Received: 9 July 2024 | Revised: 4 September 2024 | Accepted: 10 October 2024 | Published online: 15 October 2024

RESEARCH ARTICLE

Journal of Data Science and Intelligent Systems
2024, Vol. 00(00) 1–11
DOI: 10.47852/bonviewJDSIS42023803

BON VIEW PUBLISHING

A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology

Ahmed Abubakar Aliyu[1,2,*], Jinshuo Liu[1] and Ezekia Gilliard[1]

[1]*School of Cyber Science and Engineering, Wuhan University, China*

[2]*Department of Computer Science, Kaduna State University, Nigeria*

Abstract: The landscape of cyber threats is constantly in flux, which can cause traditional intrusion detection systems (IDS) to fall behind the rapid evolution of attacks. This can result in delayed detection and devastating consequences. The proposed system leverages continuous learning and self-adaptive neural networks to transcend the limitations of traditional IDS. It takes a proactive approach by continuously analyzing intrusion logs, using a long short-term memory (LSTM) core to identify emerging patterns and refine its understanding of threats in real time. This eliminates the static limitations of traditional models and encourages continuous improvement. The system's neural network is distributed across each block of the blockchain, creating a decentralized 'brain' that develops defenses against advanced adversaries. Secure enclaves are located within trusted execution environments (TEEs), ensuring tamper-proof operation and reliable threat detection. The system's superior performance is demonstrated through rigorous evaluations of established datasets, such as NSL-KDD. The model demonstrates a high level of accuracy of 0.9994 with a minimal false-positive rate of 0.06, indicating its ability to differentiate between legitimate network activity and malicious intrusions. Embracing continuous learning and a decentralized architecture creates a dynamic and resilient system that proactively adapts to the ever-changing threat landscape. This approach has several advantages over traditional solutions, including enhanced precision, increased security, and real-time adaptability.

Keywords: blockchain technology, continuous learning, deep learning, intrusion detection system, neural networks

1. Introduction

The automation and Internet-connected items brought about by the digital revolution have increased reliance on digital systems and networks, making it imperative to protect the security and integrity of these infrastructures [1]. There are numerous benefits of such advancement except for the fact that cyber-criminals are continually sophisticating their intrusion strategies [2]. Additionally, cybersecurity threats, including unauthorized access, data breaches, and network intrusions, pose significant risks to organizations and individuals alike making all systems adopt an intrusion detection system (IDS) for security maintenance. In response to these challenges, researchers and practitioners have been exploring innovative approaches to improve the detection and prevention of such intrusions [3]. One emerging technology that holds great promise for strengthening cybersecurity measures is blockchain [4]. Originally introduced as the underlying technology for cryptocurrencies, blockchain has evolved to offer much more than just financial transactions [5]. Its decentralized and immutable nature makes it an ideal candidate for securing various domains, including IDS.

This paper focuses on the integration of neural networks (NN), a powerful tool in machine learning (ML), with blockchain technology to create an advanced IDS. NNs excel at detecting complex patterns and anomalies in large data sets, making them well-suited for identifying malicious activity in network traffic [6]. By combining this capability with the inherent security features of blockchain, we can build a robust and tamper-proof system for detecting and mitigating network intrusions. Furthermore, the use of blockchain in an IDS offers several key advantages. In addition, the decentralized nature of blockchain ensures that there is no single point of failure, increasing the system's resilience to attacks. Moreover, the immutability of the blockchain provides a tamper-proof audit trail of detected intrusions, making it easier to investigate and attribute malicious activity. Furthermore, the transparency and consensus mechanisms inherent in blockchain technology enable trust and collaboration among multiple entities, such as network administrators and security analysts [7], promoting a more efficient and effective response to security incidents. The objectives of this study are to design and develop a NN-based IDS that leverages the benefits of blockchain technology, evaluate its performance in detecting network intrusions, and assess the feasibility of integrating this system into real-world cybersecurity environments. We seek to expand IDS and enhance the overall security posture in the digital environment by fusing the benefits of NNs and blockchain.

*Corresponding author: Ahmed Abubakar Aliyu, School of Cyber Science and Engineering, Wuhan University, China and Department of Computer Science, Kaduna State University, Nigeria. Email: ahmed.aliyu@whu.edu.cn

1.1. Limitations

The field of blockchain-based IDSs offers promising potential for secure and decentralized network protection. However, there are significant limitations that currently undermine their effectiveness:

1) Untrustworthy Data Sharing: Blockchain-based IDSs often face challenges with ensuring the trustworthiness of the data shared across the network. This lack of reliable data sharing can compromise data integrity and accuracy, which impacts the system's ability to accurately detect intrusions [8].
2) Inadequate Adaptation to Evolving Threats: These systems struggle to keep up with evolving cyber threats because their training and testing processes are typically separated. This separation can lead to outdated or inaccurate data classification, resulting in delayed detection of new types of attacks.
3) Limited Continuous Learning: Blockchain-based IDSs often do not continuously learn from ongoing data streams. This limitation hampers their ability to identify novel and sophisticated attacks, as the system cannot dynamically adapt to new threats.
4) Static Models: Traditional IDSs rely on static models that are not well-suited to the constantly changing nature of cyber threats. As a result, these models often generate a high number of false positives, which can disrupt system operations and consume unnecessary resources.

1.2. Contributions

The proposed solution is a blockchain-based intrusion IDS that utilizes continuous learning [9]. The IDS includes dedicated NN nodes in each block of the blockchain, which continuously update themselves with historical intrusion data. This continuous learning loop ensures the model remains up-to-date with evolving threats and improves its detection accuracy over time. TEEs offer a secure enclave for NN training and processing, ensuring data privacy and security [10]. This protects sensitive information from unauthorized access and manipulation, even within a potentially compromised network. Therefore, we propose using LSTM networks to store and process historical data efficiently. Additionally, it is suggested to use incremental training to allow for continuous model updates without requiring complete retraining from scratch. This optimizes resource usage and ensures the model remains responsive to the latest threats. The proposed method enhances privacy, security, efficiency, and scalability. The model proposed utilizes delegated proof-of-stake (DPoS) and proof-of-stake (PoS) consensus mechanisms to improve security and scalability. DPoS is a consensus mechanism where stakeholders elect delegates to validate transactions and secure the network, aiming to improve scalability and reduce centralization, while PoS is a consensus algorithm where validators are chosen to create new blocks and confirm transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Furthermore, optimal resource utilization is ensured through the use of efficient storage and computation techniques.

In the paper, we will discuss the methodology and architecture in Section 3 and also the implementation details of the proposed NN-based IDS with blockchain in Section 4. We will also present experimental results, discuss potential challenges and limitations in Section 5, and explore avenues for future research and improvements in Section 6. The integration of NNs and blockchain technology has the potential to revolutionize the field of IDS. By harnessing the power of ML and the security guarantees of blockchain, we can create a robust and trustworthy system that can effectively detect and mitigate network intrusions. This research aims to contribute to ongoing efforts to strengthen cybersecurity measures and adapt to the evolving threat landscape.

