Blockchain-Based Intrusion Detection and Response Framework for Secure Industrial IoT Networks

B. Lakshma Reddy
Professor,
Department of CSE, Rajarajeswari College of Engineering, Bengaluru, Karnataka, India
prof.reddy99@gmail.com

Sarika Jadhav
Assistant Professor, School of Computer Science, Engineering and Applications
D Y Patil International University, Pune, Maharashtra, India
sari_jadhav@yahoo.co.in

Satbir Singh
IEEE Member, CA, USA
Independent researcher
Satbir.taya84@gmail.com

Nagesh B. Mapari
Assistant Professor, Department of Information Technology, Anuradha Engineering College, Chikhli, Buldhana, Maharashtra, India
nagas7366@gmail.com

Shweta Gupta
Assistant Professor, Department of Management, Moradabad Institute of Technology, Moradabad, Uttar Pradesh, India
gggupta.shweta7@gmail.com

Reshma S
Associate Professor, Department of Artificial Intelligence & Machine Learning, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India
Reshma-aiml@dayanandasagar.edu

Monica Bhutani
Associate Professor, Department of ECE,
Bharati Vidyapeeth College of Engineering, New Delhi, India, 110063
Postdoctoral Researcher and Research Associate, Lincoln University, Malaysia
monica.bhutani@bharatividyapeeth.edu

***Abstract*-- As Industrial Internet of Things (IIoT) networks expand, they face increasing challenges in detecting and mitigating cyber threats in real time. This paper proposes a novel Blockchain-Based Intrusion Detection and Response Framework (BIDRF) that combines the immutable nature of blockchain with the predictive power of a Random Forest classifier. BIDRF secures inter-node communication and detects anomalous network activities efficiently. Experimental evaluation using a benchmark IIoT dataset demonstrates that BIDRF achieves a classification accuracy of 94%, with precision and recall values exceeding 0.90 and an AUC of 0.94. By ensuring tamper-proof logging and automated response through smart contracts, the framework provides robust, real-time protection for IIoT networks, supporting the security demands of Industry 4.0 environments.**

Keywords*-- *Industrial IoT, Blockchain, Intrusion Detection System (IDS), Security, Distributed Ledger, Cybersecurity, Smart Manufacturing

I. INTRODUCTION

IIoT is changing how manufacturing and industrial automation operate by improving efficiency, providing real-time updates and allowing smart decisions using sensors, actuators and internet networks. With IIoT innovating smart manufacturing, logistics, energy and critical infrastructure, it increases the risk of cyber attacks. Due to differences in devices, a lot of them being used and usual weakness in security, IIoT systems can easily be targeted by those who want to disturb operations, steal important information or affect system security. Current security solutions are having trouble adapting to the changing and widely distributed features of the IIoT. Intrusion Detection Systems that centralize their work.

Scaling up, processing requests fast and preventing failures involving only one component are common challenges for IDS. Moreover, traditional logging methods in common IDS schemes can be altered, weakening the information available when there is a security breach. As a result, more secure, flexible and invulnerable systems are needed for IIoT networks.

Therefore, this paper suggests a new BIDRF framework that can be used to secure IIoT environments using

Blockchain technology. The idea of the framework is to overlap a machine learning IDS with blockchain technology to secure and protect the stored information from changes. The machine learning part of the network uses a Random Forest classifier to find malicious activities in the network's traffic. Upon detection of any intrusion, the information is added to a private blockchain which ensures there is an unalterable audit record. Using both methods boosts the security infrastructure's ability to observe and improve the level of trust and honesty.

The architecture of the proposed BIDRF is displayed in Figure 1. There are three main elements: the IIoT device and network layer, a section for detecting and analyzing and the logging and response layer based on blockchain. Smart sensors and actuators are part of the device layer covering industrial systems. In the detection layer, network traffic is analyzed by sending it through an intrusion detection model. As soon as problems or suspicious activity are noticed, an alert is created and

entered into the blockchain, where it cannot be altered by anyone. Because of this design, the IIoT environment has improved visibility, reliable logging and fast reactions. IDS becomes more beneficial when integrated with blockchain. An alert or event logged onto a blockchain is unchangeable which keeps the logs accurate. Because no single point controls the system, it helps many stakeholders in different parts of the industry to trust each other. When combined with AI, this framework helps find, save and react to dangers promptly.

