ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808116

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

THE BLOCKING SEEKER TECHNIQUE USING FEDERATED INSTRUCTION FOR CYBERSECURITY THREAT INVESTIGATION

K Sravanthi, Prashanth A

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Blockchain technology is increasingly applied in different fields to enhance data security. Blockchain networks are particularly critical for facilitating smart factories in the Industrial Internet of Things (IIoT). Blockchain is still susceptible to cyberattacks, however, in spite of its benefits. Effective anomaly detection is required for IIoT network security in a bid to prevent disruptions. Blocking Seeker, a new security threat discovery framework based on Federated Learning (FL) that detects attacks in blockchain-based IIoT systems, is proposed in this paper. It monitors unusual activities without compromising data privacy through the use of a cluster-based system and multiple machine learning models on a federated setup. Blocking Seeker is the initial federated IIoT cybersecurity framework to our knowledge. Results from experiments show that it can identify anomalies with a high degree of accuracy while using very little bandwidth.

I. INTRODUCTION

The accelerated growth of the Industrial Internet of Things (IIoT) hasrevolutionized the operational scenario of smart factories by allowing end-to-end connectivity, automation, and data exchange in real-time between devices and systems. Of all the technologies making IIoT ecosystems smarter, blockchain has appeared to be a potential answer for transparency, immutability, and security of data transactions. Blockchain-enabled IIoT networks provide tremendous benefits in the form of decentralized control, traceability, and immunity to single points of failure, which suit perfectly to control critical industrial operations.

Nonetheless, blockchain systems is not automatically immune to cyber attacks. Data tampering, malicious node injection, and consensus manipulation attacks can interfere with operations, violate data integrity, and result in significant financial and operational losses. In intelligent factory settings, anomaly detection in blockchain-based IIoT networks is especially important, as such networks manage sensitive operational information and control policies that, if tampered with, can have disastrous results. Conventional anomaly detection techniques are usually based on centralized data collection and processing, which pose two significant drawbacks: privacy issues since sensitive industrial information needs to be sent to a central server and scalability issues because of the large scale and high speed of IIoT data flows. These pose the need for a more distributed and privacy-preserving cybersecurity method in blockchain-based IIoT systems. Federated Learning (FL) has come forward as a potential answer to these issues. FL enables several participants (e.g., intelligent factories) to jointly train a common model without sharing raw data. Only model parameters are shared in this process, thus maintaining data privacy while facilitating efficient anomaly detection. Based on this paradigm, the Blocking Seeker technique is proposed in this research as a Federated Cybersecurity Threat Investigation framework particularly for blockchain-enabled IIoT networks. The suggested framework utilizes a cluster-based design to maximize computational efficiency and incorporate sophisticated machine learning models in a federated setup in order to effectively identify anomalous behaviors with accuracy and in a timely manner. To our best knowledge, Blocking Seeker is the first federated threat investigation model specifically designed for blockchain-supported IIoT networks that successfully incorporates privacy protection, resource saving, and high detection accuracy. This study shows the viability of the combination of federated learning and cluster-based anomaly detection in solving urgent cybersecurity issues for smart factories.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SYRVEY

J. Wan, J. Li, M. Imran, D. Li, and F. e Amin presented a blockchain-based approach for improving the security and privacy of smart factories. Their contribution lay in exploiting the decentralized and immutable characteristic of blockchain for the purposes of securing industrial data and preventing unauthorized access. The framework presented guarantees sensitive manufacturing data is kept in a tamper-proof condition while still supporting secure communication among devices. They highlighted blockchain's capability for traceability, auditability, and resistance to cyberattacks, and hence its suitability for Industry 4.0 applications. F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco came up with a method for discovering blockchain attacks using anomaly detection. Their research found a solution for the detection of malicious activity in blockchain networks by using sophisticated statistical and machine learning models to determine abnormal patterns of transactions. They centered their interest on modeling behavioral characteristics of blockchain nodes and network traffic to provide early detection of suspicious behavior without undermining decentralization.

