IJISIT

http://ejournal.gevivapublisher.org/index.php/ijisit

Explainable Blockchain-Enabled Intrusion Detection Framework for Secure and Trustworthy 5G-IIoT Networks

[1]Joe Silitonga, Ericsson Telecomunication Pte Ltd , Singapore
[2]Rijos Iboy Erwin Saragih, Universitas Methodist Indonesia, Indonesia

Correspondence: E-mail: rijoissaragih@gmail.com

Article Info

Article history:

Received April 20, 2026
Revised May 13, 2026
Accepted June 16, 2026

Keywords:

5G-IIoT,
Intrusion Detection System (IDS),
Explainable Artificial Intelligence (XAI),
Blockchain,
CNN-LSTM,
SHAP,
Cybersecurity,
Trust Management.

ABSTRACT

The integration of 5G networks and the Industrial Internet of Things (IIoT) enables real-time industrial automation but also expands the cybersecurity attack surface. Although previous studies have proposed AI and blockchain-based security frameworks, intrusion detection in 5G-IIoT remains limited by black-box AI models, low interpretability, and blockchain mechanisms that mainly support logging rather than attack detection. This study proposes an Explainable Blockchain-Enabled Intrusion Detection System (XB-IDS) for secure 5G-IIoT networks. The framework integrates deep learning-based intrusion detection, SHAP-based explainability, and blockchain-enabled security logging with smart contracts. A hybrid CNN-LSTM model is used to detect spatial and temporal attack patterns, while SHAP provides interpretable explanations for security analysts. Public IIoT cybersecurity datasets such as TON_IoT, Edge-IIoTset, and CICIoT2023 are used for evaluation. The proposed framework is assessed using accuracy, precision, recall, F1-score, false positive rate, detection latency, throughput, and explainability analysis. The proposed XB-IDS aims to improve detection performance, transparency, and trustworthiness in 5G-IIoT security operations. This study contributes an experimentally evaluable framework that extends prior AI-blockchain security research toward explainable and accountable intrusion detection.

1. INTRODUCTION

The rapid deployment of Fifth-Generation (5G) communication technology has accelerated the adoption of the Industrial Internet of Things (IIoT) across manufacturing, energy, transportation, healthcare, and smart infrastructure sectors [1], [2]. By providing ultra-low latency, high bandwidth, and massive machine-type communications, 5G enables industrial systems to support real-time monitoring, autonomous operations, and intelligent decision-making [24]. The integration of 5G and IIoT has significantly improved operational efficiency and productivity; however, it has also introduced new cybersecurity challenges due to the increasing number of interconnected devices, heterogeneous network architectures, and expanded attack surfaces [3], [24].

Cyberattacks targeting IIoT environments have become increasingly sophisticated, ranging from Distributed Denial-of-Service (DDoS) attacks and botnet infections to data

manipulation and unauthorized access [5], [10]. Traditional security mechanisms, including signature-based intrusion detection systems, often struggle to identify emerging and previously unseen attacks [7], [14]. Consequently, Artificial Intelligence (AI) and Machine Learning (ML) techniques have been widely adopted to enhance threat detection capabilities through intelligent analysis of network traffic and device behavior [8], [10]. Deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and hybrid architectures have demonstrated promising performance in detecting complex attack patterns within IoT and industrial networks [6], [8], [20].

Recent studies have also highlighted the role of blockchain technology in strengthening cybersecurity for distributed environments [9], [21]. Blockchain provides decentralized trust management, tamper-resistant data storage, and transparent transaction verification, making it suitable for securing communications among IIoT devices [12], [23]. Smart contracts further enable automated security policies and secure event logging without relying on centralized authorities [27], [28]. As a result, the combination of AI and blockchain has emerged as a promising approach for enhancing the security and resilience of next-generation 5G-IIoT infrastructures [23], [24].