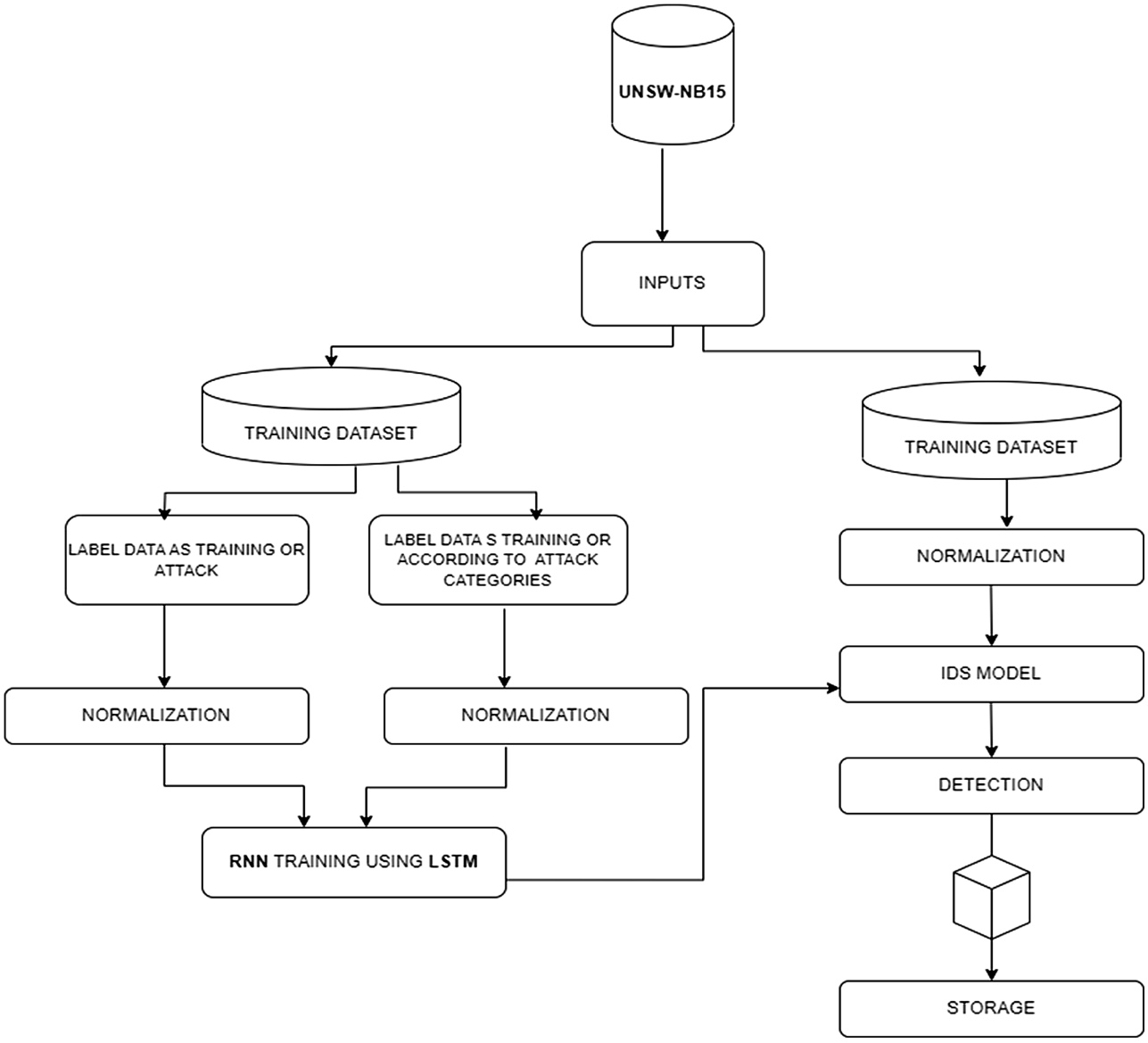
2. Literature Review

In recent years, researchers have explored various strategies to develop IDS. One prominent approach involves applying ML and deep learning (DL) techniques to smart grid systems. For instance, El Houda et al. [11] employed a software-defined network (SDN) to decouple data planes and automatically monitor and manage the communication network. However, this approach suffers from high variance and bias in detection outcomes, necessitating more flexible systems capable of handling a wide range of anomalies with reduced variance. The Multi-Zone-Wise Blockchain model has been introduced to address cybersecurity concerns by integrating blockchain with the Internet of Things (IoT) [12]. This model utilizes a two-step intrusion detection process: initially, a deep convolutional neural network (DCNN) categorizes data as normal, suspicious, or malicious. Subsequently, a generative adversarial network classifies data as normal or malicious, facilitating the reconstruction and mitigation of attack severity. Additionally, the Improved Monkey Optimization algorithm aids in recovering lost data. Information sharing among various IoT nodes has become a critical theme for enhancing malware detection. Patel and Patel [13] have also proposed a Collaborative-IDS (CIDS) where blockchain serves as a decentralized platform, enabling nodes to share information on malware and alert the system. The primary challenge in such designs is ensuring the trustworthiness of shared information, particularly in sensitive sectors like medical devices [14]. Ensuring reliable data sharing is essential for the success of these systems. A separate study by Khonde and Ulagamuthalvi [15] has introduced an AI-aligned advanced persistent threat (APT) detection system, which significantly improved trust levels. However, the sustainability and cost of such systems may be prohibitive for small enterprises. LSTM is a type of recurrent NN architecture designed to remember information for long periods, addressing the vanishing gradient problem in traditional recurrent neural networks (RNNs).

Abubakar et al. [16] have also introduced a blockchain-based technique that employs ensemble learning algorithms to enhance IDS accuracy, validated on datasets like DARPA99 and MIT Lincoln Lab. This method leverages blockchain's data integrity and transparency alongside ensemble learning's improved detection accuracy through algorithm combination. Similarly, El Houda et al. [11] developed a framework using ensemble learning to detect and mitigate security threats in SDN systems. Incorporating boosting feature selection and lightweight boosting algorithms, this framework was validated on NSL-KDD and UNSW-NB15 datasets (shown in Figure 1 [17]), demonstrating robust detection capabilities.

Another study by Janani and Ramamoorthy [12] has proposed an IoT routing attack detection model using LSTM networks and an Adaptive Mayfly Optimization Algorithm. Validated on NSL-KDD, BoT-IoT, and IoT-23 datasets, this model showed enhanced performance in detecting and classifying IoT routing attacks. Kably et al. [18] have introduced the Multi-Zone-Wise Blockchain model, emphasizing blockchain's decentralization and security benefits. However, the specific NN-based algorithms and datasets used were not detailed, limiting direct comparison with other studies. An APT detection system integrating blockchain and AI was developed by Rahman et al. [14], employing a Deep Transfer Learning-based ResNet (DTL-ResNet) approach on

Figure 1
A representative IDS framework with UNSW-NB15



private datasets. This system capitalizes on DL for feature extraction and blockchain for secure data handling.

