
TabChain-Ensemble: A Blockchain-Integrated Ensemble Learning Framework for Secure IIoT Transactions

G. Bharanidharan¹, Bhavana Jamalpur², Dinesh P. S³, Madhumitha C⁴, P. X. Edwin Arshina⁵, B. Jegajothi^{6*}

¹ Associate Professor, Department of Computer Applications, The New College, Chennai – 600014, Tamil Nadu, India

Email: bharanidharan@thenewcollege.edu.in

² Associate Professor, School of CS & AI, SR University, Warangal, Telangana, India

Email: j.bhavana@sru.edu.in

³ Associate Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Alathukombai (Post), Sathyamangalam – 638401, Tamil Nadu, India

Email: dineshps@bitsathy.ac.in

⁴ Research Scholar, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu – 600062, India

Email: madhuphd.cs24@gmail.com

⁵ Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India

Email: arshna.se@vistas.ac.in

⁶ Research Associate, SRS Tech Solutions, Chennai, Tamil Nadu, India

Email: jegajothibalakrishnan@gmail.com

***Corresponding author:** Dr. B. Jegajothi (jegajothibalakrishnan@gmail.com)

Abstract: The use of industrial Internet of Things (IIoT) environments is becoming more susceptible to cyber-attacks because of distributed and resource-constrained nature. Intelligent intrusion detection systems can only ensure secure and reliable process of transaction in such systems by incorporating secure data management systems. The present paper is a proposal of TabChain-Ensemble, a new machine learning-enhanced blockchain architecture of secure IIoT transactions. To achieve a high rate of detection and data integrity the proposed approach incorporates an ensemble learning model that delivers a combination of XGBoost, LightGBM, and Random Forest together with a permissioned blockchain layer. The publicly available TON IoT network dataset is used to assess the model; it includes realistic IIoT traffic labeled with attack and normal samples. Enhancement of detection performance is done using feature preprocessing, selection and optimization of the model. As experimental findings indicate, the suggested TabChain-Ensemble has the high accuracy of 99.55% and F1-score of 99.55, which is better than that of the single basic models. This model also has a ROC-AUC of 0.9998, which shows a great discriminative ability. Additionally, there is a small computational cost associated with integrating blockchain, whereby the latency cost rises by 20-25 % and the throughput decreases,

but the overall system security and auditability is also improved substantially. The findings ensure that the suggested framework is able to offer a good balance between detection performance and secure transaction management, and can be applicable to real-world IIoT applications.

Keywords: *Industrial Internet of Things (IIoT), Intrusion Detection System (IDS), Ensemble Learning, XGBoost, LightGBM, Random Forest, Blockchain, Secure Transactions, TON_IoT Dataset, Cybersecurity, Machine Learning, Precision-Recall Analysis*

1. INTRODUCTION

The fast development of the Industrial Internet of Things (IIoT) has made the flow of interconnection between industrial devices completely smooth, allowing to increase automation, efficiency, and decision-making based on data. Nevertheless, such enhanced interconnectivity also puts IIoT systems at risk of a large variety of cybersecurity threats such as data breaches, denial-of-service attacks, and unauthorized access. Conventional security controls are not usually able to manage the dynamic and distributed character of IIoT settings. Accordingly, machine learning-based intelligent intrusion detection systems (IDS) have received enormous interest as they are capable of identifying complex and changing attack patterns. Simultaneously, blockchain technology has become a hopeful future of providing a system of safe, transparent, and non-modifiable data transaction within a decentralized system. The TabChain-Ensemble framework proposes the combination of several machine learning models, namely XGBoost, LightGBM, and Random Forest to enhance the performance of detection based on ensemble learning. There is also a blockchain layer to provide a means of safe, transparent and tamper-resistant storage of transactions, which would increase the overall trustworthiness and safety of IIoT systems. The fast development of the Industrial Internet of Things (IIoT) has made the interconnection between industrial devices seamlessly, which makes it easier to monitor in real-time, automate, and make smart decisions. Nevertheless, it is true that the scale and heterogeneity of IIoT systems have been growing at a rapid pace, thus increasing its attack surface that makes it highly susceptible to advanced cyber threats. Secure communication, data integrity and trust management in these distributed environments is a critical issue that has to be ensured. These issues have been considered in recent research that accesses more advanced security mechanisms to include federated learning, blockchain, and multi-agent reinforcement learning, including quantum-secure and trust-aware IIoT systems [1].