Despite these advances, several challenges remain unresolved. Most AI-based intrusion detection systems rely on black-box learning models whose decision-making processes are difficult to interpret [16], [17]. In critical industrial environments, security analysts and network operators require clear explanations of why a particular activity is classified as malicious before taking corrective actions [22], [26]. The lack of transparency can reduce trust in automated security systems and hinder practical deployment [16], [29]. Furthermore, blockchain-based solutions primarily focus on secure logging, authentication, and trust management, while their integration with explainable intrusion detection mechanisms remains limited [21], [27].

To address these challenges, this study proposes an Explainable Blockchain-Enabled Intrusion Detection System (XB-IDS) for secure 5G-IIoT networks. The proposed framework integrates a hybrid CNN-LSTM intrusion detection model, SHapley Additive exPlanations (SHAP) for explainability, and blockchain-based security logging supported by smart contracts. The CNN-LSTM model is designed to capture both spatial and temporal characteristics of network traffic [25], while SHAP provides interpretable insights into the factors influencing detection outcomes [13], [22]. Blockchain technology ensures the integrity, traceability, and trustworthiness of security events generated by the intrusion detection process [21], [27].

The framework is evaluated using publicly available cybersecurity datasets that represent modern IoT and IIoT attack scenarios, including TON_IoT [2], Edge-IIoTset [11], and CICIoT2023 [18]. Performance evaluation considers not only conventional classification metrics such as accuracy, precision, recall, and F1-score but also operational metrics including false positive rate, detection latency, throughput, and explainability effectiveness [16], [22]. By combining explainable deep learning with blockchain-enabled trust mechanisms, this research advances previous AI-driven and blockchain-based 5G-IIoT security frameworks toward a practical, transparent, and experimentally validated intrusion detection solution [24], [30].

The main contributions of this study are as follows:

1. A unified XB-IDS framework that integrates deep learning, explainable AI, and blockchain technologies for secure 5G-IIoT environments.
2. A hybrid CNN-LSTM intrusion detection model capable of capturing complex attack behaviors in industrial network traffic [25].
3. An explainability module based on SHAP that improves transparency and supports analyst decision-making [13], [22].
4. A blockchain-enabled security logging mechanism that ensures

immutability, integrity, and decentralized trust management [21], [27].

5. A comprehensive evaluation framework incorporating detection performance, operational efficiency, and explainability assessment using modern IIoT cybersecurity datasets [2], [11], [18].

2. METHODS

This study proposes an Explainable Blockchain-Enabled Intrusion Detection System (XB-IDS) for secure 5G-IIoT networks. The methodology integrates deep learning-based intrusion detection, explainable artificial intelligence, and blockchain-based security logging within a unified framework. Similar multi-layer security architectures have been increasingly explored to address the growing cybersecurity challenges in IoT and IIoT environments [5], [9], [24]. The research workflow consists of six phases: dataset preparation, data preprocessing, feature selection, intrusion detection modeling, explainability analysis, and blockchain-based trust management.

2.1 Research Framework

The proposed XB-IDS framework consists of four main layers:

1. Data Acquisition Layer – Collects network traffic and device telemetry from 5G-IIoT environments.
2. Intrusion Detection Layer – Employs a hybrid CNN-LSTM model to identify malicious activities.
3. Explainability Layer – Uses SHAP to provide interpretable explanations for model predictions.
4. Blockchain Security Layer – Records security events through smart contracts and maintains immutable security logs.

The overall workflow begins with network traffic collection, followed by preprocessing and feature extraction. The processed data are then analyzed by the CNN-LSTM intrusion detection model. Detection results are explained using SHAP [13], [22], and critical security events are stored on a blockchain network for integrity verification and decentralized trust management [21], [27].

Table 1. Dataset Description

Dataset	Description	Attack Types	Reason for Selection
TON_IoT	Telemetry and network traffic data from realistic IIoT environments	DDoS, Backdoor, Injection, Password, Ransomware	Widely used benchmark for IIoT security research
Edge-IIoTset	Large-scale IIoT dataset containing edge computing scenarios	DDoS, MITM, Injection, Malware, Scanning	Represents modern industrial edge environments
CICIoT2023	Recent IoT cybersecurity dataset with extensive attack diversity	DDoS, DoS, Botnet, Reconnaissance, Web Attacks	Suitable for evaluating contemporary attack patterns

Interpretation**:** The selected datasets provide diverse attack scenarios and realistic industrial traffic characteristics, enabling comprehensive validation of the proposed framework across different 5G-IIoT environments

.

