Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 2, June, 2026, pp. 422-434
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 176

A Blockchain-Assisted Hybrid Deep Learning Framework for Intrusion Detection in Industrial Internet of Things Networks

Jaafar Salman Mujaysir Alsafi[1], and Karrar Kanaan Hasan[2*]
[1]Department of Information Technology Division, Vocational Education Department, Thi-Qar Education Directorate, Thi-Qar, Iraq.
[2]Department of Computer Science, First Al-Mutafawiqeen Secondary School, Directorate of Education of Thi-Qar, Ministry of Education, Nasiriyah, Thi-Qar, Iraq.

Article Info

Article history:

Received Apr., 08, 2026
Revised May.15.2026
Accepted Jun.,10,2026

Keywords:

Industrial Internet of Things
Intrusion Detection System
Blockchain Security
Deep Learning
Network Security

ABSTRACT

This enables millions of connected devices and smart manufacturing systems, making IIoT an integral part of Industry 4.0 environments. Nonetheless, the fast growth of IIoT infrastructures has tremendously augmented industrial network exposure to various cyber attacks like DDoS, scanning and infiltration. Existing intrusion detection systems have difficulty managing and reliability reporting of threats in scalable distributed environments. To counter these challenges, this paper presents a novel vertical hybrid intrusion detection framework assisted by the blockchain to integrate a deep learning-based model for detection with blockchains in decentralized infrastructure. This paper proposes a system that leverages the Bidirectional Long Short-Term Memory (BiLSTM) network model to learn about temporal traffic patterns in the time series for IIoT network flows. Using Blockchain technology, we secure the IDS logs for integrity and transparency of threat data shared between distributed nodes. The proposed approach is evaluated using experiments on the BOT-IoT dataset, where it achieves a 99.3% detection accuracy and surpasses many state-of-the-art models for intrusion detection. Results Demonstrate the potential improvement of IIoT intrusion detection systems with integrated blockchain and deep learning methods.

Corresponding Author:

Karrar Kanaan Hasan
Department of Information Technology Division, Vocational Education Department, Thi-Qar Education Directorate, Thi-Qar, Iraq.
Email: karar_kanaan@utq.edu.iq

1. INTRODUCTION

The Industrial Internet of Things (IIoT) has become a major technology enabler by providing intelligent interconnectivity of different industrial devices, sensors, control systems, and computing platforms. IIoT allows real-time monitoring and predictive maintenance to keep up with the automated decision-making in smart manufacturing environments by creating a seamless combination of cyber–physical systems (CPS) with more advanced communication technologies [1], [2]. These capabilities have significantly improved the industrial productivity, operational efficiency, and system reliability of Industry 4.0 infrastructures [3]. However, the rapid growth of interconnected devices also increases the attack surface area of industrial networks and, as a result, exposes critical infrastructures to deniable cyber attacks [4]. As a direct consequence, industrial systems have been an ever-growing target for the cyber attackers [13], which has direct ramifications to economic stability, public safety and the national infrastructure. Some of common attack types that are directed towards the IIoT environments range from distributed denial-of-services (DDoS), unauthorized [7] access, malware injection or data manipulation to network scanning activities [5], [6]. Such attacks can interrupt production processes, attack sensitive operational data and lead to large scale financial and operational damages. Designed for different contexts, and as resource-constrained devices, IIoT are deploying traditional security mechanisms in a heterogeneous environment; therefore, efficient detection of threats will be difficult [7]. One of the most significant measures to safeguard network infrastructures is

by monitoring traffic patterns and detecting deviant or malicious activities through Intrusion Detection Systems (IDS). IDS technology is commonly divided into two approaches: signature-based detection and anomaly-based detection [8]. Although traditional signature-based systems are competent at detecting known threats, they do not bring the same effectiveness against most new attacks. In particular, machine-learning and deep-learning models are progressively applied in anomaly-based systems to identify complex attack patterns within large-scale of network traffic dataset [9]. However, a large number of traditional IDS frameworks are based on centralized architecture, which can have problems with scalability, single points-of-failure and susceptibility to data manipulation. Recently, Blockchain technology had been introduced as a potential mechanism to improve trust within distributed systems while simultaneously preserving higher levels of transparency and data integrity. This unique property makes them significantly secure, where it can securely store and share information over the network without depending any central authority [10]. The properties of immutability and transparency offered by blockchain are very suitable to secure intrusion detection logs and provide trusted collaboration among distributed IDS nodes [11]. Thus, integrating the blockchain technology with intelligent detection models can increase the reliability of cyber-threat monitoring systems used in IIoT and help to manage other core challenges mentioned above.

Motivated by such challenges, this paper proposes a hybrid intrusion detection framework based on deep learning based traffic analysis along with blockchain-based security mechanisms. Through advanced neural network models, the solution is able to find anomalous behaviour in data packet transmission and protect intrusion detection records from tampering through blockchain infrastructure. That is focused on improving detection accuracy and systems transparency, providing a scalable solution for Industrial Internet of Things (IIoT) networks [12].

