IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Blockchain and ML for Enhancing IIoT Security Against Cyber Threats

[1]UPPALA DIVYA,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Dr. S SRIDHAR, Miracle Educational Society Group of Institutions
[3]T NARASIMHA MURTHY, Miracle Educational Society Group of Institutions
[1]divyauppala13@gmail.com

ABSTRACT:

The integration of the Industrial Internet of Things (IIoT) and Blockchain into Industrial Supply Chains (ISC) has enhanced operational capabilities, but also significant cybersecurity risks. This research conducts a comparative study of choosing the best-performing lightweight machine learning (ML) algorithms for detecting cybersecurity breaches within blockchain-enabled ISC frameworks. For the WUSTL-IIoT-2021 dataset, we trained and tested classifiers including Decision Tree, K-Nearest Neighbors, Naïve Bayes, Random Forest, and ensemble methods such as Bagging and Stacking. Model accuracy was also improved with feature selection and dataset balancing. The findings indicate that Decision Tree has the lowest latency and XGBoost the highest accuracy. This study showcases the versatility of blockchain technology with lightweight machine learning in providing actionable IIoT cybersecurity frameworks. IIoT networks may benefit from real-time, scalable, and resilient threat response systems.

Keywords: cybersecurity, IIoT, blockchain

INTRODUCTION

The growing digital transformation of industrial processes has accelerated the implementation of Industrial Internet of Things (IIoT) technologies in Supply Chains. The IIoT improves and streamlines operations using real-time data and automation; however, the threat of cyberattacks increases. It is extremely difficult for traditional systems to adequately respond to such challenges. Blockchain technology, in contrast, provides a means to address these challenges. It is a decentralized and incorruptible network that is able to secure the data's integrity in the industrial networks. Nonetheless, enforcing proactive defense measures entails having intelligent mechanisms for threat detection. This dissertation investigates how integrating lightweight machine learning (ML) models into an ISC environment backed by blockchain

technology can holistically enable proactive cyber threat detection. The use of lightweight ML algorithms is preferred for implementation on IIoT systems because of their low resource requirements. Through comparison of Decision Tree, KNN, and Naïve Bayes models, we hope to offer solutions that can optimize security in resource-limited systems. The provided solutions will strengthen cybersecurity while promoting responsiveness and scalability of the systems.

RELATED WORK

The cybersecurity landscape of the Industrial Internet of Things (IIoT) and blockchain-driven supply chains continues to attract attention. Ismail et al. (2024) performed a comparative analysis on the application of some lightweight machine learning (ML) algorithms, Naïve Bayes, KNN, and Decision Tree, as well as ensemble classifiers for cyber-attack detection in IIoT. Their findings focused on the universally noted trade-off between cost and accuracy and labeled Decision Tree as a lightweight optimal solution for real-time applications. Dandan et al. (2024) looked at an ML model for detecting security breaches within industrial networks that was integrated with blockchain technology. Although the blockchain provided some advantages in terms of data integrity and trust, the study raised concerns on the processing latency and the complexity of its on-the-spot workings with real-time threat detection. Dawoud et al. (2024) suggested a hybrid model offering a fusion of supervised and unsupervised ML models along with blockchain technology to improve intrusion detection. Enhanced accuracy was noted with this design; however, the architecture was said to have a significant computational cost which limited scalability. Reza et al. (2024) examined the use of XAI (SHAP) to improve the transparency of ML decisions within intrusion detection systems. Their interpretation-focused work, while useful, brought to light the issue of requiring extensive labeled datasets, which is rarely feasible in industrial settings. Zolanvari et al. (2019) proposed solutions to the optimization of ML models using RFE and noted improvements in performance and speed due to reduced dimensionality. While this technique reduced the risk of overfitting and the computational cost, the risk of losing crucial features was still a problem.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	Contribution	Impact on Research
Ismail et al. (2024)	Comparative analysis of lightweight ML models (e.g., DT, KNN, NB) for cyber-attack detection in IIoT.	Identified Decision Tree as a low-latency, efficient model suitable for resource-limited ISC.
Dandan et al.	Integration of blockchain with	Highlighted blockchain's

(2024)	ML models to ensure secure and tamper-proof cyber-attack detection.	potential and challenges like latency and implementation complexity.
Dawoud et al. (2024)	Hybrid intrusion detection using both supervised and unsupervised ML models in IIoT.	Demonstrated improved accuracy; emphasized challenges with scalability and processing overhead.
Reza et al. (2024)	Introduced SHAP-based Explainable AI for improving ML interpretability in intrusion detection systems.	Enhanced model transparency but exposed the dependency on large labeled datasets.
Zolanvari et al. (2019)	Applied Recursive Feature Elimination (RFE) to optimize intrusion detection ML models.	Improved performance and reduced complexity; risked excluding important features.