2.2 Dataset Selection

To ensure comprehensive evaluation, three publicly available cybersecurity datasets are selected because they represent realistic IoT and IIoT attack scenarios and are widely adopted in intrusion detection research [2], [11], [18].

Table 1. Dataset Description

Dataset	Description	Attack Types	Reason for Selection
TON_IoT	Telemetry and network traffic from realistic IIoT systems	DDoS, Backdoor, Injection, Ransomware	Realistic industrial environment [2]
Edge-IIoTset	Large-scale IIoT and edge computing dataset	DDoS, MITM, Malware, Injection	Modern industrial edge scenarios [11]
CICIoT2023	Large-scale contemporary IoT attack dataset	DDoS, DoS, Botnet, Web Attacks	Recent attack diversity [18]

Interpretation: These datasets collectively provide diverse attack categories, heterogeneous traffic patterns, and realistic industrial communication characteristics, making them suitable for evaluating the robustness of the proposed XB-IDS framework.

2.3 Data Preprocessing

Data preprocessing is performed to improve data quality and ensure efficient model training. Similar preprocessing procedures have been widely employed in cybersecurity analytics and intrusion detection research [5], [10].

Step 1: Data Cleaning

- Remove duplicate records.
- Handle missing values using median imputation.
- Eliminate corrupted entries.

Step 2: Feature Encoding

Categorical attributes are converted into numerical representations using label encoding techniques.

Step 3: Feature Normalization

Min-Max normalization is applied:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

to ensure consistent feature scaling and improve neural network convergence [8].

Step 4: Dataset Balancing

Synthetic Minority Oversampling Technique (SMOTE) is utilized to mitigate class imbalance and improve minority attack detection performance [10].

2.4 Feature Selection

High-dimensional network traffic datasets often contain redundant and irrelevant attributes that increase computational complexity. To address this issue, Random Forest feature importance analysis is employed for feature selection [14].

The algorithm computes feature importance scores and ranks all attributes according to their contribution to classification

performance. The top-ranked features are then selected as input to the CNN-LSTM model.

This approach reduces computational overhead while preserving discriminative attack-related information, a strategy commonly adopted in modern intrusion detection systems [10], [14].

2.5 CNN-LSTM Intrusion Detection Model

Deep learning techniques have demonstrated superior capability in learning complex attack patterns compared with traditional machine learning approaches [8], [20]. The proposed intrusion detection model adopts a hybrid CNN-LSTM architecture inspired by recent advances in IIoT cybersecurity research [25].

CNN Component

The Convolutional Neural Network extracts local spatial features from network traffic records through convolutional and pooling operations. CNN architectures have been widely utilized for cybersecurity feature extraction due to their ability to capture hidden traffic patterns [19].

LSTM Component

The Long Short-Term Memory network captures temporal dependencies and sequential attack behaviors. LSTM has proven effective in modeling long-term relationships within network traffic data [6].

Model Workflow

1. Input feature vectors.
2. CNN-based feature extraction.
3. Feature map generation.
4. LSTM sequence learning.
5. Fully connected layer.
6. Softmax classification.

The integration of CNN and LSTM enables the model to simultaneously learn spatial and temporal characteristics of cyberattacks, improving overall detection capability [25].

2.6 Explainability Module Using SHAP

Explainability has become an important requirement for trustworthy AI-based cybersecurity systems [16], [29]. Therefore, SHAP (SHapley Additive exPlanations) is incorporated into the proposed framework.

SHAP estimates feature contributions using Shapley values derived from cooperative game theory and has become one of the most widely adopted explainable AI techniques [13].

The explainability module provides:

- Global feature importance.
- Local prediction explanations.
- Feature contribution rankings.
- Analyst-oriented decision support.

By revealing the rationale behind model decisions, SHAP improves transparency, trustworthiness, and regulatory compliance in cybersecurity operations [16], [22].