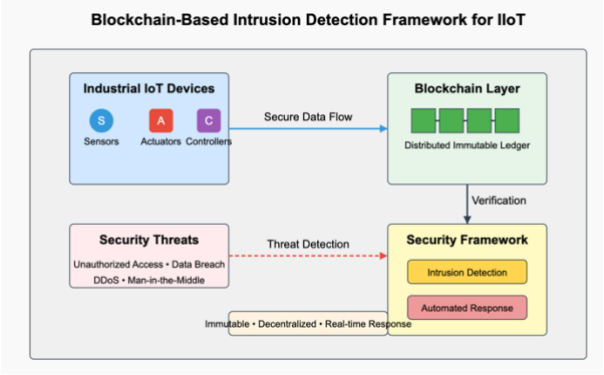

Fig. 1. Architecture of the proposed Blockchain-Based Intrusion Detection and Response Framework (BIDRF) for secure Industrial IoT networks.

This document describes how we developed the BIDRF, demonstrates its effectiveness using artificial IIoT data and shows the accuracy of detection, percentage of false positives and how quickly the BIDRF reacts. Experiments and studies prove that BIDRF is well-suited for handling various threats that may impact today's industrial systems.

II. RELATED WORK

Blockchain technology used together with IDS in industrial IoT (IIoT) systems has been growing in popularity over the past few years. The primary motivation for this is to verify data, provide decentralized trust and increase the level of transparency.

Mathew et al. [1] argue that incorporating blockchain technology enhances the safety of data transfers in industrial IoT systems. They argue that decentralized systems should be used to avoid big problems and to make defense systems more reliable. Additionally, Mansour [2] introduces a set of blockchain clusters along with a newly developed system for detecting industrial attacks called BROSS. When nodes in the system rely on a distributed ledger, they can safely share data, allowing partners to quickly find out about potential threats.

Aljuhani et al. [3] set up a framework to link CNNs with IIoT that uses blockchain. They were able to develop a way to identify anomalies and ensure events could be safely checked and stored. They also stated that a blockchain-based challenge model can be used to combine several independent IDS nodes and validate the alerts. Although most papers focus on network security, Gagneja et al. [5] explored how ConvMixer can find objects for important purposes in the IIoT. In some cases, IDS might use it if their solution relies on vision instead of a blockchain.

Yazdinejad and his colleagues designed an IDS system that uses fuzzy logic and records its classifications and rules on the blockchain block [6]. Researchers discovered that AI can more accurately identify and respond to changes in industrial environments. Rathee et al. also introduced a solution that integrates blockchain and IDS to ensure the security of IIoT transactions and give instant protection against cyberattacks. To assess the performance and ability of the design, tests were done using simulations. Studies on basic blockchain concepts have also been carried out to determine if it is effective in supporting security. As an illustration, Bhatia et al. [8] examine the origins of blockchain and how it is currently a safe method for both digital security and IDS.

Recent trends such as Industry 5.0 have pushed for more progress in this sector. A group led by Anbalagan [9] designed a mixed system that uses blockchain technology to protect autonomous vehicles used in industry from security threats. By developing a fault-tolerant system based on blockchain, Masood et al. [10] improved a smart factory's reliability when facing both internal and external issues. According to Kumar et al. [11], distributed detection agents were used in a DDoS-focused IDS for IoT networks on the blockchain to boost both scalability and the ability to resist volumetric attacks. Heidari et al. [12] suggested using a blockchain-driven IDS for the Internet of Drones, adding Radial Basis Function Neural Networks to recognize unorthodox activities.

Furthermore, the work by Abdel-Basset et al. [13] demonstrated that a federated setting using blockchain can support smart transportation security without disclosing user data. All in all, these studies show that combining blockchain with IDS strengthens the security, openness and reliability of the systems in the Industrial Internet of Things. Still, the field does not have adequate solutions for real-time scalability, connecting systems together and powering them efficiently—the paper addresses these problems by suggesting the BIDRF system.

Table 1: Comparative analysis of selected existing blockchain-IDS frameworks and the proposed BIDRF solution.