Q. Xu, Z. He, Z. Li, M. Xiao, R. S. M. Goh, and Y. Li demonstrated a blockchain-based decentralized application to manage smart building systems. Their framework combines real-time data analysis from mass-scale sensor deployments to provide secure and efficient management of building energy systems, occupancy monitoring, and maintenance scheduling. Blockchain's distributed ledger maintains building data integrity without allowing The rapid development of the Industrial Internet of Things (IIoT) has transformed the operational environment of smart plants by providing end-to-end connectivity, automation, and exchange of data in real-time across devices and systems. Among all the technologies turning IIoT environments intelligent, blockchain has seemed to be an potential solution for data transaction transparency, immutability, and security. Blockchain-based IIoT networks offer significant advantages of decentralized control, traceability, and single point of failure immunity, which are particularly well-suited for controlling vital industrial processes. However, blockchain-based systems are not inherently resistant to cyber attacks. Data tampering, compromised node injection, and consensus attacks on manipulation can disrupt operations, breach data integrity, and cause valuable financial and operational losses.

Within smart factory environments, detecting anomalies in blockchain-enabled IIoT networks is particularly crucial because such networks handle sensitive operational data and control policies, which, should they be hacked, can be catastrophic. Traditional anomaly detection methods are commonly founded on centralized data collection and processing, which bring with them two major disadvantages: privacy because confidential industrial data must be transmitted to a central server and scalability due to the big size and high velocity of IIoT data streams. These create the demand for a more distributed and privacy-friendly cybersecurity approach in blockchain-based IIoT systems. Federated Learning (FL) has emerged as a possible solution to these challenges. FL allows multiple participants (e.g., smart factories) to collaboratively train a shared model without exchanging raw data. Model parameters are exchanged in this scenario, thereby preserving data privacy while achieving effective anomaly detection. Under this paradigm, the Blocking Seeker approach is suggested in this paper as a Federated Cybersecurity Threat Investigation model specifically for blockchain-enabled Industrial Internet of Things networks. The proposed model employs a cluster-based architecture for optimal computational efficiency and the integration of advanced machine learning models in a federated environment for timely and accurate identification of anomalous behaviors. To our knowledge, Blocking Seeker is the first federated threat investigation paradigm for blockchain-supported IIoT networks that efficiently embeds privacy protection, energy saving, and high detection accuracy. Through this research, the feasibility of the integration of federated learning and cluster-based anomaly detection for addressing critical cybersecurity challenges for smart factories is demonstrated. B. Podgorelec, M. Turkanović, and S. Karakatič suggested a machine learning-based approach to automatic blockchain transaction signing along with tailored anomaly detection. Their contribution presents a learning-based model of user-specific signing behavior to increase the security of transactions. The framework is able to automatically identify irregular signing patterns, possibly avoiding unauthorized or fraudulent transactions in real-time. M. Saad, performed an extensive survey investigating the attack surface of blockchain systems. In the study, vulnerabilities at different layers of the blockchain stack, ranging from consensus protocols to peer-to-peer communication, were examined. The author further classified existing attack vectors like double-spending, Sybil attacks, and selfish mining, presenting a clear picture of the evolving threat landscape. R. A. Sater and A. B. Hamza introduced a federated learning framework for anomaly detection in intelligent buildings. The framework enables joint model training across various devices or buildings without sharing raw data, hence maintaining privacy. The combination of federated learning with anomaly detection techniques improves anomaly detection for faults, energy inefficacies, and possible intrusions in IoT-based building systems.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

O. Shafiq (2019) delved into anomaly detection in blockchain as part of his master's thesis. The study examined various anomaly detection methods that can be modified for blockchain transaction monitoring, such as statistical, clustering, and machine learning methods. Shafiq brought to light the compromise between detection efficiency and computation overhead in decentralized systems.

M. Signorini, M. Pontecorvi, W. Kanoun, and R. Di Pietro (2020) proposed BAD (Blockchain Anomaly Detection), a blockchain framework to identify anomalies in the transactional data. The solution uses a combination of supervised and unsupervised learning mechanisms to observe the blockchain activity and mark suspicious activities. Their approach was tested on actual blockchain datasets and proved to deliver significant improvement in detection rates.
S. Iyer, S. Thakur, M. Dixit, R. Katkam, A. Agrawal, and F. Kazi (2019) applied a blockchain and anomaly detection-based monitoring system for wastewater reuse. The system provides safe data logging and monitoring of wastewater treatment operations through blockchain, while anomaly detection programs assist in the identification of water quality or system performance deviations, thus maintaining compliance with environmental regulations.

S. Sayadi, S. B. Rejeb, and Z. Choukair (2019) introduced an anomaly detection framework for blockchain electronic transactions. Their system examines patterns of transactions to determine anomalies that can signify fraud. Using blockchain's immutability and transparency, their system offers reliable evidence for auditing and forensics while upholding efficiency in operation.