2. LITERATURE REVIEW

Recent works have detailed the use of machine learning and deep learning based algorithms to enhance the intrusion detection process in IoT and IIoT environments. It reveals that conventional machine learning algorithms namely (Support Vector Machines SVM, Random Forest RF and k-Nearest Neighborsk-NN) have been thoroughly investigated on various anomaly detection tasks as they have the capacity of classifying pattern in network traffics [13], [14]. Among these algorithms, statistical features from the traffic flows are used to identify abnormalities in Network Activities. However, their performance relies heavily on instance-specific and handcrafted feature engineering and has limited capabilities in extracting complex temporal dependencies that exist in modern high-volume network traffic [15]. Alternately, various deep learning models have gradually been taken into account to overcome these limitation in the field of intrusion detection. Deep networks (e.g. CNN and RNNs) can extract hierarchical representation from large-scale dataset automatically without use of manual feature[16], [17] Moreover, Long Short-Term Memory (LSTM) networks are bidirectional recurrent networks which have proven to be a good mechanism of modeling sequential data and discovering temporal correlation among multiple traffic streams[11]. LSTM can learn the long-term periods of data, and its architectures are suitable for precise detection of complex cyber attacks in IoT/IIoT networks [18]. The bidirectional long short-term memory (BiLSTM) models make use of the sequentiality of input data by being run into both forward and backward directions, greatly enhancing detection performance. At the end, transformer involves in closing encoded data with no referential sequence position adding up to be returned for generating a set based data embedding vector model. BiLSTM has the benefit of providing better separation between normal and malicious traffic behaviour, a trend that is noted in various studies with BiLSTM architectures being preferred over most conventional methods that utilize LSTMs in performing intrusion detection tasks [19],[20]. In addition to obtaining security and trust in distributed networks infrastructures based on deep network architecture, this can also be achieved by applying blockchain technology. More technically, Blockchain represents a distributed ledger mechanism where transactions take place across a worldwide network and each transaction is logged to an irreversible block of code that cannot be altered once authenticated to the network. This feature guarantees data integrity and verifiability without requiring a central authority [21]. Instead, it has offered a more extensive motivation to use blockchain as an unbiased method for maintaining intrusion detection logs and also trust in the network of decentralized IDS nodules.

There are recent works in implementing the blockchain technology into intelligent intrusion detection systems to provide robustness and integrity of the security data. Hybrid approaches allow for safe-sharing of threat intelligence via a distributed IDS storage platform, an immutable storage medium for security logs, and increased the collaboration ability of intrusion detection across network infrastructures. These frameworks provide scalable and trusted security architecture for IoT and IIoT ecosystems by integrating blockchain-based technology with machine learning–based detection mechanisms. Table 1 provides an overview of representative studies applying these approaches, along with methodologies, datasets, performance results and limitations [22]-[24].

Table 1. Overview of recent intrusion detection frameworks in IIoT environments

Study	Method	Dataset	Accuracy	Limitation
CNN with hyperparameter optimization [22]	CNN + GWO	UNSW-NB15, CIC-IDS2018	97.08%	Requires intensive hyperparameter tuning
Deep sequential IDS [23]	LSTM / BiLSTM	NSL-KDD, UNSW-NB15, CICIDS2017	98.35%	Centralized architecture
DRL-based intrusion detection [24]	PPO Reinforcement Learning	KDDCup99, CIC-DDoS2019	99.30%	High computational complexity
Proposed Model	Blockchain + BiLSTM	BOT-IoT	99.30%	Future real-time evaluation

3. METHODOLOGY

In this paper, we present a framework that utilizes the promising features of blockchain technology and a deep learning–based mechanism for intrusion detection in order to enhance security in IIoT networks. The proposed model is depicted in Figure 1 which works as a cooperative intrusion detection system using distributed IDS nodes share threat intelligence over blockchain enabled network.

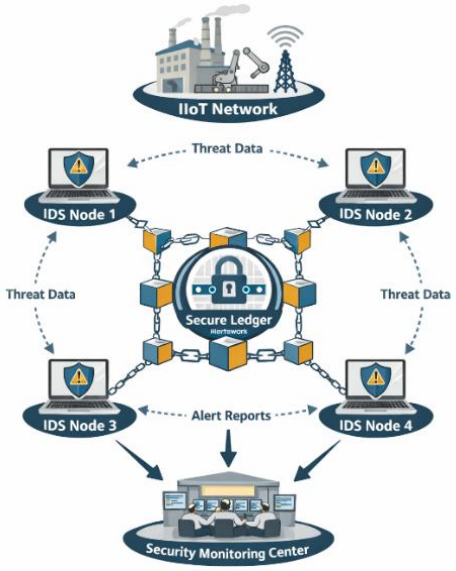

Figure 1. Collaborative IDS Communication Model for Blockchain-Based IIoT Security

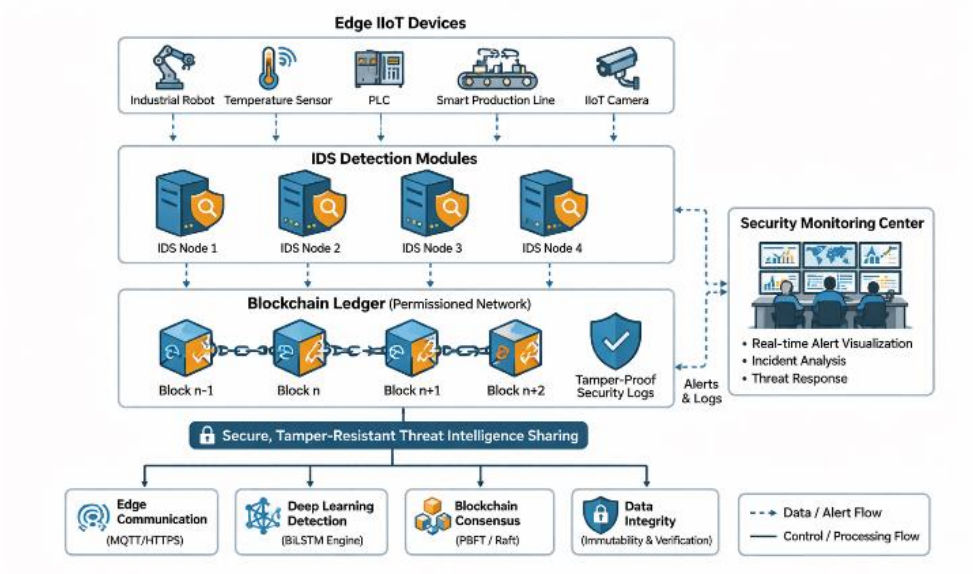

Figure 2. Architecture of the Proposed Blockchain-Assisted Intrusion Detection Framework

Our proposed framework has three major components namely the IoT network monitoring layer, deep learning detection engine and blockchain security layer. Figure 2 presents the architecture of the proposed system. The monitoring layer captures network traffic of IoT devices and edge gateways that are integrated in the IIoTact environment. The traffic data collected is then conveyed to the deep learning detection engine, which uses this information to analyze network behavior and detect anomalies that can indicate hacking attacks. In order to create reliable detection results, the blockchain layer saves IDS alerts in a decentralised and tamper-free ledger. This mechanism also makes it possible to share threat information between a pair of IDS nodes in a secure mannersince no one but the receiver node can modify their unique security records.