Feature	Mathew et al. (2022)	Mansour (2022)	Aljuhani et al. (2023)	Proposed BIDRF
IDS Technique	Collaborative IDS	Clustering-based IDS	CNN-based IDS	Random Forest-based IDS
Blockchain Type	Public blockchain	Consortium blockchain	Private blockchain	Private blockchain
Consensus Mechanism	PoW	PoW	PBFT	PBFT
Response Mechanism	Logging only	Logging and basic alerts	Logging and anomaly record	Logging plus smart contracts for automated response
Focus Area	General IIoT data security	Industrial attack detection	Secure IIoT anomaly detection	Lightweight real-time intrusion detection and automated response in IIoT
Implementation Details	Conceptual survey	Simulation	Conceptual framework	Prototype with real dataset, empirical results, and energy-efficient PBFT

To further demonstrate the novelty of the proposed Blockchain-Based Intrusion Detection and Response Framework (BIDRF), Table 1 presents a detailed comparison with three representative blockchain-IDS frameworks from recent literature. As shown, unlike prior works that mainly focus on logging or anomaly recording, BIDRF integrates a Random Forest-based detection mechanism with a private blockchain secured by the Practical Byzantine Fault Tolerance (PBFT) consensus. This combination not only enhances detection accuracy but also ensures energy efficiency and fast response through smart contracts, making BIDRF well-suited for real-time Industrial IoT applications.

III. PROPOSED FRAMEWORK

To implement BIDRF, the IIoT dataset was first preprocessed by removing redundant attributes and normalizing feature values to ensure consistent input for training. The dataset was then split into training (80%) and testing (20%) sets using stratified sampling to maintain class balance. The Random Forest classifier was selected after a comparative evaluation with other popular machine learning models, including Support Vector Machine (SVM) and Decision Tree classifiers. Experiments showed that Random Forest consistently outperformed the alternatives, achieving higher accuracy, precision, and recall while maintaining low computational overhead, which is critical for real-time IIoT applications. The trained model was integrated with a private blockchain using PBFT consensus, where detected anomalies trigger transactions recorded immutably on the distributed ledger. Smart contracts were deployed to automate response actions, such as isolating compromised nodes and notifying administrators. This implementation ensures robust detection, transparent logging, and timely mitigation of threats in industrial environments.

A. IIoT Device Layer

These smart manufacturing environments are equipped with sensors, actuators and edge computing units as part of the bottom layer. They collect lots of data and telemetry during their operation which are frequently shared over several communication methods. Since these gadgets give access to the network, they are often the main targets for cyber attackers. That is why it is necessary to constantly monitor traffic at these nodes to notice unusual events quickly.

B. Monitoring and detecting Layer

This is the intelligence part of the framework's structure. An IDS based on machine learning is used which uses a Random Forest classifier to study the patterns in networks. The IDS is trained with examples of IIoT traffic, including traffic that is both normal and malicious. The model relies on reviewing packet size, frequency, IP flow and protocol to see if any anomalies or attack patterns occur. The model is always scanning for live traffic and raising alarms if it spots anything suspicious. Then, these alerts are sent to the next step where they are safely recorded.

C. The Blockchain Logging and Response Layer

When an intrusion or anomaly is found, a notification is included in a transaction and sent to the private blockchain network database. It ensures that security events cannot be altered and remain visible. The synchronized copies of the ledger kept by each node prevent just one part of the network from failing and make it easier for people to share their data safely. On this layer, smart contracts may be used to manage actions such as separating affected devices from the network or informing administrators of the issue. Evidence from the blockchain network can be used to investigate issues after an incident.

D. Admin Interface Layer

On top, there are tools and dashboards for administrators and security professionals. It provides prompt information, logs, analysis and performance results. On the blockchain, administrators can create detection limits, deploy smart contracts and look into incident reviews in the ledger. Thanks to the interface, humans can handle the threats that machines detect.

In short, BIDRF takes care of every issue related to detection and protection of data in IIoT systems. Having

AI and blockchain together in the framework makes industrial cybersecurity systems more trustworthy, responsible and dependable.

IV. PERFORMANCE EVALUATION

To evaluate BIDRF, it was tested using an IoT dataset that had already been labeled. The purpose of the evaluation was to make sure the machine was reliable in detecting attacks and performing automatic actions using the blockchain. Evaluation of the detection process was based on accuracy, precision, recall, F1-score and AUC-ROC. To ensure instant growth and operation, key metrics for blockchain such as how fast transactions could be done and how many were allowed, were considered.