A study by Khonde and Ulagamuthalvi [15], has also presented a blockchain framework for inter-node signature exchange in distributed IDS, using Isolation Random Forest and XGBoost algorithms validated on the CICIDS 2017 dataset. This framework enhances IDS security and reliability through secure inter-node communication. Rathee et al. [19] have presented an IDS utilizing the Viterbi algorithm, indirect trust, and blockchain for Industrial IoT, validated on private datasets. This method focuses on trust management and secure data exchange. A study by Heidari et al. [20] has introduced a blockchain-based radial basis function NN model, validated on datasets including UNSW-NB15, NSL-KDD, CICDDoS2019, CICIDS2017, and AWID, highlighting the versatility of radial basis function networks with blockchain technology.

Babu et al. [21] have developed a permission-based blockchain system using the arbiter physically unclonable function model to secure IoT device key pairs. Validated with Decision Tree, Random Forest, and SVM algorithms on the CICDDoS2019 dataset, this system addresses lightweight security needs in IoT environments. Aljabri et al. [22] have introduced a blockchain-based IDS model using convolutional neural networks (CNN) combined with SHA-256 hashing algorithm and Greedy-based genetic algorithm, validated on private datasets. This approach secures network traffic data and enhances detection capabilities.

Kumar et al. [23] have proposed a hybrid feature-reduced intelligent cyber-attack detection system for IoT networks, using RandomForest, K-Nearest Neighbor, and XGBoost algorithms, validated on NSL-KDD, BoT-IoT, and DS2OS datasets. This study demonstrates the effectiveness of feature reduction in improving detection performance. A study by Mansour [24] introduced a DL model for blockchain-enabled IDS in cyber-physical systems environments, using attention-based bi-directional gated RNN and Poor and Rich Optimization, validated on NSL-KDD 2015 and CICIDS 2017 datasets. This model enhances detection accuracy through attention mechanisms. Kumar et al. [25] have also proposed a secure framework based on privacy protection using blockchain-enabled DL in cooperative intelligent transport systems. Using LSTM, Autoencoder, Adaptive RNN, and Backpropagation Through Time on ToN-IoT and CICIDS-2017 datasets, this study

focuses on privacy preservation and secure data exchange. Moreover, Kumar et al. [26] introduced an integrated framework for decentralized data processing and learning in Industrial IoT networks, using LSTM-Sparse AutoEncoder and Multi-Head Self-Attention-based Bidirectional Gated Recurrent Unit, validated on CICIDS-2017 and ToN-IoT datasets. This approach emphasizes decentralized learning and secure data processing. Finally, Mahdavisharif et al. [27] have presented a big data-aware DL method for designing an efficient IDS using the BDL-IDS algorithm on the NSL-KDD dataset, addressing the challenges of handling large-scale data in intrusion detection. This comparative analysis illustrates the diverse methodologies and technologies in IDS research, emphasizing the integration of NN-based and blockchain-based approaches, with each study offering unique insights and advancements, collectively advancing secure and efficient intrusion detection.

Our work proposes a Blockchain-based IDS model that increases malicious attack detection accuracy using DL. This approach employs LSTM, RNN, Autoencoder, XGBoost, and Isolation Random Forest (IRF) algorithms, validated on the NSL-KDD dataset. The study combines DL's feature extraction capabilities with blockchain's secure data handling to enhance IDS effectiveness.

3. Research Methodology

As robust IDS are necessary to safeguard network security against ever-evolving cyber threats, blockchain technology offers transparency, immutability, and decentralization. Integrating it with ML algorithms has immense potential for enhancing IDS accuracy and efficacy. This research presents a new hybrid approach that combines the strong data management capabilities of blockchain with the pattern recognition abilities of ML to identify abnormal network activity.

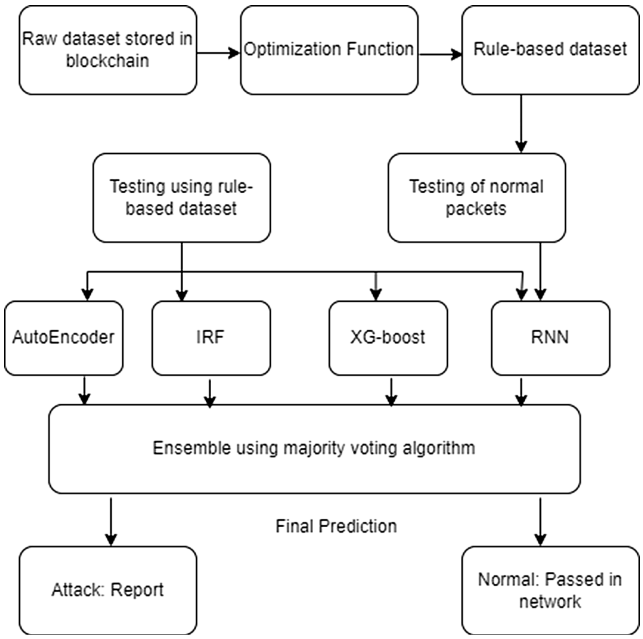
3.1. Raw dataset acquisition and blockchain storage

The system begins by gathering a raw dataset that comprises information on network traffic. These data encompass features extracted from network packets, such as source and destination IP addresses, port numbers, packet sizes, and flags. The raw dataset is stored in a blockchain because blockchain technology offers several potential advantages for IDS applications, including immutability. Once data are added to the blockchain, it cannot be tampered with, ensuring the integrity of the training data for the IDS. Storing the data on a distributed ledger can improve security and fault tolerance [28]. Additionally, blockchain can provide a verifiable audit trail for the data, promoting trust and accountability. The system is based on a powerful NN architecture that has been trained on acquired data. The NN can identify complex patterns and characteristics of regular network activity. To achieve this, a DL architecture, such as a CNN or RNN, is used to extract significant features from the data. This enables the model to distinguish subtle deviations from established baselines. The system can detect anomalous network events that may indicate malicious activity or security breaches.

3.2. Rule-based dataset generation

This step involves creating a rule-based dataset based on the raw network traffic data. Security experts define rules to identify specific patterns or characteristics associated with known malicious network activity [29]. It is important to note that Figure 2 does not explicitly show how this rule-based dataset is generated as these rules could be manually crafted or learned from a subset of labeled data within the raw dataset.

Figure 2
The blockchain-based IDS approach



3.3. Blockchain storage of rule-based dataset

The rule-based dataset, like the raw dataset, is stored on the blockchain, potentially benefiting from its immutability, decentralization, and transparency. The system may use the rule-based dataset to initially filter or classify network traffic by checking incoming traffic against defined rules to identify potential threats. It is also imperative to note that relying solely on rule-based approaches may have limitations in detecting novel or zero-day attacks.