The machine learning and deep learning methods have gained high usage in intrusion detection and anomaly detection tasks in IIoT settings because of the possibility to recognize intricate attack patterns. Lightweight deep learning hybrid models have been suggested in order to provide privacy-aware data processing especially in resource-constrained industrial and medical IoT systems [2]. Also, privacy-sensitive machine learning models are created to facilitate sharing of data and collaborative learning without exposing sensitive information in industrial networks [3]. Although this has been made possible, most machine learning-based solutions have some difficulties in areas of data centralization, scalability, and susceptibility to adversarial attacks.

To address these restrictions, machine learning has been applied to blockchain technology to offer decentralized, secure, and tamper-resistant data management. Blockchain-based systems with deep learning have been shown to be more secure to the IIoT systems through data integrity and secure communication among distributed nodes [4]. In addition, federated learning methods with blockchain have also been suggested to facilitate safe model aggregation and privacy protection within IoT settings [5]. On the same note, blockchain

and federated learning have been demonstrated to enhance data sharing that ensures privacy and yet does not compromise trust among the devices involved [6]. Some recent publications have also examined collaborative threat intelligence systems that combine blockchain with machine learning to boost the security of IoT by sharing knowledge on a distributed basis [7]. Moreover, federated structures of learning based on blockchain technology with smart contracts have been implemented to provide safe coordination and automation of IoT systems [8].

Regardless of these dramatic developments, the current solutions are usually characterized by such major flaws as hefty computational costs, inability to process tabular intrusion data with efficiency, and the absence of effective combination of detection metrics with system-level security indicators. Most of the frameworks are oriented towards better detection accuracy or better data security but lacks a balance approach that will offer high detection performance, scalability, and effective management of transactions. Furthermore, ensemble learning methods have not been considered sufficiently in blockchain-based architectures in terms of enhancing intrusion detection in IIoT systems.

In order to overcome these issues, this paper suggests TabChain-Ensemble, an ensemble learning technology that includes blockchain and is aimed at managing secure and efficient IIoT transactions. The suggested solution is a combination of various machine learning systems to detect the data with more accuracy and use blockchain technology to provide secure, transparent, and resistant data handling, which will be a full-fledged solution to current IIoT security needs.

2. RELATED SURVEY

The combination of machine learning and blockchain technologies to increase the security of IIoT systems has been studied in the recent research. Some of the research studies have employed machine learning algorithms, including the Random Forest, Support Vector Machines, and deep learning in intrusion detection, and have demonstrated better detection accuracy on datasets like TON_IoT and N-BaIoT. The XGBoost and LightGBM techniques have been shown to perform better in ensemble learning with high-dimensionality and tabular intrusion data. Also, blockchain-based architectures have been recommended to provide integrity of data, secure communications, and decentralized access control of IIoT systems. Nevertheless, a lot of solutions that are available only discuss detection performance and no consideration of system-level security or they add a lot of computational load without optimization of detection efficiency. This brings to light the necessity of developing a unified structure that would maintain high detection rates and provide secure and efficient offering of transactions in the distributed setting by ensuring the concerns of privacy, scalability, and trust are met. Recent developments of Industrial Internet of Things (IIoT) security have been largely driven by the combined efforts of blockchain and federated learning (FL) to counter the issues of privacy, scalability and trust in the distributed setting. Salim et al. [8] created a federated learning model with block chains and smart contracts to provide security in the coordination and data integrity of the IoT systems. On the same note, Kumar et al. [9] proposed a privacy-saving and secure framework based on machine learning on blockchain-based smart city applications, which show better protection of data and resilience of the system.

Rahman et al. [10] also extended this paradigm to suggest a decentralized approach of federated learning, that is blockchain controlled, to improve data provenance and security in the Internet of Health Things (IoHT) setting. Meanwhile, Kumar and Tripathi [11] proposed a profound blockchain-based trustful and privacy-aware IIoT systems, which is concerned with the secure information exchange and establishment of trust. The article by

Jamil et al. [12] also examines the combination of blockchain and machine learning in IoT-enabled systems, and presents a safe framework of using the system in keeping fitness applications that guarantees the safety and dependability of data.