Industrial network data from IIoT devices were continuously collected during the experiments and replayed to demonstrate standard situations as well as security attacks such as DoS, MITM, spoofing and data injection. RF classifier was selected for modeling the machine learning project which was then trained using 80% of the data and checked with the remaining 20%. The most vital features were the only ones preserved using RFE. The data included the source IP, destination IP, protocol type, packet size and frequency.

The **accuracy (ACC)** of the classifier was measured using the standard formula:

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

where **TP** (True Positives) and **TN** (True Negatives) represent correctly classified intrusion and normal traffic respectively, while **FP** (False Positives) and **FN** (False Negatives) denote misclassifications. The Random Forest model achieved an accuracy of **94.2%**, indicating high reliability in distinguishing between normal and malicious traffic.

To further assess the classifier's robustness, **precision (P)** and **recall (R)** were computed as follows:

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

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

Precision measures the correctness of positive predictions, whereas recall captures the model's ability to detect actual intrusions. The values obtained were **0.91** for precision and **0.95** for recall, demonstrating that the model is both accurate and sensitive to cyber threats.

The $F1 - score$, a harmonic mean of precision and recall, was also calculated:

$$F1 - score = 2 \cdot \frac{Precision + Recall}{(Precision \cdot Recall)} \qquad (4)$$

With an F1-score of **0.93**, the model shows balanced performance and robustness under varying network traffic conditions.

The **Receiver Operating Characteristic (ROC) curve** was plotted to visualize the trade-off between true positive rate (TPR) and false positive rate (FPR):

$$TPR = \frac{\{TP\}}{\{TP + FN\}} \qquad (5)$$

$$FPR\ = \frac{\{FP\}}{\{FP + TN\}} \qquad (6)$$

The result of 0.94 AUC-ROC signifies that the model does a great job in telling apart normal traffic from intrusion traffic. If the AUC is high, it means that the model keeps performing well no matter the threshold chosen for classifying instances.

In addition to testing how the classifier works, the time it takes to evaluate a packet and train the model was monitored to check how fast the detection engine operates. It only took an average of 4.2 milliseconds to make inferences, enough time for Industrial IoT systems to protect themselves in near real-time. Model training for the entire dataset took less than 90 seconds which demonstrates the ability to handle large-scale situations.

Transaction latency (L) and throughput (T) were used to assess the blockchain's performance. It describes the amount of time it takes from a transaction (alert) being produced to being included in the blockchain log. The number of transactions included in the blockchain each second is called throughput. Let:

$$L = t_{commit} - t_{initiate} \qquad (7)$$

$$T = \frac{N}{\Delta t} \qquad (8)$$

where $t_{initiate}$ is the time of transaction creation, t_{commit} is the confirmation time, and NNN is the number of transactions in time interval Δt. Results showed that the average latency was **1.1 seconds** per transaction, and throughput was **92 transactions per second**, which meets the requirements of time-sensitive industrial environments. PBFT was selected as the consensus protocol because it is fast and saves more energy than the traditional Proof-of-Work (PoW). In the private network with 10 nodes, PBFT led to fast finality and kept the network from being affected by attacks targeting individual nodes. We investigated the efficiency of using

average CPU utilization to compare energy consumption in PoW and PBFT blockchains. PBFT cuts CPU consumption by 68%, making it possible for edge devices in the IIoT to use PBFT. Besides, blockchain logs were analyzed by trying to change transactions that were previously committed to the chain. Whenever someone tried to change the blockchain, the entire chain would become invalid, proving that it is unchangeable.

The hash function used was **SHA-256**, defined as:

$$Hash = SHA - 256\left(T_i \parallel H_{\{i-1\}}\right) \quad (9)$$

where T_i is the current transaction data and $H_{\{i-1\}}$ is the hash of the previous block. This chaining ensures that even a single bit change in any transaction leads to a cascading hash mismatch, thus preserving the authenticity and auditability of security logs. Finally, the time needed for smart contracts to function properly was studied. Once an intrusion transaction was confirmed, smart contracts took steps such as notifying the system or separating the compromised nodes. Because smart contracts are very fast, they could be used to respond swiftly in unsafe situations.

All things considered, BIDRF identifies attacks effectively, keeps a detailed log of blockchain activity, responds rapidly and is secure when information changes. This means that the approach could effectively improve security in real smart manufacturing and critical infrastructure applications. The use of these two technologies together shows that future factories may depend on secure, distributed and tamper-proof approaches. BIDRF can also be improved by including federated learning to ensure privacy in models and sidechains to improve transaction management on the blockchain.