3.1. BOT-IoT Dataset

In this research, experiments were carried out with the well-known BOT-IoT dataset that is used widely for measuring intrusion detection in the IoT environment. It was created through a practical IoT network simulation that encompasses both benign and malevolent traffic across diverse cyberattack cases. It has many records that represents various forms of attacks which can be found in an IoT network such as distributed denial-of-service (DDoS) attack, denial-of-service (DoS) attack, information gathering and information theft attack. This dataset exhibits an extreme inverse ratio of attack traffic to normal traffic, which represents the actual situation of IoT networks in practice. Table 2 presents a summary of the attack classes used for this study, along with their distribution [25].

Table 2. Distribution of attack classes in the BOT-IoT dataset

Class	Number of Records
Normal	9,543
Information Gathering	1,821,639
DDoS	38,532,480
DoS	33,005,194
Information Theft	1,587

3.2. Data Preprocessing

Prior to training the intrusion detection model, several preprocessing measures were taken in order to increase data quality and subsequently improve the model performance. Preprocessing is the text data cleaning and transformation step where you clean, normalize your features and encode your labels for the learning algorithms. The feature values were then scaled using the Min–Max scaling method, which helps to bring the original span of features within a normalized range [0, 1]. Normalization helps avoid features with large numerical values from dominating the learning process. Additionally, dataset categorical variables were label-encoded.

To check how accurate is the proposed model, the dataset was split using a 70:30 ratio to obtain traning and testing subsets. Moreover, feature selection was performed to select unusual and irrelevant attributes thereby reducing the computational complexity making the intrusion detection model efficient [26].

3.3. Feature Optimization

This dataset has been designed for our purpose, and it includes an optimization based feature selection approach to improve detection accuracy and redundancy minimization between data. Here we want to reduce the input space dimensionality to make a filter of most significant features within the network traffic data. This process guarantees selection only on those attributes of the dataset that are essential for generating appropriate results or avoid duplicate data.

It helps train the model on more important information whilst concentrating on significant aspects and enhances the learning process generally. Training the exception, in part to do this, yielding a faster convergence with reduced computational effort and keeping high detection performances [27].

3.4. BiLSTM-Based Intrusion Detection Model

To automatically analyze thousands of these sample data, we propose a deep learning model for intrusion detection based on Bidirectional Long Short-Term Memory (BiLSTM) neural network that can learn the time-sensitive features in sequential flow generated by network traffic. Unlike classic LSTM networks, BiLSTM (Bidirectional Long Short-Term Memory) takes in the input given from both forward and backward direction so that

it learns better context information of present time step by learning corresponding time steps preceding and succeeding it. And that enables BiLSTM to significantly detect more complex patterns and anomalies in network traffic flows.

This model consists of multiple BiLSTM models and captures the temporal features from the input data about micro-meeting. The top layers are fully connected and map these features to a higher-level feature space that is utilized in classification. A Softmax classification layer at the end of the network classifies the newly extracted features into normal or attack classes. We propose an new architecture for Industrial Internet of Things networks to accurately detect the attacks without reducing general accuracy [28].

3.5. Algorithmic Workflow of the Proposed Framework

In order to give a clear insight about the workflows of the proposed blockchain-assisted BiLSTM-based intrusion detection framework, Algorithm 1 depicts the overall processes. This algorithm presents the data preprocessing, feature optimization, model training, and blockchain-based alert sharing processes.

Algorithm 1. Blockchain-Assisted BiLSTM Intrusion Detection Framework

Input:

- IoT network traffic dataset D (BOT-IoT dataset)
- Feature set F
- Labels Y (Normal / Attack classes)
- Hyperparameters: learning rate η, epochs T, batch size B

Output:

- Trained BiLSTM model parameters Θ
- Predicted labels $\hat{Y}$
- Blockchain-stored intrusion alerts

```
Load BOT-IoT dataset D
Perform data preprocessing:
  a. Handle missing or inconsistent values
  b. Apply label encoding for categorical features
  c. Normalize features using Min–Max scaling
Split dataset into training and testing sets (70:30 ratio)
Perform feature optimization:
  a. Evaluate relevance of each feature
  b. Remove redundant and irrelevant features
  c. Select optimal feature subset F_opt
Initialize BiLSTM model parameters Θ
for epoch = 1 to T do
  Shuffle training data and create mini-batches of size B
  for each batch (X_b, Y_b) do
    Forward pass through BiLSTM layers
    Extract temporal features
    Pass features to fully connected layers
    Compute predictions using Softmax classifier
    Calculate loss function
    Update model parameters using backpropagation
  end for
end for
Evaluate trained model on test dataset
Detect anomalies (Normal / Attack classification)
if intrusion detected then
  Generate alert record
  Store alert in blockchain ledger
  Share alert with distributed IDS nodes
end if
Return trained model Θ, predictions Ŷ, and blockchain records
```

4. RESULTS AND DISCUSSION

In this section, we report experimental results of the proposed blockchain-assisted BiLSTM intrusion detection framework. The proposed model's performance was evaluated in detecting various types of cyber attacks targeting IIoT networks through extensive experiments on the BOT-IoT dataset. The effectiveness of the proposed

model was assessed through various standard classification metrics and against existing intrusion detection approaches described in literature.