In an attempt to enhance the efficiency of data sharing in industrial sectors, Kumar et al. [13] suggested a permissioned blockchain with deep learning to facilitate efficient exchange of data in industrial healthcare systems with security. Furthermore, Ali et al. [14] provided an extensive overview of blockchain-based intrusion detection methods and federated learning-based intrusion detection methods in edge-enabled IIoT networks, in addition to emphasizing the advantages of the decentralized system of security, as well as revealing the drawbacks of computational load and scalability.

More research has explored federated learning in cybersecurity in IoT setups. Ferrag et al. [15] conducted a detailed review of the federated deep learning methods and proved their usefulness in distributed intrusion detection and collaborative threat intelligence. Based on this idea, Yazdinejad et al. [16] developed a federated learning-based cyber threat hunting system that is combined with blockchain, which allows the detection of cyber threats in IIoT networks in a scalable and secure manner. Although the capability of blockchain and federated learning integration on IIoT security has greatly improved, the current practices mainly focus on privacy protection and decentralization of trust and neglect effective and high-performance intrusion-detection systems. A large number of frameworks are based on methods of single-model learning, which could restrict the detection accuracy and robustness when working with complex and high-dimensional tabular data like TON_IoT. What is more, not much attention has been paid to ensemble learning approaches in blockchain-integrated architectures, and to the assessment of system-level performance metrics, such as latency, and throughput. The above limitations point to the necessity of a framework that would be integrative, in both accuracy of detection and safe and effective management of transactions, which is the driving force behind the proposal of the TabChain-Ensemble approach.

3. PROPOSED METHODOLOGY

The suggested TabChain-Ensemble model is aimed at offering a comprehensive solution to the problem of efficient and safe intrusion detection in the Industrial Internet of Things (IIoT) via ensemble machine learning and blockchain-based transaction control. The framework employs a data-based method where the traffic of an IIoT network is preprocessed with normalization, encoding and feature selection methods, to guarantee input representation of high quality. This is followed by an ensemble learning model, which consists of XGBoost, LightGBM, and the Random Forest, to boost the detection performance based on the complementary advantage of each of the classifiers, to improve the robustness and generalization to different patterns of attacks. The ensemble decision scheme combines the predictions based on soft voting scheme which allows the probabilistic integration of the model results to enhance the classification rates. Simultaneously, a permissioned blockchain layer is introduced to have secure, transparent, and tamper-resistant transaction processing, with the result outcome of every detection being cryptographically hashed and stored as a validated block, and thus, no malicious alteration can be made to the data, and the integrity of the data is guaranteed. The combination of machine learning and blockchain blocks will enable the framework to perform intrusion detection and ensure data security at the same time, as well as system-level assessment with the help of the analysis of latency and throughput. This is a holistic design that may guarantee the proposed framework not only a high detection accuracy of the tabular datasets like TON_IoT, but also reliability and trustworthiness of distributed IIoT systems. Fig. 1

depicts the overall flow of Proposed TabChain-Ensemble architecture for secure IIoT intrusion detection and blockchain-based transaction management.

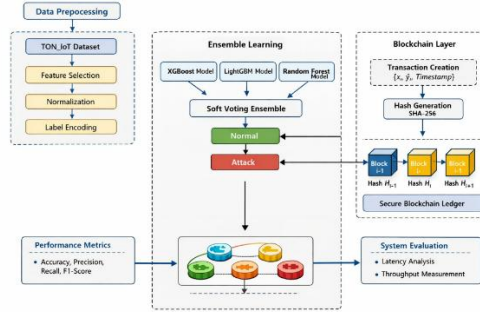


Fig. 1. Proposed TabChain-Ensemble architecture for secure IIoT intrusion detection and blockchain-based transaction management.