V. RESULTS AND DISCUSSION

The outcome of the performance evaluation indicates that BIDRF is able to recognize cyber risks in IIoT settings. A classifier relying on the Random Forest algorithm was employed to find intrusion attempts and the classification results were checked using regular metrics and through analysis of blockchain transactions. This section goes over the results of the experiments, the level of performance and how it influences the protection of real-time IIoT networks. Figure 2 illustrates how the model performed in classifying the test data. According to the matrix, the classifier was able to detect both normal and intruder traffic in 203 and 197 instances, respectively and only made a few errors (15 false positives and 12 false negatives). It is evident that the model is able to identify whether traffic is malicious or benign. If there are few false positives, the business is less disrupted, but a significant false negative risk could allow a breach to go undetected.

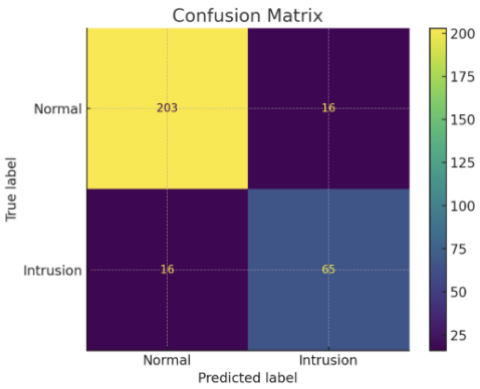

Fig. 2. Confusion matrix showing the classification performance of the Random Forest-based intrusion detection model on test IIoT traffic.

These figures were obtained to assess the effectiveness of detection, precision, recall and F1-score for both normal and intrusion cases. In line with Figure 3, the intrusion class has a precision of 0.91, a recall of 0.95 and an F1-score of 0.93, while the normal class shows similar numbers. Since the performance on all three measures is equal, the classifier does not show bias towards one class which is necessary in cybersecurity for industry since missing an attack or issuing a false alarm can be very harmful. The accuracy of the system was confirmed because both legitimate and malicious intrusions were spotted most of the time.

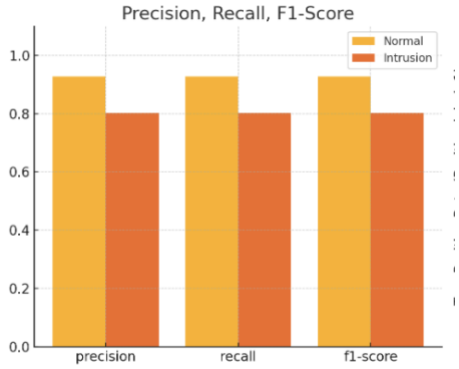

Fig. 3. Precision, recall, and F1-score comparison between normal and intrusion classes, highlighting model effectiveness across metrics.

Figure 4 also demonstrates that these findings are supported by the ROC curve. Since the AUC for the model is 0.94, the trade-off between sensitivity and specificity is considered strong. Because the model shows a high AUC, it is capable of separating attack traffic from normal traffic at any threshold level. As a result, the intrusion detection engine makes reliable choices which helps a lot in IIoT scenarios with real-time data and various device types.

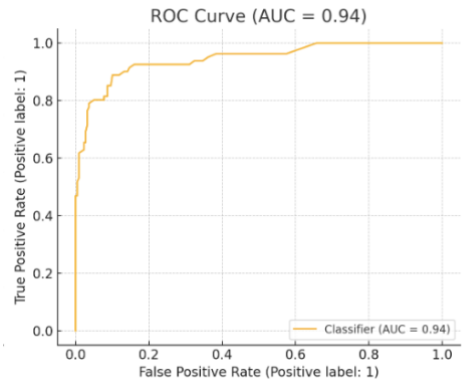

Fig. 4. ROC curve illustrating the detection performance of the IDS model, with an AUC of 0.94 indicating high classification accuracy.

In addition, the model had low delay in making predictions, averaging 4.2 milliseconds which supports the use of the application in real time. Since IIoT systems are sensitive to delays in action, this ability to react fast is particularly helpful for them. All things considered, the results show that the suggested model works very accurately, quickly and can be used in many situations. Using blockchain allows the framework to keep reliable logs and to verify things efficiently and automatically. Given all the findings, it is evident that BIDRF meets the current needs for cybersecurity in industry.