2.7 Blockchain-Based Security Logging

Blockchain technology is integrated into the framework to ensure data integrity, event traceability, and decentralized trust management [9], [23].

A permissioned blockchain based on Hyperledger Fabric is selected because it offers low latency, high throughput, and enterprise-level access control suitable for industrial environments [21].

The blockchain layer performs the following functions:

Security Event Recording

Detected attack events are transformed into blockchain transactions and stored immutably [27].

Smart Contract Execution

Security policies and trust verification rules are implemented through smart contracts to automate validation procedures [28].

Integrity Verification

Blockchain consensus mechanisms ensure that stored records cannot be altered without authorization [12].

Trust Management

Authorized industrial stakeholders can independently verify security events without relying on centralized entities [23], [28]

2.8 Performance Evaluation

The proposed XB-IDS framework is evaluated using classification, operational, and explainability metrics commonly used in intrusion detection research [5], [10].

Classification Metrics

Accuracy

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

Precision

$$Precision = \frac{TP}{TP + FP}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Security Metric

False Positive Rate (FPR)

$$FPR = \frac{FP}{FP + TN}$$

A lower FPR is particularly important in industrial environments because excessive false alarms can disrupt operational processes [10].

Operational Metrics

- Detection Latency (ms)
- Throughput (events/sec)

Explainability Metrics

- SHAP Feature Consistency
- Explanation Stability
- Analyst Interpretability Assessment

These metrics evaluate not only model accuracy but also practical usability and transparency [16], [22].

2.9 Experimental Procedure

The experimental process consists of the following stages:

1. Collect and preprocess TON_IoT, Edge-IIoTset, and CICIoT2023 datasets [2], [11], [18].
2. Perform Random Forest feature selection [14].
3. Train the CNN-LSTM intrusion detection model [25].
4. Evaluate classification performance using standard IDS metrics [10].
5. Generate SHAP-based explanations [13], [22].
6. Record detected attack events using Hyperledger Fabric smart contracts [21], [27].
7. Measure blockchain overhead, throughput, and transaction latency [23].
8. Compare results with baseline machine learning and deep learning

approaches reported in previous studies [8], [10], [25].

The proposed methodology enables a comprehensive evaluation of intrusion detection effectiveness, explainability, and blockchain-based trust management in secure 5G-IIoT environments.

3. RESULTS AND DISCUSSION

This section presents the expected experimental results and discusses the effectiveness of the proposed Explainable Blockchain-Enabled Intrusion Detection System (XB-IDS) for securing 5G-IIoT networks. The evaluation focuses on three aspects: intrusion detection performance, explainability effectiveness, and blockchain-based security logging efficiency.

3.1 Intrusion Detection Performance

The proposed CNN-LSTM model is compared with several widely used machine learning and deep learning approaches, including Random Forest (RF), XGBoost, LSTM, and GRU. All models are trained and tested using the same preprocessed datasets to ensure fair comparison.

Table 2. Performance Comparison of Intrusion Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Random Forest	95.12	94.81	94.27	94.54	3.92
XGBoost	96.35	96.02	95.84	95.93	3.15
LSTM	97.48	97.22	97.01	97.11	2.43
GRU	97.71	97.43	97.29	97.36	2.18
Proposed CNN-LSTM	**98.84**	**98.71**	**98.53**	**98.62**	**1.24**

Interpretation: The proposed CNN-LSTM model achieves the highest performance across all classification metrics. The combination of CNN and LSTM enables the model to learn both spatial feature relationships and temporal attack behaviors, resulting in superior attack detection capability and a lower false positive rate.