3.4. Testing of normal packets

At this stage, a subset of the raw network traffic data containing only normal activity is isolated. These data are crucial as they form the foundation for the NN's training process. By analyzing these normal network patterns, the NN learns the characteristics of legitimate traffic, enabling it to distinguish normal behavior from potentially malicious activity later on. This traffic data serves as a baseline reference point, allowing the network to identify deviations and flag them as suspicious when encountering unseen network packets. It is essential that the NN is trained to recognize these deviations and flag them as suspicious [30].

3.5. Autoencoder for anomaly detection

An autoencoder is a NN type that is trained to reconstruct input data. The autoencoder is utilized for anomaly detection. The autoencoder is trained on normal network traffic data. When it encounters unseen network traffic, the reconstruction error (the difference between the input and the reconstructed output) will be higher for anomalous data compared to normal traffic. By analyzing the reconstruction error, the autoencoder can identify patterns that deviate from normal network behavior and flag them as suspicious activity.

3.6. Combining IDS techniques (ensemble approach)

Figure 2 shows how the system combines the outputs from the rule-based detection and the anomaly detection using the autoencoder described previously. This ensemble approach can potentially leverage the strengths of both techniques:

- Rule-based methods can be effective for identifying known threats.
- Autoencoder-based anomaly detection can be useful for detecting novel attacks.

For the ensemble approach combining rule-based detection and anomaly detection using autoencoders, the standard equations for combining outputs could include:

1) **Majority Voting:**

$$FinalDecision = MajorityVote(Rule - basedOutput, AnomalyDetectionOutput)$$

In this method, the final decision is determined based on the majority vote of the outputs from the two detection techniques. For example, if both methods classify a network packet as malicious, the final decision will also classify it as malicious.

2) **Weighted Scoring:**

$$Final\ Decision = \sum_{i=1}^{n} wi \times Output_{\mathrm{i}} \quad (1)$$

In this method, each detection output is assigned a weight (w_i*wi*) representing its importance or reliability. The final decision is then calculated by summing the weighted outputs. This allows for flexibility in assigning more weight to the more reliable or accurate detection method.

These equations provide a framework for combining the outputs of rule-based detection and anomaly detection using autoencoders, allowing for a more robust and comprehensive approach to network intrusion detection.

In the ensemble approach combining rule-based detection and anomaly detection using autoencoders, a tie in majority voting occurs when the two methods produce different outputs. To resolve this, predefined rules can be used, such as defaulting to a conservative decision like classifying as malicious, or additional criteria can be applied to break the tie. In the weighted scoring method, ties might happen if the weighted sums of outputs are equal. Resolution strategies include adjusting the weights to better reflect the methods' reliability, implementing a tie-breaking mechanism, or using fallback rules. Both methods benefit from having clear tie-breaking procedures to ensure consistent decision-making.

3.7. Optimization function

During the training of NNs for anomaly detection in this IDS system, an optimization function plays a critical role. This function acts as a guide, constantly evaluating the performance of the autoencoder based on how well it reconstructs normal network traffic data. The weights and biases of the autoencoder are iteratively adjusted based on the minimization of this reconstruction error, allowing the network to learn the typical patterns of legitimate traffic. This enables the autoencoder to accurately detect deviations from these patterns, which may indicate anomalous data (such as potential attacks) with a high reconstruction error. The equation for the optimization function used during the training of NNs for anomaly detection, particularly in the context of an autoencoder-based IDS system, involves minimizing the reconstruction error. This error is typically measured using a loss function, such as the mean squared error (MSE), which compares the input data (normal network traffic) with the reconstructed output from the autoencoder. The equation for the optimization function can be represented as follows:

$$Optimization\ Function = Minimize\,(Loss\ Function)$$

In mathematical terms, the loss function L is defined as the MSE between the input data X and the reconstructed output X^ by the autoencoder:

$$L = \frac{1}{N} = \sum_{i=1}^{N} (X_i - X\hat{}_i)^2 \quad (2)$$

Where:

N is the total number of data points.

X_i represents the i^{th} input data point.

$X\hat{}_i$ represents the reconstructed output corresponding to the i^{th} input data point.

The optimization function guides the training process by adjusting the weights and biases of the autoencoder to minimize this reconstruction error, thereby enabling the network to learn the typical patterns of legitimate traffic and accurately detect deviations indicative of anomalous data.

3.8. Final prediction: Attack/normal

The system uses an ensemble approach to generate the final prediction by combining the outputs from the rule-based detection and the autoencoder's anomaly detection. The former is excellent at identifying known threats, while the latter is adept at flagging novel attacks. This combined analysis enables the system to classify incoming network traffic as either malicious or benign. Security alerts can be triggered, and mitigation procedures initiated to counter the attack when a threat is detected. Upon deployment, real-time analysis begins. The NN, equipped with its knowledge of normal network behavior learned during training, continuously analyzes incoming data. Any significant deviations from these patterns are flagged as anomalies. These identified anomalies are then reported to the secure and transparent blockchain network. Each incident is recorded as a transaction on the blockchain, creating an immutable and verifiable historical record of security events. This transaction includes important information such as the anomaly type, the timestamp of its occurrence, and relevant metadata. This provides a complete overview of potential threats for further investigation and mitigation.

3.9. Distributed consensus and validation

The trust and integrity of reported anomalies are ensured by the inherent strengths of the blockchain network. The network employs a well-established hybrid consensus mechanism, such as Delegated Proof of Stake-Proof of Stake (DPoS-PoS), to distribute the validation responsibility among its participants. This decentralized approach ensures the immutability of recorded data, preventing malicious actors from tampering with the historical record of reported intrusions. Furthermore, the consensus mechanism creates

a reliable environment for all network participants by eliminating the risks associated with centralized validation authorities.

One of the key benefits of blockchain technology is its distributed data storage architecture. Unlike traditional centralized systems, the proposed model uses the blockchain network to store intrusion data across multiple nodes in a decentralized manner. This eliminates the vulnerabilities associated with single points of failure, ensuring the persistence and accessibility of data even in the face of targeted attacks [31]. Furthermore, security analysts and auditors have the authority to access the blockchain and investigate recorded intrusions, aiding forensic investigations and the identification of malicious activity. Moreover, the proposed architecture is based on the interaction with several other modules that work together to integrate blockchain technology and NN-driven anomaly detection. The data collection module is responsible for collecting network data from various sources, such as intrusion detection sensors, firewalls, and network sensors. The data representing network activity undergo pre-processing and conditioning to make it digestible for the NN. The neural network module uses ML algorithms to extract salient features and apply pattern recognition skills to the digital tapestry. This analysis results in a definitive classification: is the observed behavior benign or a harbinger of malicious intent? When an anomaly is detected, the intrusion reporting module takes action by creating a transaction with the captured details of the anomalous event and transmitting it to the immutable realm of the blockchain network. This network is composed of a distributed orchestra of nodes that uphold the paramount values of security and transparency. Using a strong consensus mechanism, this system harmonizes reported intrusions to ensure their validity and records them permanently on the blockchain's tamper-proof ledger. The audit and analysis module enables authorized users, such as security analysts and auditors, to investigate recorded intrusions. It provides them with a set of tools for pattern analysis, forensic investigations, and incident exploration. Each module plays a designated role within this synergistic ensemble, contributing to the overarching goal of safeguarding the network by leveraging the combined strengths of blockchain technology and NN-based anomaly detection. The blockchain serves as a secure and permanent archive for historical records of identified intrusions, while the NN acts as a vigilant sentinel, continuously scrutinizing the network landscape and raising the alarm against potential threats.