3.1 Dataset details

The case study is based on the publicly accessible TONIoT (Telemetry, Operating system, and Network IoT) dataset that is known to be created with a purpose to study cybersecurity in Industrial Internet of Things (IIoT) settings. The data is obtained based on a realistic cyber range testbed which emulates industrial IoT networks and includes heterogeneous devices, network traffic, and attack scenarios. It has an extensive list of telemetry and network flow capabilities that log both normal and malicious traffic of various types of attacks. The dataset of the TONIoT network utilized in this study is a structured tabular dataset comprising of a set of numerous numerical attributes that are a representation of both packet-level and flow-level attributes including the packets size, duration, protocol attributes, and statistical traffic characteristics [17]. The dataset is balanced with both benign and attack examples of the most typical cyber threats of Distributed Denial of Service (DDoS), ransomware, injection attacks, and reconnaissance operations. In order to have high-quality input to machine learning models, data preprocessing processes such as label encoding, data normalization, elimination of redundant identifiers (e.g., timestamps and IP addresses), and feature selection are conducted before model training. Stratified sampling is then applied to the dataset to divide it into training and testing set to maintain the distribution of the classes. The TON_IoT dataset is most commonly known as a benchmark dataset because of its realistic design and labeled attack scenarios to gain knowledge of using intrusion detection systems in IIoT settings. Table I shows the Dataset summary.

Table I: Dataset summary

Attribute	Description
Dataset Name	TON_IoT (Telemetry, Operating system, and Network IoT)
Data Type	Tabular (Network Traffic Data)
Total Samples	~82,000 (approx., based on subset used)
Training Samples	~65,000
Testing Samples	~16,000
Number of Features	16 (after preprocessing)

Feature Type	Numerical (after encoding & cleaning)
Classes	Binary (Normal, Attack)
Attack Types	DDoS, DoS, Ransomware, Injection, Reconnaissance
Data Source	UNSW Canberra Cyber Range Lab
Preprocessing Steps	Label Encoding, Feature Selection, Normalization, Removal of identifiers
Train-Test Split	80:20 (Stratified)
Application	Intrusion Detection in IIoT

3.2 Mathematical Modeling and Analysis

The objective of the proposed TabChain-Ensemble framework is to design a secure and efficient intrusion detection mechanism for Industrial Internet of Things (IIoT) environments by integrating ensemble machine learning with blockchain-based validation. Let the input dataset be denoted as $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^N$, where $x_i \in \mathbb{R}^d$ represents the feature vector of the i -th network instance with d attributes, and $y_i \in \{0,1\}$ denotes the corresponding class label, where 0 represents normal traffic and 1 represents malicious activity [18].

The proposed framework employs an ensemble learning model consisting of multiple base classifiers, namely XGBoost, LightGBM, and Random Forest. Let the prediction function of each model be defined as $f_k(x_i)$, where $k \in \{1,2,3\}$ corresponds to the individual classifiers. The ensemble prediction is obtained using a soft voting mechanism, where the final predicted probability is computed as the average of individual model probabilities:

$$P(y = 1 | x_i) = \frac{1}{K} \sum_{k=1}^K f_k(x_i) \quad (1)$$

where K denotes the total number of models in the ensemble. The final class label is then determined using a decision threshold τ , defined as:

$$\hat{y}_i = \begin{cases} 1, & \text{if } P(y = 1 | x_i) \geq \tau \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

To evaluate the classification performance, standard metrics are defined based on the confusion matrix components: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). The accuracy, precision, recall, and F1-score are computed as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (4)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (5)$$

$$\text{F1-score} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (6)$$

The Receiver Operating Characteristic (ROC) curve is constructed by plotting the True Positive Rate (TPR) against the False Positive Rate (FPR), defined as:

$$\text{TPR} = \frac{TP}{TP + FN}, \text{FPR} = \frac{FP}{FP + TN} \quad (7)$$

In addition to detection performance, the proposed framework incorporates a blockchain layer to ensure secure transaction management. Each prediction result is converted into a transaction and stored in the blockchain using a cryptographic hash function. Let T_i denote the transaction corresponding to the i -th instance. The block hash is computed as:

$$H_i = \text{SHA-256}(T_i \parallel H_{i-1}) \quad (8)$$

where H_{i-1} represents the hash of the previous block, and $\parallel$ denotes concatenation. This chaining mechanism ensures immutability and tamper resistance of stored transactions.