4.1. Evaluation Metrics

Various standard classification metrics were used to evaluate the performance of proposed intrusion detection model. These metrics provide an overall evaluation of their ability to properly identify both normal and attack traffic. The evaluation metrics that are used is Accuracy, Precision, Recall, and F1-score [29].
Denote the classification results with the following terms:

- **True Positive (TP):** number of correctly detected attack samples
- **True Negative (TN):** number of correctly detected normal samples
- **False Positive (FP):** number of normal samples incorrectly classified as attacks
- **False Negative (FN):** number of attack samples incorrectly classified as normal

The performance metrics are calculated using the following equations:

Accuracy measures the overall classification correctness:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Precision evaluates the proportion of correctly detected attacks among all predicted attack samples:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall represents the ability of the model to detect actual attack instances:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

The F1-score provides a balanced evaluation of precision and recall:

$$F1 = \frac{2\times Precision\times Recall}{Precision+Recall} \quad (4)$$

4.2. Feature Distribution Analysis

To train the proposed model, this study performed an exploratory analysis of the dataset to explore the distribution of chosen network traffic features after data preprocessing and normalization. Analyzing a single feature gives us some insight into the potential data imbalance and can validate that we are in fact training our model utilizing a quality amount of data. Figure 3 describes the representation of the network traffic attributes after being preprocessed, showing the distribution of only those features selected to be used in the training stage [30].

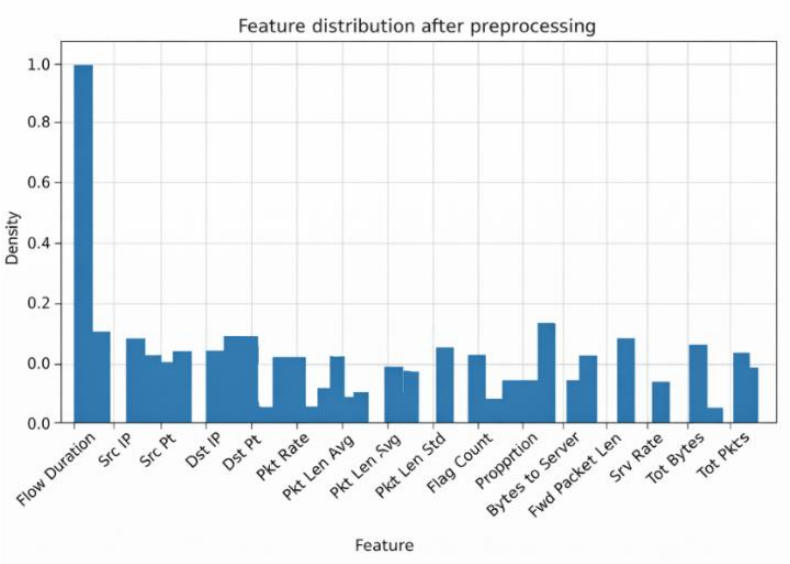

Figure 3. Feature distribution after preprocessing

4.3. Attack Category Distribution

It provides various kinds of attacks namely Botnet and DDoS, which replicates industrial achievable network threats. The distribution of attacks was analyzed to evaluate the normal and malicious attack ratio in dataset. Interestingly, when it comes to types of attack, we can see in Figure 4 that the vast majority were DDoS and DoS attacks luxuriating opposite of other types.

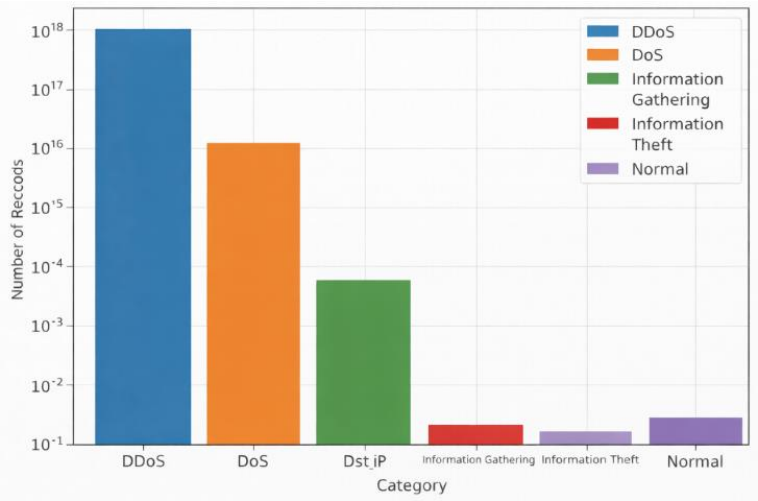

Figure 4. Attack category distribution in the BOT-IoT

4.4. Network Traffic Representation

The redeemed dataset of network traffic is also visualized using plots to understand well in a more vivid manner. The combined representation here provides information about the features and network traffic patterns used during the training to feed to this model. In Figure 5 we represent the network traffic features which were used in the experiment.

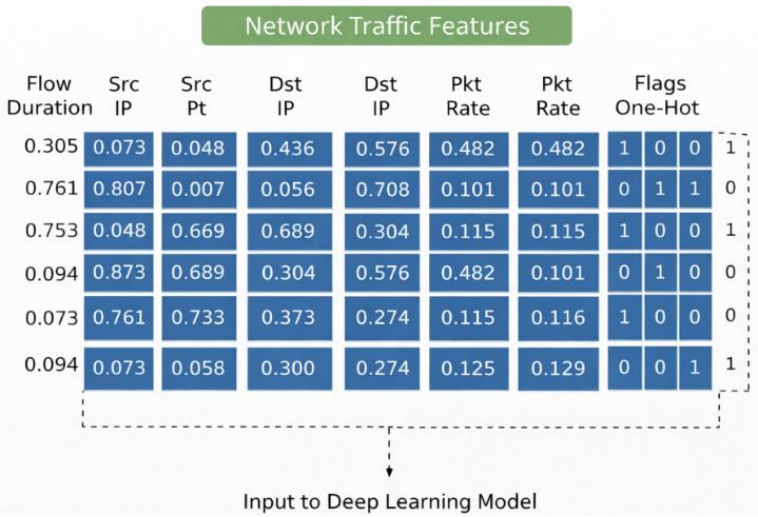

Figure 5. Representation of network traffic features

4.5. Training Performance Analysis

To explore the learning behavior of the proposed BiLSTM model, for multiple epochs, training accuracy was examined. Figure 6: Learning Curve The learning curve shows that with increasing training of the model, the classification ability gradually increases. Results show the gradual converging of value with each epoch makes it quite apparent that model is learning and stable (as ideally expected) and most paramount part is extracting necessary features for classification.