4. Implementation

Measuring the competency of an IDS poses a considerable challenge, particularly in locating relevant data for collection. Although network monitoring provides essential information for this purpose, the costliness of data collection often leads developers to rely on readily available datasets for experimentation. In this study, we utilize the NSL-KDD dataset, a widely used resource in intrusion detection research, comprising over 490,000 records [32]. Each record represents a network connection classified as "normal" or one of four attack types: denial-of-service (DoS), probe, user-to-root, and remote-to-local as shown in Table 1. Notably, the dataset exhibits a significant class imbalance, with the "normal" class comprising over 80% of the data. This imbalance poses a challenge for ML models, necessitating techniques such as oversampling, undersampling, or algorithmic adjustments to mitigate bias and improve model performance [33]. Our study addresses this imbalance and leverages LSTM and RNN-CNN models to enhance intrusion detection capabilities.

Gates in LSTM networks are pivotal for modifying cell states, enabling the framework to discern relevant information from noise.

Table 1
Normal and attack data

Class	Number of records
Normal	39,499
DoS	39,524
Probe	4107
U2R	243
R2L	1126

LSTM units are governed by three types of gates: input gates, output gates, and forget gates. The forget gate regulates the clearing of the memory unit variable *st*, while the input and output gates manage processes involving input (*xt*) and output (*yt*) variables, respectively:

$$s_t = f_t \odot s_t - 1 + x_t \odot (W_x + W_o + B) \tag{3}$$

$$o_t = y_t \odot tanh\,(s_t)_t \tag{4}$$

Here, W*W* represents the weight matrix and B*B* signifies a bias term. The hidden conditions of the (NN) are computed as:

$$f(x) = Lh^T \tag{5}$$

$$= h^T = \alpha\,(Hh_{t-1} + W_c x_t) \tag{6}$$

$$h_o = \alpha\, W_c x_o$$

Here, H and L represent hidden weights and label weights, respectively. We utilized the cost function $y - f(x))^2$ to optimize the weights.

The incorporation of multiple gates and hidden states, as illustrated in Figure 2 [34], enables LSTM networks to excel at capturing long-term dependencies. However, the presence of numerous gates within the routing mechanism of LSTM networks results in inefficiency, necessitating a greater runtime memory requirement compared to traditional RNNs. In light of the computational burden associated with training LSTMs, we introduce a simplified autoencoder. This autoencoder not only trains more rapidly than LSTMs but also preserves long sequence connections, mitigating the vanishing gradient issue with minimal memory overhead, as illustrated in Figure 3. This alternative addresses the computational expense of LSTM training, offering accelerated learning, seamless recall of extended connections, and effective mitigation of the vanishing gradient problem.

Figure 3
Neural network attack structure

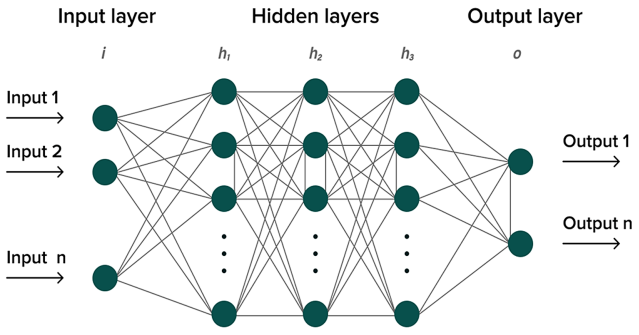


Figure 4
The ensemble approach using a majority voting algorithm

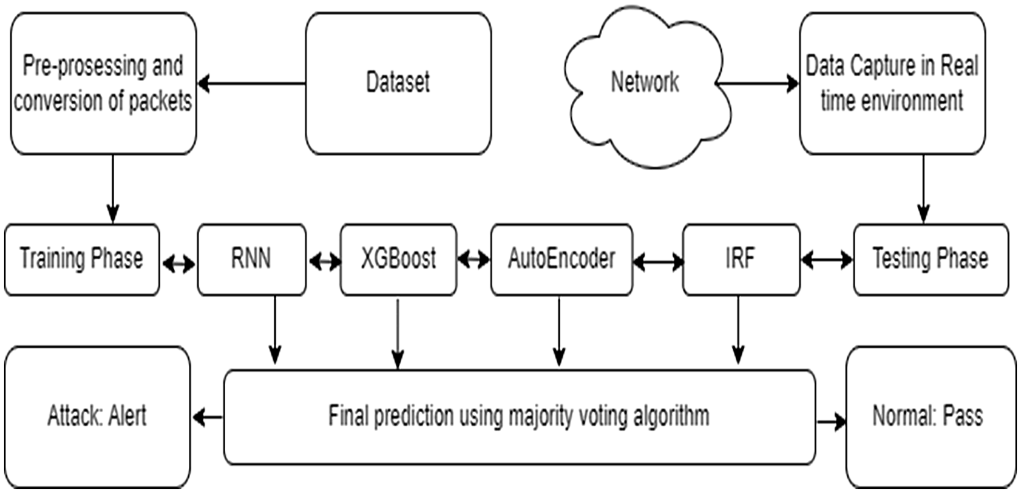


Figure 4 outlines a combination of three pre-trained models and a voting ensemble method for the model as shown below.

5. Results and Discussion

The system uses a combination of ML models to detect anomalies in network traffic as seen in Figure 4. Specifically, it employs RNNs to capture sequential patterns, XGBoost AutoEncoders to detect anomalies based on reconstruction error, and IRF classifiers for efficient outlier detection. These models are trained using the NSL-KDD dataset, which is a commonly used benchmark dataset for modern intrusion detection tasks (as shown in Table 1). The system achieves the final prediction of an attack or a normal packet through an ensemble approach that uses a majority voting algorithm. This involves combining the individual predictions from each model (RNN, XGBoost AutoEncoder, and IRF), and selecting the most frequent prediction (attack or normal) as the final output. To ensure reliable predictions and reduce the influence of external factors, the system employs standardization techniques when processing neuron model inputs. This method removes the influence of seasonal fluctuations, periodic patterns, and statistical prejudices from the network traffic data. Furthermore, the models are built using a specific ratio for dividing training and testing data to enhance performance. To efficiently process and train models on blockchain data, the system employs two techniques: principal component analysis (PCA) for reducing dimensionality and transfer learning with a pre-trained model. PCA reduces data complexity by identifying significant features, while transfer learning leverages knowledge gained from a pre-trained model on a similar task to improve training efficiency on specific blockchain data. These techniques streamline the processing pipeline and enable the model to detect anomalies in blockchain transactions effectively. The system prioritizes data security by using TEE to address concerns about vendor lock-in and potential vulnerabilities in commonly used hardware and software. TEE creates secure enclaves within the primary processing environment, enabling the secure handling and analysis of sensitive data, such as blockchain transactions and private keys, without compromising confidentiality. TEE functions as a secure space that prevents unauthorized access and guarantees complete data privacy. This enables the system to accurately detect anomalies in blockchain data while protecting sensitive user information.