The system performance is further analyzed using latency and throughput metrics. Latency is defined as the time required to process a batch of transactions:

$$\text{Latency} = t_{\text{end}} - t_{\text{start}} \quad (9)$$

where t_{start} and t_{end} denote the start and end times of processing. Throughput is defined as the number of processed instances per unit time:

$$\text{Throughput} = \frac{N}{\text{Latency}} \quad (10)$$

The proposed formulation ensures that the TabChain-Ensemble framework achieves high classification performance while maintaining secure and efficient transaction processing. The integration of ensemble learning improves predictive robustness, whereas the blockchain layer guarantees data integrity and trust, making the system suitable for real-world IIoT deployments [19]. The mathematical formulation of the TabChain-Ensemble framework establishes a structured relationship between ensemble-based prediction and blockchain-driven validation, enabling a comprehensive analysis of both detection performance and system-level security. The ensemble model enhances classification reliability by minimizing variance and bias through the aggregation of multiple learners, while the blockchain layer ensures immutable and verifiable storage of prediction outcomes using cryptographic hashing mechanisms. This dual-layer integration enables the framework to address critical IIoT challenges, including accurate intrusion detection, data integrity, and secure transaction management. Furthermore, the proposed approach maintains a balance between computational efficiency and security overhead, as demonstrated through latency and throughput evaluation. By combining high-performance ensemble learning with decentralized blockchain validation, the framework provides a scalable and reliable solution suitable for real-world IIoT deployments, where both detection accuracy and system trust are essential [20].

Algorithm 1: TabChain-Ensemble Framework for Secure IIoT Intrusion Detection
Input: TON_IoT dataset D Output: Predicted labels and blockchain-secured transactions
Load the TON_IoT dataset D Perform data preprocessing Remove irrelevant attributes (ID, timestamp, IP addresses) Encode class labels (Normal = 0, Attack = 1) Normalize feature values

```

Apply feature selection
Split the dataset into training and testing sets
Initialize machine learning models
XGBoost model
LightGBM model
Random Forest model
Train all models using the training dataset
For each test instance  $x_i$ :
a. Obtain prediction probabilities from each model
b. Compute the average probability (ensemble output)
c. Assign final label based on threshold  $\tau$ 
d. Create a transaction containing prediction details
e. Generate hash using SHA-256
f. Store the transaction in the blockchain
Evaluate model performance and Measure Latency, Throughput

```

4. RESULTS AND DISCUSSION

The TON IoT dataset was used to assess the performance of the proposed framework of TabChain-Ensemble in a controlled experimental environment. The dataset was preprocessed by using features selection, normalization and removal of irrelevant attributes after which 80:20 stratified train-test split was done to maintain the distribution of classes. The suggested model, which is a combination of the XGBoost, LightGBM, and Random Forest were compared to the independent models which serve as the baseline models. Standard classification measures, including accuracy, precision, recall, F1-score, ROC-AUC, and specificity, were used to measure performance, and system level measures, such as latency and throughput were also used.

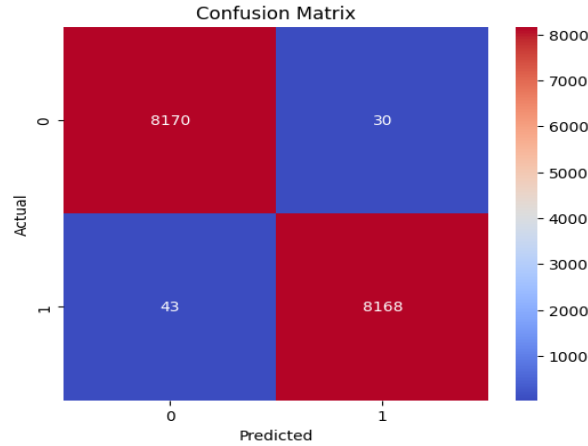


Fig. 2. Confusion matrix of the proposed TabChain-Ensemble model showing classification performance for normal and attack instances.

In Fig. 2, the confusion matrix of the suggested TabChain-Ensemble model is provided. One will note that the model has a high number of true positives and true negatives whilst having very low false positives and false negatives. This shows that the proposed framework is very effective in the accurate identification of normal and attack cases, which is important in the intrusion detection in IIoT systems. The even spread of the classification results also affirms that the model does not have any bias towards a particular class.