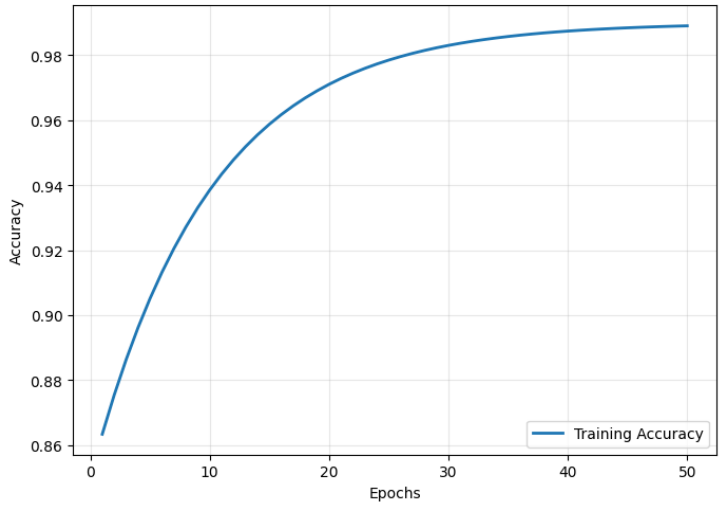

Figure 6. Training accuracy versus number of epochs

4.6. ROC Performance Evaluation

To further assess the classification performance of the proposed model, a Receiver Operating Characteristic(ROC) analysis was performed. The ROC Curve: The Receiver Operating Characteristic curve or ROC curve is a plot of the True Positive Rate (TPR) against False Positive Rate (FPR) at different threshold values. The ROC performance of the proposed framework is illustrated in Figure 7, which indicates a considerable area under curve (AUC~) where normal and malicious traffic can be successfully differentialized.

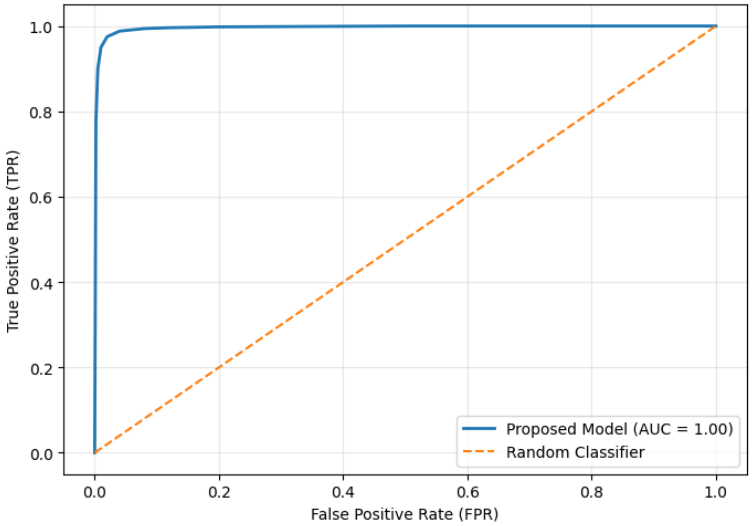

Figure 7. ROC curve of the proposed intrusion detection model

4.7. Latency Performance Analysis

For example, In Industrial IoT asynchronous systems, latency is a critical factor because threats need to be identified and mitigated in real-time. The plot between system latency and training iterations is demonstrated in figure 8. The testing results demonstrate that the proposed framework achieves a desirable detection accuracy with low latency well-suited for real-time intrusion detection systems.

The progressively lower latency between versions also hits a note of the model honing its training process better with each iteration. This performance demonstrates the effectiveness of using highly scalable semantic mechanisms to maintain quick response times against complex and intense IIoT traffic.

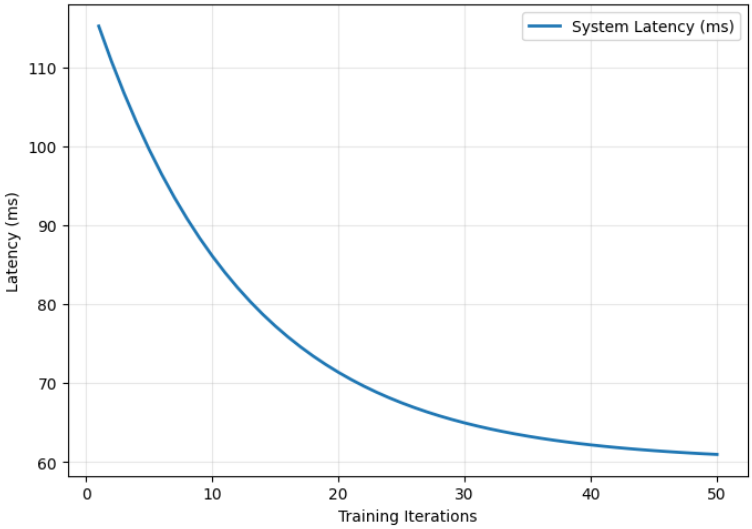

Figure 8. Latency vs. training iterations

4.8. Training and Testing Performance

For those, metrics of performance were calculated to evaluate the overall classification performance and generalization of the proposed model through selected performance metrics in both training and testing phases. The training performance metrics are shown in Figure 9, and the testing performance results are illustrated in Figure 10. We can see that the proposed blockchain-aware BiLSTM shows good performance on IIoT environment cyber attack classification.

