; Liang, W.; Xiao, L.; et al. PrivBCS: A Privacy-Preserving and Efficient Crowdsourcing System with Fine-Grained Worker Selection Based on Blockchain. *Connect. Sci.* **2023**, *35*, 2202837. [CrossRef]
17. Rahman, Z.; Yi, X.; Khalil, I. Blockchain-Based AI-Enabled Industry 4.0 CPS Protection Against Advanced Persistent Threat. *IEEE Internet Things J.* **2023**, *10*, 6769–6778. [CrossRef]
18. Alkadi, O.; Moustafa, N.; Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. *IEEE Access* **2020**, 8, 104893–104917. [CrossRef]
19. Khonde, S.R.; Ulagamuthalvi, V. Hybrid Intrusion detection System Using Blockchain Framework. *EURASIP J. Wirel. Commun. Netw.* **2022**, 2022, 58. [CrossRef]

20. Rathee, G.; Kerrache, C.A.; Ferrag, M.A. A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems. *J. Sens. Actuator Netw.* **2022**, *11*, [CrossRef]
21. Heidari, A.; Navimipour, N.J.; Unal, M. A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones. *IEEE Internet Things J.* **2023**, *10*, 8445–8454. [CrossRef]
22. Babu, E.S.; BKN, S.; Nayak, S.R.; et al. Blockchain-Based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks. *Comput. Electr. Eng.* **2022**, *10*, 108287. [CrossRef]
23. Mansour, R.F. Artificial Intelligence Based Optimization with Deep Learning Model for Blockchain Enabled Intrusion Detection in CPS Environment. *Sci. Rep.* **2022**, *12*, 12937. [CrossRef]
24. Aliyu, A.A.; Liu, J. Blockchain-Based Smart Farm Security Framework for the Internet of Things. *Sensors* **2023**, *23*, 7992. [CrossRef]
25. Kumar, R.; Kumar, P.; Tripathi, R.; et al. A Privacy-Preserving-Based Secure Framework Using Blockchain-Enabled Deep-Learning in Cooperative Intelligent Transport System. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 16492–16503. [CrossRef]
26. Janani, K.; Ramamoorthy, S. Threat Analysis Model to Control IoT Network Routing Attacks through Deep Learning Approach. *Connect. Sci.* **2022**, *34*, 2714–2754. [CrossRef]
27. Zheng, J.; Wang, X.; Yang, Q.; et al. A Blockchain-Based Lightweight Authentication and Key Agreement Scheme for Internet of Vehicles. *Connect. Sci.* **2022**, *34*, 1430–1453. [CrossRef]
28. Kumar, P.; Kumar, R.; Garg, S.; et al. A Secure Data Dissemination Scheme for IoT-Based e-Health Systems using AI and Blockchain. In Proceedings of the GLOBECOM 2022 - 2022 IEEE Global Communications Conference, 4–8 December 2022. [CrossRef]
29. Aljabri, A.; Jemili, F.; Korbaa, O. Convolutional Neural Network for Intrusion Detection Using Blockchain Technology. *Int. J. Comput. Appl.* **2023**, *46*, 67–77. [CrossRef]
30. Kumar, P.; Gupta, G.P.; Tripathi, R. Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks. *Arab. J. Sci. Eng.* **2021**, *46*, 3749–3778. [CrossRef]
31. Kumar, P.; Kumar, R.; Kumar, A.; et al. Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT Network. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2802–2813. [CrossRef]
32. Kumar, P.; Kumar, R.; Gupta, G.P.; et al. A Blockchain-Orchestrated Deep Learning Approach for Secure Data Transmission in IoT-Enabled Healthcare System. *J. Parallel and Distrib. Comput.* **2023**, *172*, 69–83. [CrossRef]
33. Kumar, R.; Kumar, P.; Aloqaily, M.; et al. Deep-Learning-Based Blockchain for Secure Zero Touch Networks. *IEEE Commun. Mag.* **2023**, *61*, 96–102. [CrossRef]
34. Kumar, R.; Aljuhani, A.; Kumar, P.; et al. Blockchain-Enabled Secure Communication for Unmanned Aerial Vehicle (UAV) Networks. In DroneCom '22: Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, New York, NY, USA, 24 October 2022. [CrossRef]