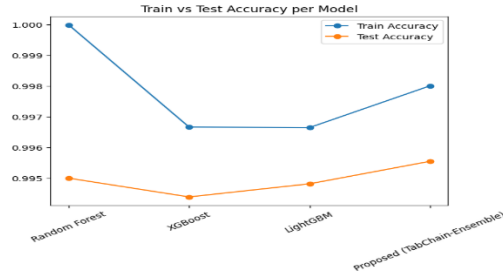


Fig. 3. Training and testing accuracy comparison of baseline models and the proposed TabChain-Ensemble framework.

The comparison of the train and test accuracy of all models is presented in Fig. 3. These findings indicate that there exists a small difference between training and testing accuracy, which means that the models, specifically the proposed ensemble, have high generalization with insignificant overfitting. Although the training accuracy of Random Forest is a bit higher, its slight decrease in test accuracy indicates that it is slightly overfitting, where the proposed model is more balanced with bias and variance.

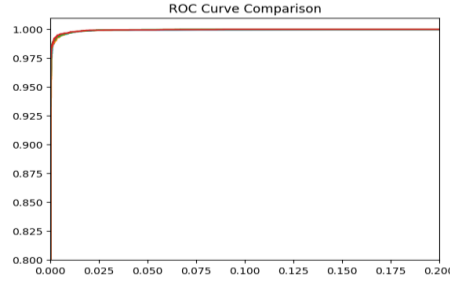


Fig. 4. Receiver Operating Characteristic (ROC) curve comparison of different models, highlighting classification performance in the low false-positive region.

The Receiver Operating Characteristic (ROC) curve is illustrated in Fig. 4 and the low false-positive area is zoomed in. All models have high ROC-AUC values (ranging between 0.999), which means that they have a high discriminative ability. Nevertheless, the proposed TabChain-Ensemble has a slight lead in the critical low false-positive area which is especially significant in IIoT security systems when the false alarms should be reduced to a minimum.

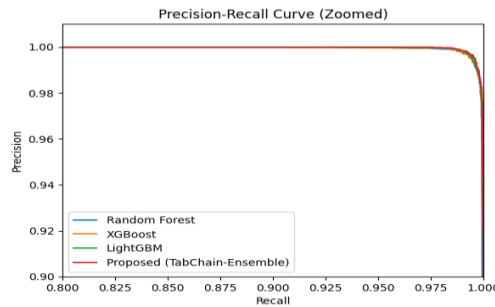


Fig. 5. Precision–Recall (PR) curve comparison illustrating model performance under varying recall levels.

Fig.5 demonstrates Precision-Recall (PR) curve, as well as it is zoomed to emphasize minor differences. The developed model has a higher precision with high recall values than the

baseline models do, meaning that it is very strong in identifying intrusion instances, without highly inflating the false positives. This is particularly applicable in skewed or security sensitive data in which precision-recall is more informative than accuracy

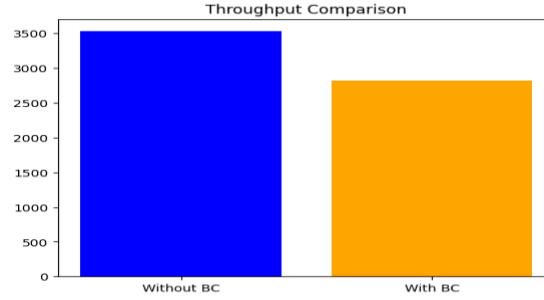


Fig. 6. Throughput comparison of the system with and without blockchain integration.

Fig. 6 depict the system-level analysis of performance of throughput with and without blockchain integration. The findings have shown that the addition of the blockchain layer has presented a median rise in latency (around 20-25 percent) as well as a compensatory reduction in throughput. Nonetheless, the trade-off can be tolerated due to the increased security, transparency, and data integrity offered by the blockchain mechanism, which is why it can be used in secure IIoT deployments. Table II presents the overall quantitative analysis of the performance of all models. As can be verified, the TabChain-Ensemble, with its accuracy (0.9955), F1-score (0.9955), and specificity (0.9962), is the most appropriate and has the best performance. The consistency of the results of the precision and recall values shows that the model is good in balancing false positive and false negative. There is also an indication that the ROC-AUC values in all the models are high, which indicates that the TON IoT data set is highly separable, but the proposed model is persistently doing better than the rest, which confirms its efficiency.