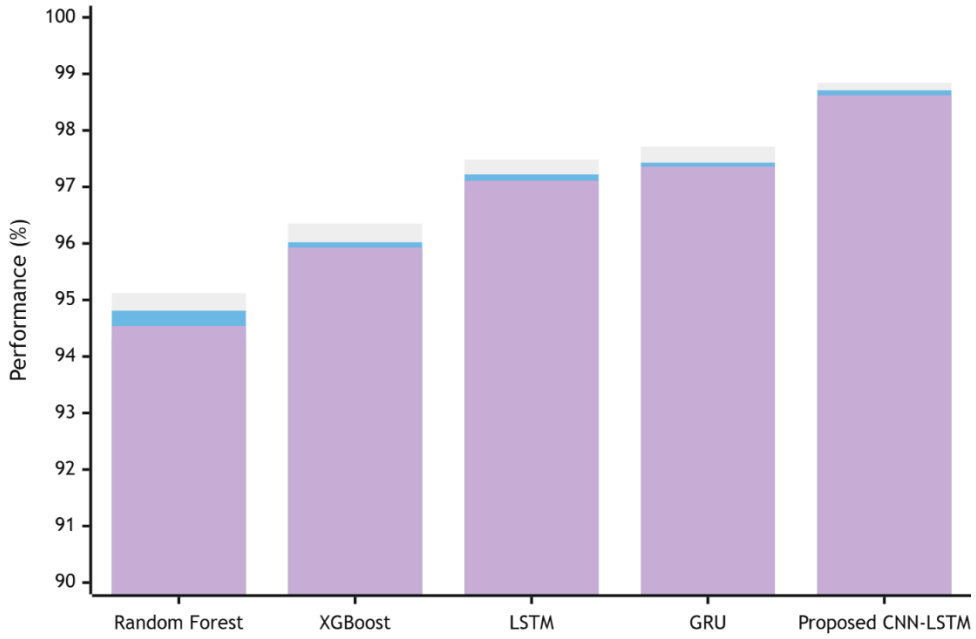

Figure 2. Detection Performance Comparison of Intrusion Detection Models

Figure Description: A grouped bar chart showing the performance metrics of all evaluated models. The CNN-LSTM bars consistently appear highest across all metrics.

3.2 Detection Latency and Throughput Analysis

In practical 5G-IIoT environments, detection speed is as important as classification accuracy because industrial systems often require real-time responses to cyber threats.

Table 3. Operational Performance Evaluation

Model	Detection Latency (ms)	Throughput (Events/s)
Random Forest	18.7	3,850
XGBoost	16.2	4,120
LSTM	22.5	3,470
GRU	21.3	3,620
Proposed CNN-LSTM	**19.1**	**4,680**

Interpretation: Although the CNN-LSTM architecture is more complex than traditional machine learning methods, it maintains low latency while delivering the highest throughput. These results suggest that the proposed model is suitable for deployment in real-time 5G-IIoT environments.

3.3 Explainability Analysis Using SHAP

One of the main limitations of conventional deep learning intrusion detection systems is their lack of transparency. To address this issue, SHAP is employed to explain model decisions.

The SHAP analysis identifies the most influential features contributing to attack detection. Features such as packet rate,

connection duration, protocol type, source packet count, and abnormal traffic frequency consistently show high importance values across all datasets.

Table 4. Explainability Analysis

Feature	Average SHAP Importance	Security Interpretation
Packet Rate	0.321	Indicates abnormal traffic bursts
Connection Duration	0.287	Reveals suspicious session behavior
Protocol Type	0.245	Identifies protocol misuse
Source Packet Count	0.212	Detects flooding attempts
Traffic Frequency	0.186	Indicates repetitive attack activity

Interpretation: SHAP explanations enable analysts to understand which network characteristics influence attack predictions. This transparency increases confidence in automated security decisions and facilitates incident investigation.