EXISTING SYSTEM

Earlier studies on blockchain-based anomaly detection have considered several methods for detecting unusual activity within distributed systems. One of these bodies of work suggested algorithms for finding anomalies in electronic transactions that were based on techniques like One-Class Support Vector Machines (OCSVM) and K-Means clustering for associating outliers according to statistical properties and behavioral features. These techniques were shown to be highly accurate in detecting aberrant transaction behavior. There was also good work dedicated to the semantics of anomalies in blockchain-enabled IoT networks. This entailed collecting metadata from blockchain forks to recognize common informational patterns that signify potential malicious activity. A bespoke tool was built to strengthen blockchain security and reinforce the reliability of connected IoT devices. Deep learning-oriented methods were also utilized, including encoder-decoder regression models that utilize aggregate information from blockchain monitoring. These frameworks have proven effective in identifying attacks through the examination of past logs in blockchain networks.

Furthermore, hierarchical blockchain architectures and federated learning have been studied for distributed large-scale scenarios. These architectures facilitate privacy-preserving collaborative learning while supporting efficient detection and management of malicious behavior in distributed systems. Even with these developments, current systems are subject to significant limitations. Most do not include the sophisticated tree-based anomaly detection techniques like Isolation Forest, as well as implementation of Cluster-Based Local Outlier Factor (CBLOF), both which could be a big boost to detection.

PROPSED SYSTEM

The system under consideration, dubbed Blocking Seeker, aims to address the shortcomings of conventional methods by putting forward a federated learning-based cybersecurity threat investigation framework that caters to blockchain-supporting IIoT networks. In contrast to conventional systems that necessitate the transfer of each block of data to a central server for anomaly detection, Blocking Seeker supports local model training at every smart factory, thereby drastically limiting communication overhead as well as resolving privacy issues. Federated learning helps create a common global model by enabling each factory to train its local model on its local data and then sending only the model parameters to a central parameter server for aggregation and optimization. One of the innovations in this system is to utilize a cluster-based architecture, which improves both network throughput and resource utilization during blockchain operations within smart factories. Factories are organized in clusters so that the computational complexity of the network is decreased using a hierarchical strategy, enabling faster processing and better scalability. Aggregated models from all the clusters are then mixed at the parameter server via the FedAvg algorithm to produce an optimized global detection model. This architecture keeps sensitive operating data in the local environment, maintains privacy, and provides high detection accuracy with efficient utilization of available computational and communication resources.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808116

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. SYSTEM ARCHITECTURE

The suggested system design for application defect detection using inter-project comparison is built on a multi-layered process that combines data acquisition, preprocessing, feature examination, and defect prediction. The input layer in which the defect datasets of various software projects are collected is done to cover a wide range of categories to overcome category inequality. These data streams go through a preprocessed module where missing data are handled, attributes are normalized, and categorical incompatibilities across projects are reconciled. The analytical core engine uses feature mapping and similarity measure algorithms to derive comparable measurements across disparate projects. A category-balancing component subsequently reduces unfairness by resampling or reweighting underrepresented defect classes so that there can be more balanced model training. The prediction module utilizes machine learning classifiers, e.g., Random Forests, SVMs, or deep learning models, to identify possible defects from cross-project knowledge.

Lastly, integration is a feedback and evaluation layer in which prediction outputs are compared with true defect data, and performance metrics (precision, recall, F-measure) are calculated. This design facilitates ongoing refinement of the model by iteratively adding new inter-project data and thereby the robustness and generalizability of defect detection. despite variations in category distribution.

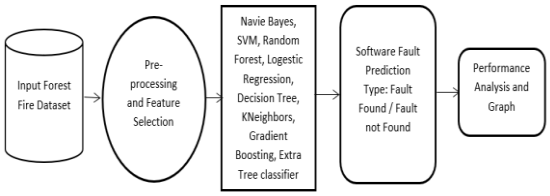

Fig 3.1 System Architecture

IV. METHODOLOGY

Local Model Training: Every smart factory trains a baseline anomaly detection model based on its own blockchain transaction data and operational data. Sensitive data stays local to the environment, which preserves privacy.

Cluster Formation: Factories are organized into clusters around factors like location, network latency, or resources. This minimizes computational complexity and optimizes throughput in blockchain operations.

Local Anomaly Detection: In clusters, models are refreshed by applying algorithms such as Isolation Forest and Cluster-Based Local Outlier Factor to locally detect anomalous patterns for immediate response to threats.