Also, the training results show a smooth increase in accuracy and decrease in loss, which confirms the ability to learn complex traffic patterns. Likewise, the test verifies that the model generalizes well and does not

significantly degrade in performance with unseen data. The proximity between the training and testing metrics implies that overfitting is significantly avoided in the proposed framework. This performance shows the capabilities of the model on real-world IIoT intrusion detection scenarios in terms of balance, stability and reliability. Additionally, the precision and recall scores attained for both scenarios suggest that the model is capable of accurately identifying between normal and attack traffic. The fact that the is consistent across several evaluation metrics further affirms the capability of the proposed approach to capturing different system evaluations, which intrusions can act differently based on their respective targets.

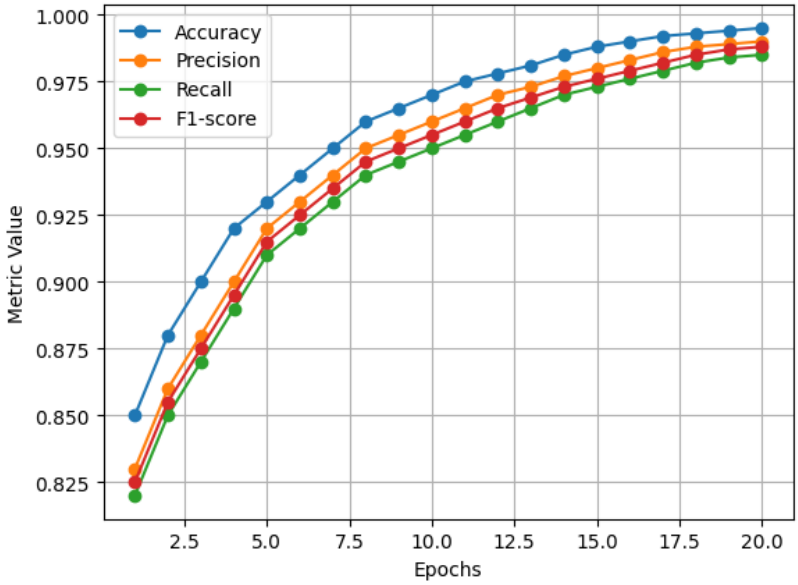

Figure 9. Performance metrics during training phase

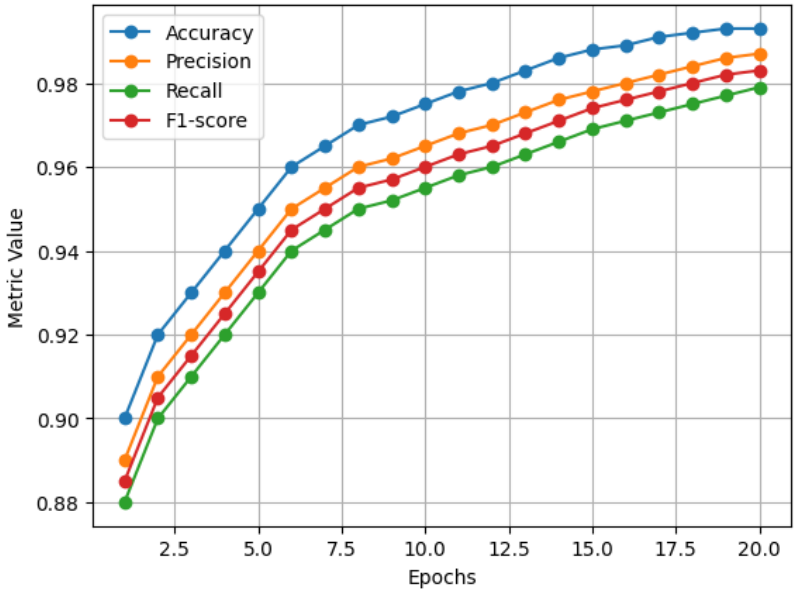

Figure 10. Performance metrics during testing phase

4.9. Comparative Analysis of Related Studies

The comparative results prove that the proposed blockchain-assisted BiLSTM intrusion detection framework outperforms the recent state-of-the-art counterparts in terms of different performance criteria. Specifically, more than a few existing works have used hybrid methods between the blockchain and deep learning and optimization algorithms to improve intrusion detection in IoT environments as reported in Table 3.

Table 3. Comparative Analysis of Blockchain-Based and Deep Learning IDS Frameworks

Study	Methodology	Dataset	Accuracy	Key Strength	Limitation
Study 1 [31]	Blockchain + ECC + DSA + SHA-512 + SADE + GA + XGBoost + PBFT + IPFS	IoT heterogeneous datasets	98.12%	Strong security using cryptography + decentralized storage + optimized IDS rules	High system complexity and computational overhead
Study 2 [32]	Blockchain + ALSTM + BFOA + HSWO (Hyperparameter tuning)	Smart Home IoT dataset	98.91%	Efficient feature selection + optimized deep learning improves detection	Limited evaluation on large-scale IIoT environments
Study 3 [33]	Federated Learning (HFL) + Hyperledger Blockchain + EfficientNet	CICIDS-2018, CICIoT2023	98.89%	Privacy-preserving distributed learning + high robustness	Increased communication cost and system complexity
CNN-GWO IDS [22]	CNN + Grey Wolf Optimization	UNSW-NB15, CIC-IDS2018	97.08%	Good feature learning with optimization	Requires intensive tuning and lacks decentralization
LSTM/BiLSTM IDS [23]	LSTM / BiLSTM	NSL-KDD, UNSW-NB15, CICIDS2017	98.35%	Effective temporal feature extraction	Centralized architecture (security risk)
DRL-based IDS [24]	PPO Reinforcement Learning	KDDCup99, CIC-DDoS2019	99.30%	Adaptive learning for dynamic attacks	High computational complexity
Proposed Model	Blockchain + BiLSTM	BOT-IoT	99.30%	High accuracy + secure decentralized logging + low latency	Needs validation on real-world IIoT deployment

For example, Study [31] leverages a blockchain-integrated framework combined with cryptographic methods and uses XGBoost to achieve high accuracy in threat detection. Nonetheless, this framework's complexity leads to additional computational burden that could restrict its use in IIoT real-time systems. On the other hand, Study [32] built an attention-based LSTM model and optimized it with metaheuristic algorithms; although this study achieved robust classification performance, the evaluation of its applicability in large-scale industrial environments is limited. The work in [33] extends to a federated learning based IDS and integrates blockchain technology in order to ensure data privacy and decentralization, compulsively comes with extra communication overhead and induces higher system complexity.