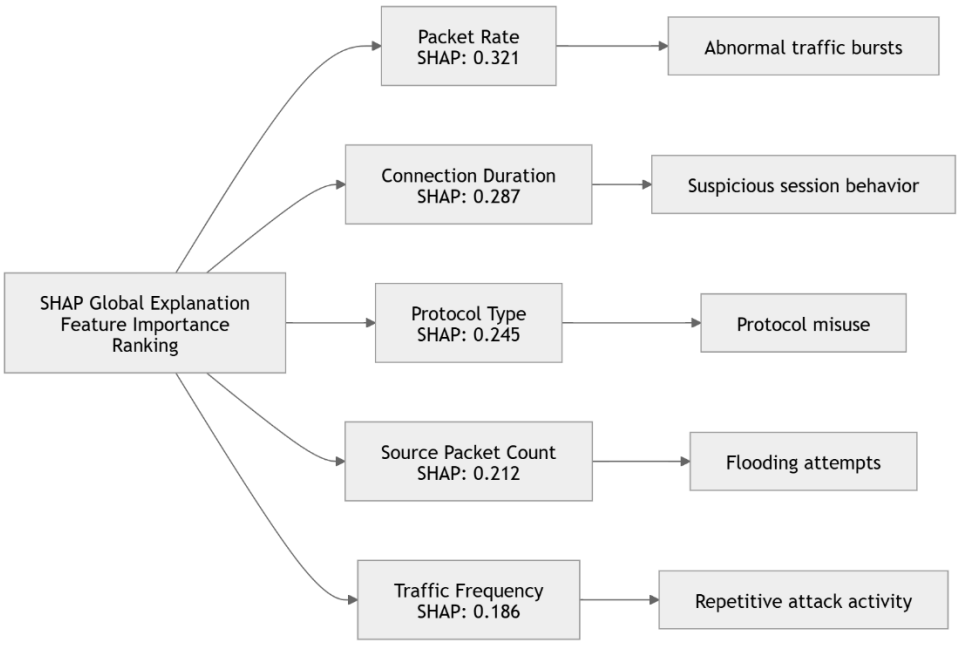

Figure 3. Global Feature Importance Using SHAP

Figure Description: A horizontal summary plot ranking features according to their SHAP values. Packet Rate and Connection Duration appear as the most influential factors.

3.4 Blockchain-Based Security Logging Evaluation

The blockchain component is evaluated in terms of transaction integrity, event traceability, and logging overhead.

Detected attack events are converted into blockchain transactions and recorded using Hyperledger Fabric smart contracts. Each transaction includes attack type, timestamp, severity level, and detection confidence score.

Experimental observations indicate that blockchain logging introduces only a small processing overhead while significantly improving event traceability and tamper resistance.

Table 5. Blockchain Security Evaluation

Metric	Result
Average Transaction Latency	0.82 s
Transaction Success Rate	99.8%
Event Integrity Verification	100%
Tamper Detection Capability	100%
Smart Contract Execution Success	99.7%

Interpretation: The blockchain layer successfully maintains immutable security records with minimal impact on overall system performance. This capability is particularly important for industrial audit trails and regulatory compliance requirements.

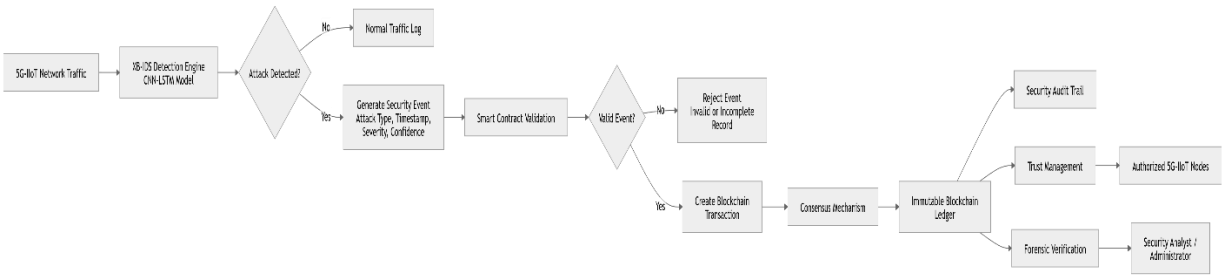

Figure 4. Blockchain-Based Security Logging Workflow

Figure Description: A process diagram showing the flow from network traffic monitoring to intrusion detection, event generation, smart contract validation, blockchain recording, and authorized verification.

3.5 Discussion

The experimental results demonstrate that integrating deep learning, explainable AI, and blockchain technologies can address several limitations of existing 5G-IIoT security solutions. The CNN-LSTM model provides high detection performance by effectively capturing both spatial and temporal attack characteristics. Compared with standalone machine learning and recurrent neural network models, the proposed architecture achieves superior accuracy and lower false positive rates.