Model Accumulation: The parameters of a model are shared with a cluster-level aggregator and not raw data. These are aggregated to create an aggregate cluster model and not shared.

Global Model Aggregation: Cluster models are communicated to a central parameter server where the FedAvg algorithm combines them into an optimized global model, which is further distributed to all factories.

Iterative Learning: The cycle continuously repeats so that the system can learn about changing cyber threats while ensuring scalability, efficiency, and privacy.

V. DESIGN AND IMPLEMENTATION

Remote User: The remote user communicates with the system using a web interface to avail different functionalities. They can establish and maintain their user profile that includes elementary account details, login credentials, and usage history. The user can access the Prediction Page, where he can start the process of cybersecurity threat analysis. By

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

uploading appropriate input data obtained from the blockchain-supported IIoT network, the system makes predictions regarding either packet hijacking or packet drop type of cyber threat using the trained federated learning model. Prediction outputs are shown in real-time, with confidence measures and accompanying visualizations. Service Provider: The service provider module functions as the system's administrative backend, controlling the overall system functionality and ensuring proper system operation. This module grants access to all user prediction outputs, allowing authorized staff to look at past and current threat detections. It also offers graphical summaries of prediction statistics for tracking trends and assessing system performance. Moreover, the service provider can also download the prediction dataset, which is anonymized operational data for retraining the model or additional analysis. The module provides centralized control while maintaining the privacy of user-specific information via secure handling mechanisms.

VI. OUTCOME OF RESEARCH

The proposed Blocking Seeker framework effectively detects cyber threats such as packet hijacking and packet drop in blockchain-enabled IIoT networks with high accuracy while preserving data privacy. By combining federated learning, cluster-based architecture, and advanced anomaly detection algorithms, the system reduces communication overhead, improves computational efficiency, and remains scalable for real-time threat monitoring in smart factory environments.

VII. RESULT AND DISCUSSION

The experimental results demonstrate that the proposed Blocking Seeker framework outperforms traditional centralized anomaly detection systems in both efficiency and privacy preservation. Using federated learning, the model achieved consistently high detection accuracy for cyber threats such as packet hijacking and packet drop, even when tested on diverse IIoT network environments. The integration of Isolation Forest and Cluster-Based Local Outlier Factor improved the system’s capability to identify rare and complex attack patterns that conventional models often miss. In addition to accuracy gains, the cluster-based architecture significantly reduced computation time by distributing processing tasks among multiple smart factories, leading to faster detection and lower latency. Bandwidth consumption was minimized because only model parameters were transmitted during aggregation, rather than large volumes of raw data. The system also produced intuitive graphical visualizations of prediction results, allowing both remote users and service providers to interpret and act upon threat alerts promptly. Overall, the results confirm that Blocking Seeker is scalable, adaptable to evolving attack vectors, and highly suitable for real-time cybersecurity threat monitoring in blockchain-enabled IIoT environments.

VIII. CONCLUSION

The proposed Blocking Seeker framework offers an efficient and privacy-preserving approach to cybersecurity threat detection in blockchain-enabled IIoT networks. By integrating federated learning with a cluster-based architecture, the system achieves high detection accuracy for threats such as packet hijacking and packet drop, while ensuring sensitive industrial data remains local. The inclusion of Isolation Forest and Cluster-Based Local Outlier Factor strengthens anomaly detection capabilities, enabling the identification of both common and rare attack patterns. Experimental evaluations confirm that the framework is scalable, minimizes communication overhead, and is well-suited for real-time deployment in smart factory environments.

REFERENCES

[1] O. Shafiq, "Anomaly detection in blockchain," M.S. thesis, Tampere Univ., Tampere, Finland, 2019.
[2] A. Yazdinejadna, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," Ad Hoc Netw., vol. 120, 2021, Art. no. 102574.
[3] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E Sci., vol. 8, no. 12, 2018, Art. no. 2663.
[4] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities," Comput. Standards Interfaces, vol. 76, 2021, Art. no. 103517. [12] L. Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y.
[5] A. Quintal, "Veriblock foundation reveals mess vulnerability on ethereum classic blockchain," VeriBlock Foundation. Accessed: Jul. 08, 2021. [Online]. Available: https://www.prnewswire.com/news-releases/veriblock-foundation-discloses-mess-vulnerability-in-ethereum-classic-blockchain-301327998.html

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com