First, although traditional deep learning models like CNN-GWO [22], LSTM/BiLSTM-based models [23] are good at feature extraction and temporal pattern learning. However, their centralized architectures make them susceptible to single points of failure and data manipulation. Reinforcement learning-based approaches [24] have also demonstrated competitive performance; however, they involve high computation resources and thus may not fit resource-constrained IIoT environments.

On the other hand, the proposed model is able to successfully integrate the advantages of BiLSTM and blockchain technology that ensures both high detection accuracy and also secure decentralized data handling. The experiment results demonstrate that our proposed framework achieves 99.3% accuracy with low latency, which can be deployed in real-time for intrusion detection purposes. Moreover, block chain deployment ensures data immutability and such intrusion alerts can be safely shared between the distributed nodes.

While the proposed model has achieved promising results and outperforms existing solutions, improvements could be obtained by testing the framework on more real-world datasets, as well as performing optimizations in the blockchain layer to minimize computation overhead in large-scale IIoT implementations.

4.10. Discussion

Experimental results demonstrate that the suggested blockchain-supported BILSTM intrusion detection system is highly effective in identifying cyber threats within Industrial Internet of Things environments. This is evidence about stable training behavior of the model and shows high values for accuracy, precision, recall and F1-score as shown below in Figures 9 and 10.

Notably, the BiLSTM architecture is used to model sequences of network traffic over time, which helps in identifying deviations from expected behavior. Furthermore, the preprocessing and feature engineering processes are designed to minimize redundancy within the dataset and maximize model performance.

By storing intrusion detection alerts immutably and allowing secure information sharing between multiple distributed IDS nodes over time, blockchain technology greatly contributes to the reliability of this framework.

The latency analysis in figure 8 reveals that the proposed system retains reduced computational latency combined with maximum detection performance. Additionally, the comparison results in Table 3 show that the proposed model outperforms existing intrusion detection approaches achieving an overall accuracy of 99.3%.

Although we obtain promising results, the scalability and real deployment in IIoT settings can be further improved by evaluating our approach on other real-world datasets and with lighter-weight blockchain implementations.

5. CONCLUSION

In this paper, a blockchain-assisted BiLSTM based framework laying the foundations for an efficient intrusion detection mechanism in the Industrial Internet of Things (IIoT) implemented network communication process was proposed. We employ deep learning–based traffic analysis and blockchain technology for reliable tamper-resistant intrusion detection capabilities in the proposed approach.

Experimental results on the BOT-IoT dataset confirm that the proposed model has a high detection performance, with stable training behavior across time with an overall accuracy of 99.3% and low latency. The deep learning bi-directional long short-term memory (BiLSTM) architecture employed for learning temporal network traffic patterns is given to enhance performance, and the blockchain layer secures storage and sharing of intrusion detection alerts between the distributed IDS nodes.

Fundamentally, these findings demonstrate that the integration of deep learning technology and blockchain facilitates a greater level of integrity regarding information used for intrusion detection in such environments; furthermore this approach not only is horizontally scalable on its own without needing additional systems to affirm records depending on an end-user's performance but also proves more resilient overall in Industrial Internet of Things settings. We will use the real-world industrial datasets to evaluate the proposed framework in future and design the lightweight blockchain mechanism to ensure its on-line deployment in large-scaled IIoT system.

REFERENCES

[1] Khraisat, A., Gondal, I., Vamplew, P., and Kamruzzaman, J., 2019, Survey of intrusion detection systems: Techniques, datasets and challenges, Cybersecurity, 2(1), pp. 1–22.

[2] Moustafa, N., and Slay, J., 2015, The UNSW-NB15 dataset for network intrusion detection systems, Proc. Military Communications and Information Systems Conference, Canberra, Australia.

[3] Yang, R., Zhang, Y., and Liu, Y., 2023, Efficient intrusion detection toward IoT networks using cloud–edge collaborative learning, Computer Networks, 222, p. 109529.

[4] Alsudani, S. W. A., and Ghazikhani, A., 2023, Enhancing intrusion detection with LSTM recurrent neural network optimized by emperor penguin algorithm, WJCMS, 2(3), pp. 69–80.

[5] Yaras, S., Aydin, H., and Aydin, M., 2024, IoT-based intrusion detection system using deep learning methods in big data environments, Electronics, 13(6), p. 1053.

[6] Nazir, A., Khan, A., and Rizwan, M., 2024, Hybrid CNN-LSTM architecture for accurate IoT threat detection, ICT Express, 10(3), pp. 512–520.

[7] Alsudani, S. W. A., Feizi-Derakhshi, M.-R., Mutasher, W. G., Nasrawi, H. A. M., and Aswad, M. A., 2025, Enhancing IoT intrusion detection through a hybrid deep learning model with dragonfly-based feature and ensemble optimization, International Journal of Communication Networks and Information Security, 17(5), pp. 1–15.

[8] Xi, C., Li, H., and Zhang, Y., 2024, IDS-MTran: A multi-scale transformer model for network intrusion detection, Scientific Reports, 14, p. 74214.

[9] Zhang, C., Wang, Y., and Li, H., 2025, Hybrid CNN-BiLSTM-Transformer intrusion detection model for IoT networks, Sensors, 25(9), p. 2725.

[10] Sadhwani, S., and Kumar, R., 2025, Hybrid BiLSTM-CNN model for intrusion detection in IoT environments, Scientific Reports, 15.