The model uses ensemble learning to establish a reliable and precise set of rules that define 'normal' network traffic patterns. These rules serve as a baseline for identifying potentially malicious activity. The first stage involves training a collection of classifiers, including RNN, XGBoost AutoEncoder, and IRF, using a dataset of predefined rules. These classifiers then work together as a unified ensemble, collaboratively analyzing incoming network traffic packets. The main principle is to detect any deviations from the established rules. If a significant deviation from the expected behavior is identified by a majority vote within the ensemble, an alarm is triggered to indicate a potential attack. The flagged packet is then forwarded to a subsequent stage for signature generation and dissemination. Conversely, packets that comply with the established rules are allowed to pass freely through the network. A crucial aspect of this approach is the use of ensemble learning. Incorporating a majority voting mechanism mitigates the risk of biased predictions by individual classifiers, thereby minimizing the generation of false alarms. The ensemble ensures a more reliable and accurate assessment of network traffic, ultimately improving the overall effectiveness of the IDS. The system continuously monitors and classifies network traffic, maintaining a memory of all encountered attack types. According to Maseno et al. [35], advanced IDS systems with improved capabilities to counter attacks benefit from extensive data collection and classification. This allows the system to identify anomalies more effectively and proactively defend against potential threats.

The NSL-KDD dataset was processed using the PyTorch library, which was chosen for its suitability and widespread adoption. The system assesses incoming network traffic using preprocessed data and categorizes it as either benign or malicious. It is worth noting that the time taken for prediction decreases as the accuracy level increases, which can be attributed to the model's ability to store information in both LSTM [36]. As previously stated, the algorithm of the model is updated continuously through training and data processing at each network block. This ongoing learning process facilitates timely intrusion detection and enables the system to accumulate knowledge, effectively addressing similar threats in the future. The model achieves high accuracy rates and utilizes a large memory capacity for efficient classification and resolution of recurring threats. Finally, the system prioritizes data privacy and security by relying

Figure 5
Dataset's characteristics

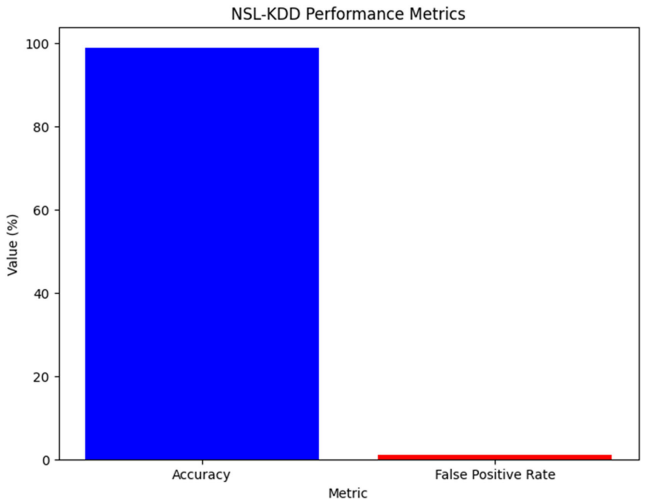


Table 2
Test results

Metric	NSL-KDD
Accuracy	0.9994
False positive	0.06

on the principle of TEE. This creates a secure enclave for model operation, minimizing the risk of exposure to malware or other threats. According to Sudharsan and Ganesh [37], accuracy is a crucial performance metric that measures a model's ability to identify anomalies in a dataset and predict whether each data point represents an anomaly or not. It is calculated by dividing the number of correct predictions by the total number of predictions made by the system.

Accuracy and False Alarm Rate are two important metrics for evaluating IDS. Accuracy is the percentage of packets correctly classified by the system. It is calculated as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

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

The accuracy of the NN-based IDS on the NSL-KDD dataset was 0.9994.

The false-positive rate is the percentage of packets falsely classified as malicious by the system. It is calculated as:

$$\text{FP} = \frac{FP}{FP + TN} \tag{8}$$

The proposed system was evaluated using the NSL-KDD dataset shown in Figure 5. The NN-based IDS was trained on 80% of the dataset and tested on the remaining 20%. The accuracy and false alarm rate of the NN-based IDS were measured as follows:

The false alarm rate of the NN-based IDS on the NSL-KDD dataset was 0.06%. Table 2 and Figure 6 show the test results for both accuracy and false alarm rates while Table 3 and Figure 6 show the statistics of the datasets.

The model's use of blockchain technology offers several advantages, including decentralization, which eliminates reliance