PROPOSED APPROACH

The approach in question aims to protect cyber-attack threats using lightweight machine learning (ML) algorithms within blockchained Industrial Supply Chains (ISC). Taking into account the IIoT environment's limited resources, the solution favors high accuracy models which identify threats at a low computational cost. The approach starts with data harvesting from IIoT devices and utilizes the WUSTL-IIOT-2021 dataset which contains labeled normal and attack traffic records. To solve the class imbalance issue, Random Under Sampling is applied. To improve feature selection and focus on the most relevant attributes, the Extra Trees Classifier is used, which decreases dataset dimensionality and enhances processing speed. Several ML algorithms are trained and assessed, including Decision Tree, K-Nearest Neighbors, Naïve Bayes, Random Forest, and ensemble algorithms such as Bagging, Stacking, and CatBoost. Decision Trees are known for their rapid execution, which enhances real-time applicability, while XGBoost provides the best classification results. To securely document all actions and maintain data integrity, the system incorporates blockchain technology which fortifies the data against alteration and clears operational obfuscation. Combining ML and blockchain technology fosters proactive and resilient cybersecurity frameworks. This approach is modular and IIoT supply chains can easily scale and adapt to these frameworks.

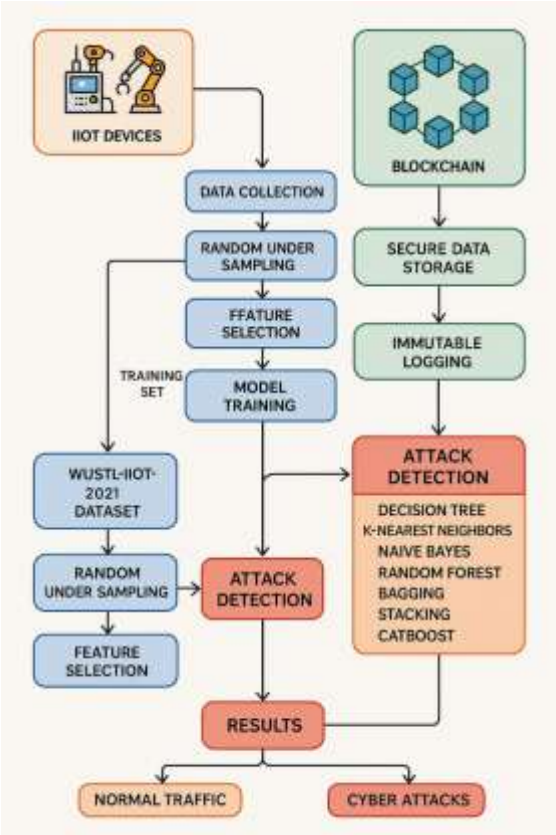


Figure 1: Proposed Cyber Attack Prediction System

METHODOLOGIES

The methodology for this project follows a structured, multi-phase approach to implement lightweight machine learning techniques for cyber-attack detection in blockchain-enabled industrial supply chains. The process begins with data collection and loading, using the WUSTL-IIOT-2021 dataset which includes millions of records from IIoT network traffic labeled as normal or malicious. Due to significant class imbalance, Random Under Sampling is applied to create a balanced and manageable dataset for effective training.

Next, data preprocessing is performed by removing irrelevant features such as IP addresses and timestamps, converting categorical variables using label encoding, handling missing values, and applying normalization with StandardScaler to maintain uniform feature scales.

Following preprocessing, feature selection is executed using the Extra Trees Classifier, which identifies the most informative features based on their importance scores. SelectFromModel is then used to retain features above the average threshold, reducing dimensionality and enhancing model performance.

The refined dataset is split into training (80%) and testing (20%) sets. Several machine learning algorithms are then trained and tested, including Random Forest, Decision Tree, K-Nearest Neighbors (KNN), Gaussian Naïve Bayes, Bagging, Stacking, CatBoost, and XGBoost. Each model is evaluated based on accuracy, precision, recall, and F1-score to determine its effectiveness.