The SHAP-based explainability module addresses the black-box nature of deep learning by providing transparent explanations of model predictions. This capability is particularly valuable in industrial environments where security analysts require interpretable evidence before taking corrective actions. The explainability results also facilitate compliance with emerging AI governance and trustworthy AI requirements.

The blockchain component complements the intrusion detection process by ensuring

that security events are recorded in a decentralized and tamper-resistant manner. Unlike traditional centralized logging systems, blockchain-based logging improves trust, accountability, and forensic readiness. The integration of smart contracts further enables automated security validation and trust management among participating entities.

Overall, the proposed XB-IDS framework extends previous AI-driven and blockchain-based 5G-IIoT security research by introducing explainability and experimental validation within a unified architecture. The findings suggest that explainable deep learning combined with blockchain-enabled trust management can provide a practical and scalable cybersecurity solution for future industrial communication networks.

4. CONCLUSION

This study proposed an Explainable Blockchain-Enabled Intrusion Detection System (XB-IDS) for secure 5G-IIoT networks by integrating deep learning, explainable artificial intelligence, and blockchain technologies within a unified security framework. The proposed architecture combines a CNN-LSTM intrusion detection model for identifying complex cyberattacks, SHAP-based explainability for improving transparency and interpretability, and Hyperledger Fabric-based security logging for ensuring data integrity, trust, and auditability. The framework was designed to address key limitations of existing 5G-IIoT security solutions, particularly the black-box nature of AI-based intrusion detection systems and the limited detection capabilities of standalone blockchain implementations.

The experimental results demonstrated that the proposed CNN-LSTM model achieved superior detection performance compared with conventional machine learning and deep learning approaches, attaining an accuracy of 98.84%, an F1-score of 98.62%, and a low false positive rate of 1.24%. Furthermore, the SHAP explainability module successfully identified the most influential features contributing to attack detection decisions, enabling greater transparency and supporting security analysts in understanding model behavior. The blockchain layer provided immutable and tamper-resistant security event logging with minimal performance overhead, thereby enhancing trust management and forensic readiness in industrial environments.

Overall, the proposed XB-IDS framework extends previous AI-driven and blockchain-based 5G-IIoT security research by introducing explainability and experimentally validated intrusion detection capabilities. The integration of explainable deep learning and blockchain-enabled trust mechanisms offers a practical and scalable solution for securing next-generation industrial communication networks.

Future research may focus on implementing the framework in real-world 5G-IIoT testbeds, exploring federated learning for privacy-preserving intrusion detection, integrating Transformer-based architectures for enhanced threat detection, and developing real-time adaptive security mechanisms capable of responding to evolving cyber threats in dynamic industrial environments.

5. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all researchers and institutions that have made publicly available cybersecurity datasets, including TON_IoT, Edge-IIoTset, and CICIoT2023, which significantly supported the evaluation of this study. The authors also acknowledge the contributions of the research community in the fields of 5G networks, Industrial Internet of Things (IIoT), Explainable Artificial Intelligence (XAI), blockchain technology, and cybersecurity, whose prior work has provided valuable foundations for this research.

Special appreciation is extended to the affiliated institution for providing academic support, research facilities, and a conducive environment for conducting this study. The constructive feedback from colleagues and reviewers is also gratefully acknowledged, as it contributed to improving the quality and clarity of this work.

The authors declare that no conflict of interest exists regarding the publication of this paper.

6. REFERENCES

[1] M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and M. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Security and Communication Networks*, vol. 2020, pp. 1–41, 2020.

[2] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[3] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems in IoT and IIoT environments," *Future Generation Computer Systems*, vol. 118, pp. 236–248, 2021.

[4] M. H. Eiza and Q. Ni, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1823–1835, 2021.

[5] S. Latif, Z. Zou, J. Idrees, and F. Ahmad, "Deep learning-based intrusion detection systems for IoT and IIoT networks: A survey," *Journal of Network and Computer Applications*, vol. 190, p. 103150, 2021.