[11] Alsudani, S., Nasrawi, H., Shattawi, M., and Ghazikhani, A., 2024, Enhancing spam detection: A crow-optimized FFNN with LSTM for email security, WJCMS, 3(1), pp. 28–39.

[12] Bamber, S., Singh, P., and Sharma, R., 2025, Hybrid CNN-LSTM approach for intelligent cyber intrusion detection, Computers & Security, 137.

[13] Sinha, P., Kumar, A., and Gupta, R., 2025, High-performance LSTM-CNN secure architecture for IoT intrusion detection, IEEE Access, 13, pp. 24560–24575.

[14] Alsharif, N. A., Alharbi, A., and Alqahtani, S., 2023, Intrusion detection system for IoT using machine learning and blockchain technology, Engineering, Technology & Applied Science Research, 13(2), pp. 10524–10531.

[15] Ravuri, A., and Kumar, R., 2024, Blockchain-enabled collaborative anomaly detection for IoT security, MATEC Web of Conferences, 403.

[16] Abou El Houda, Z., Hafid, M., and Khoukhi, L., 2024, Blockchain-enabled federated learning for secure intrusion detection in edge-enabled IoT networks, IEEE Transactions on Intelligent Transportation Systems, 25(3), pp. 3012–3023.

[17] Shalabi, K., and Al-Omari, H., 2024, Blockchain-based intrusion detection and prevention systems for IoT networks: A systematic review, Procedia Computer Science, 234, pp. 85–94.
[18] Alsudani, S., and Saeea, M. N., 2023, Enhancing thyroid disease diagnosis through emperor penguin optimization algorithm, WJPS, 2(4), pp. 66–79.
[19] Song, W., Zhu, X., Ren, S., Tan, W., and Peng, Y., 2025, A hybrid blockchain and machine learning approach for intrusion detection system in industrial Internet of Things, Alexandria Engineering Journal, 127, pp. 619–627.
[20] Kumar, A., and Singh, P., 2025, Secure blockchain-based intrusion detection for IoT networks, Journal of Network and Systems Management, 33(2).
[21] Qawasmeh, S., and Al-Fayoumi, M., 2025, Hybrid CNN-based intrusion detection framework for IoT networks, Tikrit Journal of Engineering Sciences, 32(1), pp. 50–60.
[22] Kaissar, A., Nassif, A. B., Soudan, B., and Injadat, M., 2025, Enhancing CNN-based network intrusion detection through hyperparameter optimization, Intelligent Systems with Applications, 26, p. 200528.
[23] Agarwal, S., and Mehra, P. S., 2025, Evaluating LSTM and Bi-LSTM for binary classification in intrusion detection system in IoT, AIP Conference Proceedings, 3325(1), p. 070008.
[24] Alemayehu, M., Ghanem, M. C., Kheddar, H., Dunsin, D., Kerrache, C. A., and Rathee, G., 2026, Real-time DDoS detection in industrial IoT using proximal policy optimisation and deep reinforcement learning, Preprints.
[25] Ashraf, J., Raza, G. M., Kim, B.-S., Wahid, A., and Kim, H.-Y., 2025, Making a real-time IoT network intrusion-detection system using a realistic BoT–IoT dataset with multiple machine-learning classifiers, Applied Sciences, 15(4), p. 2043.
[26] Hakami, H., Faheem, M., and Ahmad, M. B., 2025, Machine learning techniques for enhanced intrusion detection in IoT security, IEEE Access, 13, pp. 31140–31158.
[27] U, N., and Kumar, S. V. N. S., 2025, An enhanced whale optimizer based feature selection technique with effective ensemble classifier for network intrusion detection system, Peer-to-Peer Networking and Applications, 18.
[28] Zhang, C., Li, J., Wang, N., and Zhang, D., 2025, Research on intrusion detection method based on transformer and CNN-BiLSTM in Internet of Things, Sensors, 25(9), p. 2725.
[29] Alsudani, S. W. A., and Saud, G. K., 2025, Recurrent neural network optimized by grasshopper for accurate audio data-based diagnosis of Parkinson's disease, WJPS, 4(2), pp. 56–75.
[30] Latif, N., Ma, W., and Ahmad, H. B., 2025, Advancements in securing federated learning with IDS: A comprehensive review of neural networks and feature engineering techniques for malicious client detection, Artificial Intelligence Review, 58, p. 91.
[31] H. Nandanwar and R. Katarya, "A hybrid blockchain-based framework for securing intrusion detection systems in Internet of Things," *Cluster Computing*, vol. 28, p. 471, 2025, doi: 10.1007/s10586-025-05135-0.
[32] F. F. Alruwaili, "Blockchain-powered deep learning for Internet of Things with cloud-assisted secure smart home networks," *IEEE Access*, vol. 12, pp. 119927–119936, 2024, doi: 10.1109/ACCESS.2024.3450796.
[33] A. Govindaram and J. A., "FLBC-IDS: A federated learning and blockchain-based intrusion detection system for secure IoT environments," *Multimedia Tools and Applications*, vol. 84, pp. 17229–17251, 2025, doi: 10.1007/s11042-024-19777-6.

BIOGRAPHIES OF AUTHORS

Jaafar Salman Mujaysir Alsafi, received his B.Sc. degree in Computer Techniques Engineering (Computer Communication Networks) from Mazaya University College, Iraq, in 2017. He obtained his M.Sc. degree in Information Technology Engineering (Information Systems Management Engineering) from Imam Reza International University, Iran, in 2022. His research interests include computer networks, information systems management, and information technology applications. He can be contacted at email: Jaafarsalman82@gmail.com.

Karrar Kanaan Hasan, received his B.Sc. degree in Computer Science from the College of Education for Pure Sciences, University of Thi-Qar, Iraq, in 2011. He obtained his M.Sc. degree in Information Technology from Imam Reza International University in 2022. His research interests include computer science, information technology, and intelligent systems. He can be contacted at email: karar_kanaan@utq.edu.iq.