In addition, the system is integrated with blockchain technology to record IIoT transaction data securely, ensuring immutability and integrity. Blockchain acts as a trust anchor, supporting the ML detection process by providing verified data inputs and secure audit trails.

The entire pipeline is designed to be lightweight, scalable, and compatible with IIoT environments. Visualizations such as feature importance graphs and performance bar charts are generated to aid analysis. The combination of low-latency

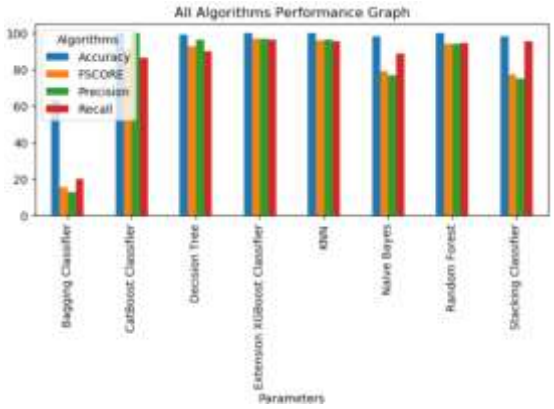
ML models and secure blockchain infrastructure presents a reliable, efficient cybersecurity solution for modern industrial supply chains.

RESULTS

The experimental evaluation was conducted using the WUSTL-IIOT-2021 dataset, focusing on both performance metrics and computational efficiency. After preprocessing and feature selection, the dataset was reduced from 41 to 14 critical features. Models were trained on 80% of the data and tested on the remaining 20%, ensuring a reliable assessment of detection capabilities.

Among the evaluated algorithms, XGBoost and K-Nearest Neighbors (KNN) exhibited the highest accuracy and F1-scores, making them effective for detecting a wide range of cyber-attacks. Decision Tree, though slightly lower in accuracy, demonstrated the fastest execution time and minimal resource consumption, marking it as the most lightweight and practical model for real-time IIoT environments.

Ensemble models like Bagging and Stacking showed moderate results but required significantly more computational power, making them less ideal for lightweight implementations. The performance metrics accuracy, precision, recall, and F1-score were visualized using bar graphs, making it easy to compare model effectiveness.



All Algorithms Performance Graph

Attach Detection

DISCUSSION

The findings of this study highlight the effectiveness of lightweight machine learning models in detecting cyber-attacks within blockchain-enabled industrial supply chains. Decision Tree, despite its simplicity, provided rapid classification with minimal computational load, making it well-suited for real-time deployment in IIoT systems. XGBoost, on the other hand, delivered the highest accuracy and robustness in identifying complex attack patterns but at the cost of higher resource usage.

The use of ensemble models such as Bagging and Stacking offered marginal performance improvements but introduced latency and required more memory, which

may not be feasible in constrained IIoT environments. This underlines the trade-off between model complexity and system efficiency—a critical factor in industrial applications.

Moreover, blockchain integration significantly enhanced system transparency, data integrity, and auditability. It ensured that all activity logs remained tamper-proof, strengthening trust and reliability across the supply chain network.

A key observation is the importance of preprocessing and feature selection, which played a vital role in reducing noise and optimizing detection accuracy. By selecting the most relevant features, the models trained faster and generalized better on test data.

CONCLUSION

This report demonstrated the lightweight ML model-based cyber-attack detection framework for blockchain-empowered Industrial Supply Chains (ISC) while maintaining high efficiency and robust security. This research examines algorithms such as Decision Tree, KNN, Naïve Bayes, and XGBoost, determining that Decision Tree is the most resource-efficient and XGBoost the most accurate in cyber threat detection. Applying feature selection dramatically increased speed and accuracy by simplifying the dataset. Using blockchain applications ensures immutability and secure logging of transactions which complements the machine learning threat detection system by fortifying data trustworthiness. The proposed system solves the lack of computational resources, the need for active real-time surveillance, and escalating cyber-attacks in the IIoT environments. The validated results demonstrated that integrating optimized machine learning models and blockchain technology decisively enhances cybersecurity within the industrial supply chain. Subsequent research might investigate the use of hybrid machine learning models, real-time applications, and innovative explainable AI functionalities aimed at enhancing detection transparency and adaptability to evolving threat environments.

REFERENCES

[1] M. Umair, M. A. Cheema, O. Cheema, H. Li, and H. Lu, ‘‘Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT,’’ Sensors, vol. 21, no. 11, p. 3838, Jun. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/11/3838

[2] S. Ismail and H. Reza, ‘‘Security challenges of blockchain-based supply chain systems,’’ in Proc. IEEE 13th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), Oct. 2022, pp. 1–6.