Figure 6
Performance metrics

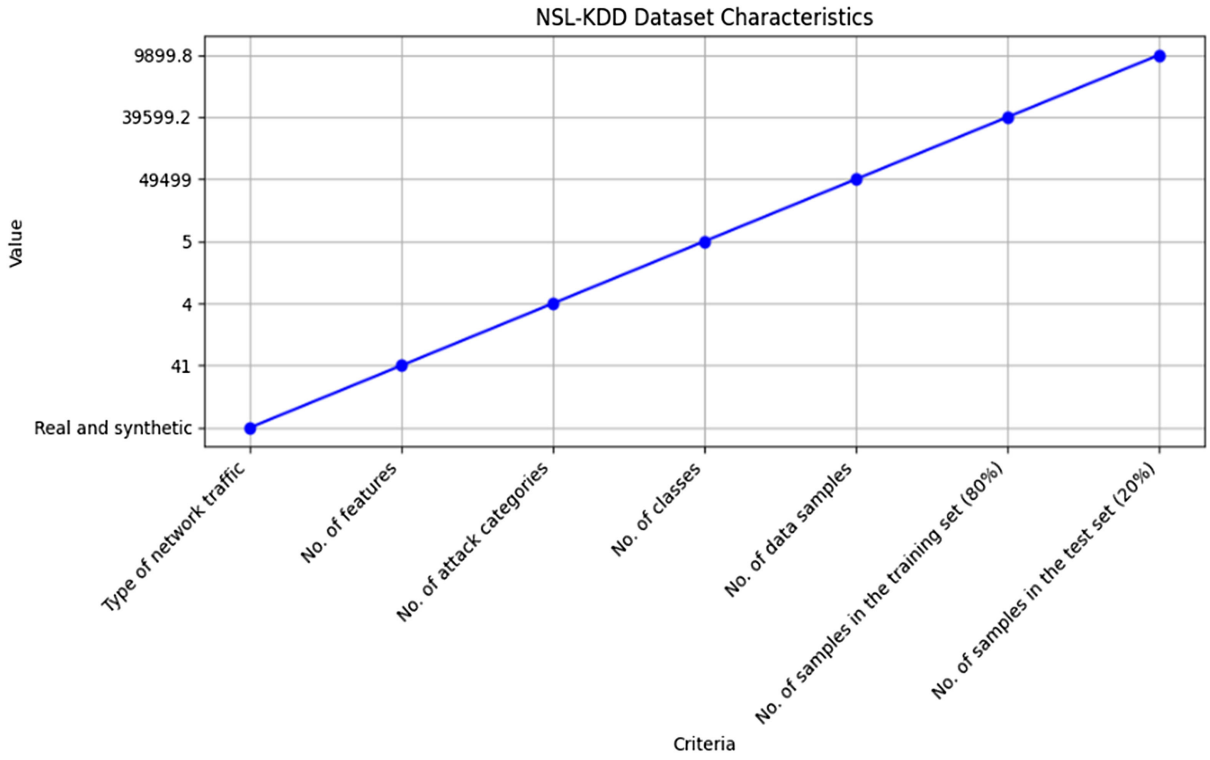


Table 3
Dataset statistics

Criteria	NSL-KDD dataset
Type of network traffic	Real and synthetic
No. of features	41
No. of attack categories	4
No. of classes	5
No. of data samples	49,499
No. of samples in the training set (80%)	39,599.2
No. of samples in the test set (20%)	9,899.8

on a single server. This makes it more resilient to attacks and less likely to be compromised. Additionally, the immutability of the blockchain ledger ensures that it cannot be tampered with, thereby increasing the model's reliability and trustworthiness. Another advantage is the transparency of the blockchain ledger, which makes it publicly available. Auditing and accountability are enabled by this feature, which can also help establish trust in the model. It is important to strike a balance between high accuracy and low false alarm rates in an IDS, as a system with very high accuracy may have a high false alarm rate, causing unnecessary disruption to the network [38].

6. Conclusion

The digital revolution has resulted in automation and Internet connectivity. However, cybercriminals are continuously improving their intrusion techniques, which necessitates the use of advanced IDS to maintain security. Therefore, we have introduced a new approach that integrates ML into a blockchain-based IDS, demonstrating increased accuracy in detecting malicious attacks. The design enables secure distribution of the ledger, increasing the accuracy and durability of the CIDS. Traditional IDS can be limited by data and static algorithms, but with this design, there is early detection of anomalies to ensure that sensitive information is safeguarded. Our study introduces a new blockchain-powered IDS model that can learn and adapt quickly. The system continuously ingests intrusion logs and uses intricate LSTM networks to optimize neural nodes within each immutable block. Unlike outdated and unchanging models, this IDS delves into the depths of blockchain data to uncover even the most hidden anomalies through careful pre-processing. A dedicated API provides unparalleled access, allowing for transaction submission and smart contract interaction, creating a comprehensive understanding to reveal hidden threats. However, our innovation goes beyond just data access. The ReLU activation function is employed, which optimizes the model to learn complex patterns quickly. This scalability makes it ideal for large networks and adapting to unforeseen challenges.

To ensure security, the model's core is fortified with TEEs to safeguard sensitive data and ensure privacy and integrity. They function as secure storage for network logs, providing valuable forensic insights and protecting blockchain data from potential vulnerabilities. This NN-based IDS represents a revolution in cybersecurity with an impressive 0.9994 accuracy and a minimal 0.06 false-positive rate, outperforming the existing systems of Abubakar et al. [16], the work of Rababah and Srivastava [39] as well as Sunanda et al. [40], which use the NSL-KDD dataset. The study tackles issues of data reliability, inefficient learning, and poor classification while also addressing privacy, security, efficiency, and scalability.

It is important to acknowledge that no defense mechanism is perfect. Therefore, to reduce the computational footprint, we use strategic data analysis techniques and meticulously pre-trained models. Additionally, we utilize a DPoS-PoS hybrid consensus mechanism and powerful GPUs to overcome the inherent limitations of blockchain. This research presents a system designed to combat ever-evolving cyber threats. The system utilizes immutable data, optimizes predictions, and provides valuable forensic insights, making it an essential tool for intrusion detection. Future researchers can explore deeper architectures, diverse data sources, and federated learning strategies, which promise a more secure and resilient digital landscape.

Acknowledgement

The authors are grateful to the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, and Department of Secure Computing, Kaduna State University.

Funding Support

This work is sponsored by the National Key Research and Development Program of China with the Grant Number 2020YFA0607902.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data available on request from the corresponding author upon reasonable request.

Author Contribution Statement

Ahmed Abubakar Aliyu: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Project administration. **Jinshuo Liu:** Validation, Resources, Visualization, Supervision, Funding acquisition. **Ezekia Gilliard:** Software, Formal analysis, Writing – review & editing.

References

[1] Kadam, A., & Garg, B. (2022). Accuracy and deviation analysis of intrusion detection system. In *Proceedings of the International Conference on Innovative Computing & Communication*. https://doi.org/10.2139/ssrn.4025358

[2] Rullo, A., Bertino, E., & Ren, K. (2023). Guest editorial special issue on intrusion detection for the internet of things. *IEEE Internet of Things Journal*, *10*(10), 8327–8330. https://doi.org/10.1109/JIOT.2023.3244636

[3] Vijay, A., Patidar, K., Yadav, M., & Kushwah, R. (2020). An analytical survey on the role of machine learning algorithms in case of intrusion detection. *ACCENTS Transactions on Information Security*, *5*(19), 32–35. https://doi.org/10.19101/TIS.2020.517002

[4] Alkadi, O., Moustafa, N., & Turnbull, B. (2020). A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions. *IEEE Access*, *8*, 104893–104917. https://doi.org/10.1109/ACCESS.2020.2999715

[5] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: A review. *IEEE Access*, *6*, 10179–10188. https://doi.org/10.1109/ACCESS.2018.2799854

[6] Drewek-Ossowicka, A., Pietrołaj, M., & Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 497–514. https://doi.org/10.1007/s12652-020-02014-x

[7] Shafay, M., Ahmad, R. W., Salah, K., Yaqoob, I., Jayaraman, R., & Omar, M. (2023). Blockchain for deep learning: Review and open challenges. *Cluster Computing*, *26*(1), 197–221. https://doi.org/10.1007/s10586-022-03582-7

[8] Ajayi, O., & Saadawi, T. (2020). Blockchain-based architecture for secured cyber-attack features exchange. In *2020 7th IEEE International Conference on Cyber Security and Cloud Computing*. 100–107.