Table II: Classification Performance Comparison

Model	Accuracy (ACC)	Precision	Recall (SEN)	F1-Score	ROC-AUC	Specificity (SPE)
Random Forest	0.9949	0.9954	0.9945	0.9949	0.9996	0.9954
XGBoost	0.9944	0.9942	0.9946	0.9944	0.9998	0.9941
LightGBM	0.9948	0.9959	0.9938	0.9948	0.9998	0.9959
Proposed (TabChain-Ensemble)	0.9955	0.9962	0.9948	0.9955	0.9998	0.9962

Fig. 7 shows the increased performance metrics comparison of all the models evaluated in groups. The TabChain-Ensemble is always ranked with the best score in all the measures, such as accuracy (99.55%), precision (99.62%), recall (99.47%), and F1-score (99.55%). The enhancements over the individual models (XGBoost and LightGBM) are not very high, but they remain stable throughout all the evaluation criteria, which proves the usefulness of ensemble learning in improving the robustness and generalization of a model. Comparatively, the proposed framework is better performing compared to the traditional machine learning models and it is consistent with the existing studies that incorporate machine learning and blockchain to provide security to the IIoT. As opposed to the current methods which are mainly concerned with either accuracy in detection or security process, TabChain-Ensemble is an all round solution since it offers high-performance intrusion detection as well as secure transaction management. Enhanced predictive performance is

achieved by the integration of ensemble learning, and trust and data integrity are achieved by the blockchain layer. All these attributes render the proposed TabChain-Ensemble framework a useful and scalable solution to the real-world IIoT security application.

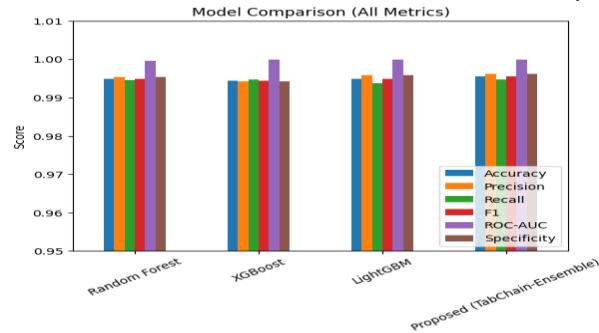


Fig. 7. Comparison of classification performance metrics (accuracy, precision, recall, F1-score, ROC-AUC, and specificity) across different models.

5. CONCLUSION

A new blockchain-enhanced ensemble learning framework presented in this paper includes TabChain-Ensemble, which is an ensemble learning framework developed to guarantee safe and precise intrusion detection in the context of the Industrial Internet of Things (IIoT). The presented solution is based on the XGBoost, LightGBM, and the Random Forest strengths to enhance the classification robustness and generalization, and introduce a permissioned blockchain layer to guarantee a secure, transparent, and tamper-resistant process of managing transactions. Evaluating the TON_IoT dataset experimentally, it was revealed that the proposed model has better performance with the highest accuracy and F1-score of 99.55% and a high ROC-AUC of 0.9998 compared to single base models. The findings also verify that the ensemble method is an efficient way to minimize the classification error, and the blockchain implementation can increase the data integrity at a reasonable cost of latency and throughput. These results demonstrate the practicality of the suggested framework in terms of maintaining the accuracy of detection and system-wide security, and it is applicable to the IIoT in the field. Moreover, the incorporation of lightweight blockchain software and edge-based federated learning may also be added to minimize the computational load and enhance the scalability. The study of adaptive ensemble strategies and real-time implementation in dynamic IIoT environments is also an interesting avenue to develop a better system responsiveness and robustness. In general, the suggested TabChain-Ensemble framework can be a powerful basis of intelligent, scalable and secure IIoT security solutions.

REFERENCES

1. Alandjani, G. (2025). A MARL-federated blockchain-based quantum secure framework for trust management in industrial internet of things. *Scientific Reports*, 15. <https://doi.org/10.1038/s41598-025-23055-2>
2. Almaiah, M., Ali, A., Hajje, F., Pasha, M., & Alohal, M. (2022). A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Sensors (Basel, Switzerland)*, 22. <https://doi.org/10.3390/s22062112>
3. Arachchige, P., Bertók, P., Khalil, I., Liu, D., Çamtepe, S., & Atiquzzaman, M. (2020). A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. *IEEE Transactions on Industrial Informatics*, 16, 6092-6102. <https://doi.org/10.1109/tii.2020.2974555>
4. Aljuhani, A., Kumar, P., Alanazi, R., Albalawi, T., Taouali, O., Islam, A., Kumar, N., & Alazab, M. (2024). A Deep-Learning-Integrated Blockchain Framework for Securing Industrial IoT. *IEEE Internet of Things Journal*, 11, 7817-7827. <https://doi.org/10.1109/jiot.2023.3316669>