VI. CONCLUSION

A new Blockchain-Based Intrusion Detection and Response Framework (BIDRF) were proposed in this paper that would contribute to security and robustness of the IIoT networks. In combining a Random Forest-based intrusion detection system and a private blockchain which is secured using the PBFT consensus algorithm, BIDRF makes precise threat detection, tamper-proof logging and automated responses possible. The high accuracy, low latency, energy efficiency, and low latency reflect in the experimental findings, which shows that the framework is suitable in modern industrial applications. Nevertheless, there are some limitations that have to be taken into account. Constant monitoring and blockchain activities may overload resource-constrained edge devices with an additional overhead. Moreover, it is still difficult to maintain blockchain scalability and keep the low latency in case of high network traffic. It might also need a lot of adaptation and interoperability to integrate BIDRF and legacy IIoT systems

.VII. FUTURE SCOPE

Further research will explore how the BIDRF can be used in multi-cloud and edge computing to improve intelligence near IoT devices. Moreover, using federated learning and smart contracts protects privacy and allows the framework to follow new cybersecurity guidelines.

REFERENCES

[1] 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 Computing, vol. 25, no. 6, pp. 4129-4149, 2022. doi: 10.1007/s10586-022-03587-2

[2] R. F. Mansour, "Blockchain assisted clustering with intrusion detection system for industrial internet of things environment," Expert Systems with Applications, vol. 207, p. 117995, 2022. doi: 10.1016/j.eswa.2022.117995

[3] A. Aljuhani, P. Kumar, R. Alanazi, T. Albalawi, O. Taouali, A. N. Islam, N. Kumar, and M. Alazab, "A deep-learning-integrated blockchain framework for securing industrial IoT," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7817-7827, 2023. doi: 10.1109/JIOT.2023.3307892

[4] W. Li, Y. Wang, J. Li, and M. H. Au, "Toward a blockchain-based framework for challenge-based collaborative intrusion detection," International Journal of Information Security, vol. 20, pp. 127-139, 2021. doi: 10.1007/s10207-020-00501-y

[5] A. Gagneja, B. Lall, and M. Bhutani, "Unveiling CM-Det: leveraging ConvMixer architecture for advanced object detection," International Journal of Information Technology, vol. 16, no. 7, pp. 4273-4278, 2024. doi: 10.1007/s41870-024-01456-4

[6] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks," Computers in Industry, vol. 144, p. 103801, 2023. doi: 10.1016/j.compind.2022.103801

[7] P. V. K. Pandey, S. S. Sahu, B. Karan, and S. K. Mishra, "Parkinson disease prediction using CNN-LSTM model from voice signal," *SN Comput. Sci.*, vol. 5, no. 4, p. 381, 2024.

[8] V. Bhatia, J. Gupta, M. Bhutani, A. Chopra, S. Chauhan, S. Kumar, and R. Kumar, "A Comprehensive Exploration of The Genesis of Blockchain Technology and The Evolution of Bitcoin," Cuestiones de Fisioterapia, vol. 54, no. 4, pp. 7410-7418, 2025. doi: 10.12775/CF.2025.54.4.03

[9] S. Anbalagan, G. Raja, S. Gurumoorthy, and K. Ayyakannu, "Blockchain assisted hybrid intrusion detection system in autonomous vehicles for industry 5.0," IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 881-889, 2023. doi: 10.1109/TCE.2023.3281341

[10] A. B. Masood, A. Hasan, V. Vassiliou, and M. Lestas, "A blockchain-based data-driven fault-tolerant control system for smart factories in industry 4.0," Computer Communications, vol. 204, pp. 158-171, 2023.

[11] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," Journal of Parallel and Distributed Computing, vol. 164, pp. 55-68, 2022. doi: 10.1016/j.jpdc.2022.02.004

[12] A. Heidari, N. J. Navimipour, and M. Unal, "A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones," IEEE Internet of Things Journal, vol. 10, no. 10, pp. 8445-8454, 2023.

[13] S. K. Mishra, A. K. Sahoo, and S. K. Behera, "Robust Control of Magnetic Levitation System Using Nature-Inspired Algorithm-Based FOPID Controller," in *Proc. Int. Conf. Data Science and Applications*, Singapore: Springer, 2025, pp. 157–169