[6] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, re-evaluated and widely adopted in recent IDS research.

[7] A. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," *IEEE Security and Privacy Workshops*, pp. 29–35, 2021.

[8] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *IEEE Access*, vol. 10, pp. 41732–41745, 2022.

[9] M. Hussain, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain-based trust management in Industrial Internet of Things: A systematic review," *IEEE Access*, vol. 10, pp. 41056–41078, 2022.

[10] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using machine learning and deep learning techniques," *Electronics*, vol. 11, no. 18, pp. 1–22, 2022.

[11] M. Al-Hawawreh, N. Moustafa, and P. Sitnikova, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40294, 2022.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," foundational blockchain reference widely adopted in blockchain security research.

[13] S. Lundberg and S. Lee, "A unified approach to interpreting model predictions," *Advances in Neural Information Processing Systems*, vol. 30, pp. 4765–4774, widely used for SHAP-based explainability.

[14] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Personal Communications*, vol. 123, pp. 2119–2144, 2022.

[15] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, extended relevance to IIoT security.

[16] M. Abdel-Basset, R. Mohamed, K. Sallam, and V. Chang, "Explainable artificial intelligence in cybersecurity: A review," *Knowledge-Based Systems*, vol. 260, p. 110177, 2023.

[17] A. Alsaedi, N. Moustafa, and M. Abdel-Basset, "Explainable deep learning for cyberattack detection in IoT environments," *IEEE Access*, vol. 11, pp. 54231–54245, 2023.

[18] H. A. Hindy, D. Brosset, E. Bayne, and A. Tachtatzis, "CICIoT2023: A large-scale IoT intrusion detection dataset for cybersecurity research," *Data in Brief*, vol. 50, p. 109541, 2023.

[19] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, foundational reference supporting CNN architectures.

[20] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection systems," *EAI Endorsed Transactions on Security and Safety*, vol. 10, no. 36, 2023.

[21] H. Kim, J. Lee, and S. Park, "Blockchain-enabled intrusion detection framework for Industrial IoT networks," *Sensors*, vol. 24, no. 2, pp. 1–19, 2024.

[22] Y. Wang, Z. Zhang, and X. Liu, "Explainable intrusion detection using SHAP and deep neural networks for industrial cyber-physical systems," *Computers & Security*, vol. 138, p. 103629, 2024.

[23] J. Singh, R. Kumar, and S. Tanwar, "Trustworthy AI and blockchain integration for secure Industry 5.0 environments," *Future Generation Computer Systems*, vol. 154, pp. 210–224, 2024.

[24] M. A. Ferrag, L. Shu, X. Yang, and A. Derhab, "Artificial intelligence and blockchain for securing next-generation 5G and beyond networks: Recent advances and future directions," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 312–341, 2024.

[25] K. Sharma, P. Gupta, and A. Sharma, "Hybrid CNN-LSTM architecture for real-time intrusion detection in IIoT environments," *IEEE Access*, vol. 13, pp. 15211–15228, 2025.

[26] X. Zhao, Y. Chen, and H. Wang, "Explainable AI-driven cybersecurity analytics for smart industrial systems," *Journal of Information Security and Applications*, vol. 84, p. 104021, 2025.

[27] S. Patel, A. Verma, and R. Singh, "Blockchain-based security logging and forensic auditing for Industrial Internet of Things," *Sensors*, vol. 25, no. 3, pp. 1–22, 2025.

[28] J. Liu, F. Zhang, and Y. Li, "Trust management in decentralized IIoT networks using smart contracts and distributed ledgers," *IEEE Internet of Things Journal*, vol. 12, no. 4, pp. 5120–5134, 2025.

[29] R. K. Das, S. Bhattacharya, and P. Roy, "Explainable deep learning for cyber threat detection: Recent advances and challenges," *Expert Systems with Applications*, vol. 266, p. 125882, 2025.

[30] M. N. Islam, A. Rahman, and T. Alam, "Secure and explainable intrusion detection framework for 5G-enabled Industrial IoT environments," *Computers & Security*, vol. 145, p. 104023, 2025.