5. Kalapaaking, A., Khalil, I., Rahman, M., Atiquzzaman, M., Yi, X., & Almashor, M. (2023). Blockchain-Based Federated Learning With Secure Aggregation in Trusted Execution Environment for Internet-of-Things. *IEEE Transactions on Industrial Informatics*, 19, 1703-1714. <https://doi.org/10.1109/tii.2022.3170348>
6. Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Transactions on Industrial Informatics*, 16, 4177-4186. <https://doi.org/10.1109/tii.2019.2942190>
7. Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., X., & Pathan, M. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. *J. King Saud Univ. Comput. Inf. Sci.*, 36, 101939. <https://doi.org/10.1016/j.jksuci.2024.101939>
8. Salim, S., Moustafa, N., & Turnbull, B. (2025). BFL-SC: A blockchain-enabled federated learning framework, with smart contracts, for securing social media-integrated internet of things systems. *Ad Hoc Networks*, 169, 103760. <https://doi.org/10.1016/j.adhoc.2025.103760>
9. Kumar, P., Kumar, R., Srivastava, G., Gupta, G., Tripathi, R., Gadekallu, T., & Xiong, N. (2021). PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities. *IEEE Transactions on Network Science and Engineering*, 8, 2326-2341. <https://doi.org/10.1109/tnse.2021.3089435>
10. Rahman, M., Hossain, M., Islam, M., Alrajeh, N., & Muhammad, G. (2020). Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *Ieee Access*, 8, 205071 - 205087. <https://doi.org/10.1109/access.2020.3037474>
11. Kumar, R., & Tripathi, R. (2021). DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems. *Transactions on Emerging Telecommunications Technologies*, 32. <https://doi.org/10.1002/ett.4222>
12. Jamil, F., Kahng, H., Kim, S., & Kim, D. (2021). Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms. *Sensors (Basel, Switzerland)*, 21. <https://doi.org/10.3390/s21051640>
13. Kumar, R., Kumar, P., Tripathi, R., Gupta, G., Islam, A., & Shorfuzzaman, M. (2022). Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Transactions on Industrial Informatics*, 18, 8065-8073. <https://doi.org/10.1109/tii.2022.3161631>
14. Ali, S., Li, Q., & Yousafzai, A. (2023). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey. *Ad Hoc Networks*, 152, 103320. <https://doi.org/10.1016/j.adhoc.2023.103320>
15. Ferrag, M., Friha, O., Maglaras, L., & Janicke, H. (2021). Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. *IEEE Access*, PP, 1-1. <https://doi.org/10.1109/access.2021.3118642>
16. Yazdinejad, A., Dehghantanha, A., Parizi, R., Hammoudeh, M., Karimipour, H., & Srivastava, G. (2022). Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks. *IEEE Transactions on Industrial Informatics*, 18, 8356-8366. <https://doi.org/10.1109/tii.2022.3168011>
17. Rokh. (2025). Subset of the TON_IoT Dataset for IoT Intrusion Detection [Data set]. Zenodo. <https://doi.org/10.5281/zenodo.18074069>
18. Hamouda, D., Ferrag, M., Benhamida, N., & Seridi, H. (2022). PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs. *Pervasive Mob. Comput.*, 88, 101738. <https://doi.org/10.1016/j.pmcj.2022.101738>
19. Salim, S., Turnbull, B., & Moustafa, N. (2024). A Blockchain-Enabled Explainable Federated Learning for Securing Internet-of-Things-Based Social Media 3.0 Networks. *IEEE Transactions on Computational Social Systems*, 11, 4681-4697. <https://doi.org/10.1109/tcss.2021.3134463>
20. Khan, A., Laghari, A., Li, P., Dootio, M., & Karim, S. (2023). The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises. *Scientific Reports*, 13. <https://doi.org/10.1038/s41598-023-28707-9>