35. Gebremariam, G.G.; Panda, J.; Indu, S. Design of Advanced Intrusion Detection Systems Based on Hybrid Machine Learning Techniques in Hierarchically Wireless Sensor Networks. *Connect. Sci.* **2023**, *35*, 2246703. [CrossRef]
36. Cernera, F.; Morgia, M.L.; Mei, A.; et al. Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and in the Binance Smart Chain (BNB). In Proceedings of the 32nd USENIX Security Symposium, 9–11 August 2023. Available online: https://www.usenix.org/conference/usenixsecurity23/presentation/cernera
37. Xin, L.; Ziang, L.; Yingli, Z.; et al. TCN Enhanced Novel Malicious Traffic Detection for IoT Devices. *Connect. Sci.* **2023**, *34*, 1322–1341. [CrossRef]
38. Song, Y.; Hyun, S.; Cheong, Y.-G. Analysis of Autoencoders for Network Intrusion Detection. *Sensors* **2021**, *21*, 4294. [CrossRef]
39. Xu, S.; Zhong, J.; Wang, L.; et al. A Privacy-Preserving and Efficient Data Sharing Scheme with Trust Authentication Based on Blockchain for mHealth. *Connect. Sci.* **2023**, *35*, 2186316. [CrossRef]
40. Wang, H.; Li, F. A Text Classification Method Based on LSTM and Graph Attention Network. *Connect. Sci.* **2022**, *34*, 2466–2480. [CrossRef]
41. Maseno, E.M.; Wang, Z.; Xing, H. A Systematic Review on Hybrid Intrusion Detection System. *Secur. Commun. Netw.* **2022**, 2022, 1–23. [CrossRef]
42. Salzano, F.; Pareschi, R. Enhancing Blockchain Security through Natural Language Processing and Real-Time Monitoring. *Int. J. Parallel Emergent Distrib. Syst.* **2023**, 0, 1–16. [CrossRef]
43. Hu, J.; Liu, Y.; Wu, K. Neural Network Pruning Based on Channel Attention Mechanism. *Connect. Sci.* **2022**, *34*, 2201–2218. [CrossRef]
44. Jeon, J.; Baek, S.; Jeong, B.; et al. Early Prediction of Ransomware API Calls Behaviour Based on GRU-TCN in

Healthcare IoT. *Connect. Sci.* **2023**, *35*, 2233716. [CrossRef]
45. Zhang, S.; Tian, H.; Wang, L.; et al. A Reputation-Based Dynamic Reorganization Scheme for Blockchain Network Sharding. *Connect. Sci.* **2024**, *36*, 2327438. [CrossRef]
46. Sudharsan, R.; Ganesh, E.N. A Swish RNN Based Customer Churn Prediction for the Telecom Industry with a Novel Feature Selection Strategy. *Connect. Sci.* **2022**, *34*), 1855–1876. [CrossRef]
47. Ramraj, S.; Usha, G. Hybrid Feature Learning Framework for the Classification of Encrypted Network Traffic. *Connect. Sci.* **2023**, *35*, 2197172. [CrossRef]
48. Abbas, A.; Khan, M.A.; Latif, S.; et al. A New Ensemble-Based Intrusion Detection System for Internet of Things. *Arab. J. Sci. Eng.* **2022**, *47*, 1805–1819. [CrossRef]
49. Liu, W.; He, Y.; Wang, X.; et al. BFG: Privacy Protection Framework for Internet of Medical Things Based on Blockchain and Federated Learning. *Connect. Sci.* **2023**, *35*, 2199951. [CrossRef]
50. Anthony Jnr, B. Enhancing Blockchain Interoperability and Intraoperability Capabilities in Collaborative Enterprise-a Standardized Architecture Perspective. *Enterp. Inf. Syst.* **2024**, *18*, 2296647. [CrossRef]
51. Jia, Y.; Xiong, L.; Fan, Y.; et al. Blockchain-Based Privacy-Preserving Multi-Tasks Federated Learning Framework. *Connect. Sci.* **2024**, *36*, 2299103. [CrossRef]
52. Shan, W. Digital Streaming Media Distribution and Transmission Process Optimisation Based on Adaptive Recurrent Neural Network. *Connect. Sci.* **2022**, *34*, 1169–1180. [CrossRef]