[3] S. Ismail, H. Reza, K. Salameh, H. K. Zadeh, and F. Vasefi, ‘‘Toward an intelligent blockchainIoT-enabled fish supply chain: A review and conceptual framework,’’ Sensors, vol. 23, no. 11, p. 5136, May 2023.

[4] M. Ohm, H. Plate, A. Sykosch, and M. Meier, ‘‘Backstabber’s knife collection: A review of open source software supply chain attacks,’’ in Proc. Backstabber’s Knife Collection, Rev. Open Source Softw. Supply Chain Attacks, Lisbon, Portugal. Cham, Switzerland: Springer, Jun. 2020, pp. 23–43.

[5] M. Watney, ‘‘Cybersecurity threats to and cyberattacks on critical infrastructure: A legal perspective,’’ in Proc. Eur. Conf. Cyber Warfare Secur., vol. 21, no. 1, 2022, pp. 319–327.

[6] S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, ‘‘Towards a lightweight security framework using blockchain and machine learning,’’ Blockchain, Res. Appl., vol. 5, no. 1, Mar. 2024, Art. no. 100174.

[7] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, ‘‘Cybersecurity data science: An overview from machine learning perspective,’’ J. Big Data, vol. 7, no. 1, pp. 1–29, Dec. 2020.

[8] A. Yeboah-Ofori, S. Islam, S. W. Lee, Z. U. Shamszaman, K. Muhammad, M. Altaf, and M. S. Al-Rakhami, ‘‘Cyber threat predictive analytics for improving cyber supply chain security,’’ IEEE Access, vol. 9, pp. 94318–94337, 2021.

[9] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, ‘‘EdgeIIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning,’’ IEEE Access, vol. 10, pp. 40281–40306, 2022.

[10] Z. E. Huma, S. Latif, J. Ahmad, Z. Idrees, A. Ibrar, Z. Zou, F. Alqahtani, and F. Baothman, ‘‘A hybrid deep random neural network for cyberattack detection in the industrial Internet of Things,’’ IEEE Access, vol. 9, pp. 55595–55605, 2021.

[11] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, ‘‘X-IIoTID: A connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of Things,’’ IEEE Internet Things J., vol. 9, no. 5, pp. 3962–3977, Mar. 2022.

[12] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero, and L. A. Trejo, ‘‘Toward the protection of IoT networks: Introducing the LATAM-DDoS-IoT dataset,’’ IEEE Access, vol. 10, pp. 106909–106920, 2022.

[13] S. Ismail, D. Dawoud, and H. Reza, ‘‘Towards a lightweight identity management and secure authentication for IoT using blockchain,’’ in Proc. IEEE World AI IoTCongr. (AIIoT), Jun. 2022, pp. 077–083.

[14] S. Ismail, D. W. Dawoud, T. Al-Zyoud, and H. Reza, ‘‘Towardsblockchainbased adaptive trust

management in wireless sensor networks,'' in Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT), May 2023, pp. 163–168.

[15] N. Malik, K. Alkhatib, Y. Sun, E. Knight, and Y. Jararweh, ''A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems,'' Appl. Stochastic Models Bus. Ind., vol. 37, no. 3, pp. 391–412, May 2021.

[16] S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, ''A blockchain-based IoT security solution using multichain,'' in Proc. IEEE 13th Annu.Comput.Commun. Workshop Conf. (CCWC), Mar. 2023, pp. 1105–1111.

[17] S. Ali, Q. Li, and A. Yousafzai, ''Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey,'' Ad Hoc Netw., vol. 152, Jan. 2024, Art. no. 103320.

[18] R. K. Singh, R. Mishra, S. Gupta, and A. A. Mukherjee, ''Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda,'' Comput. Ind. Eng., vol. 175, Jan. 2023, Art. no. 108854.

[19] S. Al-Farsi, M. M. Rathore, and S. Bakiras, ''Security of blockchain-based supply chain management systems: Challenges and opportunities,'' Appl. Sci., vol. 11, no. 12, p. 5585, Jun. 2021.

[20] S. S. Mathew, K. Hayawi, N. A. Dawit, I. Taleb, and Z. Trabelsi, ''Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial IoT: A survey,'' Cluster Comput., vol. 25, no. 6, pp. 4129–4149, Dec. 2022.