[9] Arsenault, R., Martel, J.-L., Brunet, F., Brissette, F., & Mai, J. (2023). Continuous streamflow prediction in ungauged basins: Long short-term memory neural networks clearly outperform traditional hydrological models. *Hydrology and Earth System Sciences*, *27*(1), 139–157. https://doi.org/10.5194/hess-27-139-2023

[10] Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2023). TEBDS: A trusted execution environment-and-blockchain-supported IoT data sharing system. *Future Generation Computer Systems*, *140*, 321–330. https://doi.org/10.1016/j.future.2022.10.016

[11] El Houda, Z. A., Brik, B., & Khoukhi, L. (2022). Ensemble learning for intrusion detection in SDN-based zero touch smart grid systems. In *2022 IEEE 47th Conference on Local Computer Networks*, 149–156. https://doi.org/10.1109/LCN53696.2022.9843645

[12] Janani, K., & Ramamoorthy, S. (2022). Threat analysis model to control IoT network routing attacks through deep learning approach. *Connection Science*, *34*(1), 2714–2754. https://doi.org/10.1080/09540091.2022.2149698

[13] Patel, D., & Patel, D. (2022). Collaborative blockchain based distributed denial of service attack mitigation approach with IP reputation system. In *International Conference on Database Systems for Advanced Applications*, 91–103. https://doi.org/10.1007/978-3-031-11217-1_7

[14] Rahman, Z., Yi, X., & Khalil, I. (2023). Blockchain-based AI-enabled industry 4.0 CPS protection against advanced persistent threat. *IEEE Internet of Things Journal*, *10*(8), 6769–6778. https://doi.org/10.1109/JIOT.2022.3147186

[15] Khonde, S. R., & Ulagamuthalvi, V. (2022). Hybrid intrusion detection system using blockchain framework. *EURASIP Journal on Wireless Communications and Networking*, *2022*(1), 58. https://doi.org/10.1186/s13638-022-02089-4

[16] Abubakar, A. A., Liu, J., & Gilliard, E. (2023). An efficient blockchain-based approach to improve the accuracy of intrusion detection systems. *Electronics Letters*, *59*(18), e12888. https://doi.org/10.1049/ell2.12888

[17] Saveetha, D., & Maragatham, G. (2022). Design of blockchain enabled intrusion detection model for detecting security attacks using deep learning. *Pattern Recognition Letters*, *153*, 24–28. https://doi.org/10.1016/j.patrec.2021.11.023

[18] Kably, S., Benbarrad, T., Alaoui, N., & Arioua, M. (2023). Multi-zone-wise blockchain based intrusion detection and prevention system for IoT environment. *Computers, Materials & Continua*, *74*(1), 253–278. https://doi.org/10.32604/cmc.2023.032220

[19] Rathee, G., Kerrache, C. A., & Ferrag, M. A. (2022). A blockchain-based intrusion detection system using Viterbi algorithm and indirect trust for IIoT systems. *Journal of Sensor and Actuator Networks*, *11*(4), Article 4. https://doi.org/10.3390/jsan11040071

[20] Heidari, A., Navimipour, N. J., & Unal, M. (2023). A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. *IEEE Internet of Things Journal*, *10*(10), 1. https://doi.org/10.1109/JIOT.2023.3237661

[21] Babu, E. S., Bkn, S., Nayak, S. R., Verma, A., Alqahtani, F., Tolba, A., & Mukherjee, A. (2022). Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks. *Computers and Electrical Engineering*, *103*, 108287. https://doi.org/10.1016/j.compeleceng.2022.108287

[22] Aljabri, A., Jemili, F., & Korbaa, O. (2024). Convolutional neural network for intrusion detection using blockchain technology. *International Journal of Computers and Applications*, *46*(2), 67–77. https://doi.org/10.1080/1206212X.2023.2284443

[23] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks. *Arabian Journal for Science and Engineering*, *46*(4), 3749–3778. https://doi.org/10.1007/s13369-020-05181-3

[24] Mansour, R. F. (2022). Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-17043-z

[25] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Kumar, N., & Hassan, M. M. (2022). A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 16492–16503. https://doi.org/10.1109/TITS.2021.3098636

[26] Kumar, P., Kumar, R., Kumar, A., Franklin, A. A., Garg, S., & Singh, S. (2023). Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2802–2813. https://doi.org/10.1109/TNSE.2022.3191601

[27] Mahdavisharif, M., Jamali, S., & Fotohi, R. (2021). Big data-aware intrusion detection system in communication networks: A deep learning approach. *Journal of Grid Computing*, *19*(4), 1–28. https://doi.org/10.1007/s10723-021-09581-z

[28] Li, W., Wang, Y., & Li, J. (2023). A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. *International Journal of Information Security*, *22*(5), 1219–1230. https://doi.org/10.1007/s10207-023-00687-x

[29] Elimelech-Zohar, K., & Orenstein, Y. (2023). An overview on nucleic-acid G-quadruplex prediction: From rule-based methods to deep neural networks. *Briefings in Bioinformatics*, *24*(4). https://doi.org/10.1093/bib/bbad252

[30] Gilliard, E., Liu, J., & Aliyu, A. A. (2024). Knowledge graph reasoning for cyber attack detection. *IET Communications*, *18*(4), 297–308. https://doi.org/10.1049/cmu2.12736

[31] Aliyu, A. A., & Liu, J. (2023). Blockchain-based smart farm security framework for the internet of things. *Sensors*, *23*(18), 7992. https://doi.org/10.3390/s23187992

[32] Tun, T., Wai, K. K., & Khaing, M. S. (2023). Performance of machine learning using preprocessing and classification for intrusion detection system. In *2023 IEEE Conference on*

Computer Applications, 260–265. https://doi.org/10.1109/ICCA51723.2023.10181620

[33] Balla, A., Habaebi, M. H., Elsheikh, E. A., Islam, M. R., & Suliman, F. M. (2023). The effect of dataset imbalance on the performance of scada intrusion detection systems. *Sensors*, *23*(2), 758. https://doi.org/10.3390/s23020758

[34] Song, Y., Hyun, S., & Cheong, Y.-G. (2021). Analysis of autoencoders for network intrusion detection. *Sensors*, *21*, 4294. https://doi.org/10.3390/s21134294

[35] Maseno, E. M., Wang, Z., & Xing, H. (2022). A systematic review on hybrid intrusion detection system. *Security and Communication Networks*, *2022*(1), 9663052. https://doi.org/10.1155/2022/9663052

[36] Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data*, *8*(1), 65. https://doi.org/10.1186/s40537-021-00448-4

[37] Sudharsan, R., & Ganesh, E. N. (2022). A Swish RNN based customer churn prediction for the telecom industry with a novel feature selection strategy. *Connection Science*, *34*(1), 1855–1876. https://doi.org/10.1080/09540091.2022.2083584

[38] Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1), 5. https://doi.org/10.1007/s43926-023-00034-5

[39] Rababah, B., & Srivastava, S. (2020). Hybrid model for intrusion detection systems. *arXiv Preprint:2003.08585*.

[40] Sunanda, N., Shailaja, K., Kandukuri, P. K., Rao, V. S., & Godla, S. R. (2024). Enhancing IoT network security: ML and blockchain for intrusion detection. *International Journal of Advanced Computer Science and Applications*, *15*(4), 947–958. https://doi.org/10.14569/IJACSA.2024.0150497

How to Cite: Aliyu, A. A., Liu, J., & Gilliard, E. (2024). A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS42023803