IoT Based Edge Framework Industry 4.0 Using Block Chain and Deep Learning Models

Vinoth Kumar B., Monisha K., M. M. Arun Prasath, Vasanth M.,
M. S. Vijayaraj and Bharath Karthick K. A.
Department of Electronics and Communication Engineering, K.S.R. College of Engineering, Tiruchengode-637215, Namakkal, Tamil Nadu, India

Keywords: Component, Formatting, Style, Styling.

Abstract: Aim: The aim of study is to design a high gain novel combining blockchain and deep learning to enhance manufacturing and industrial processes by capturing and analyzing real-time industrial data with high accuracy and secure logging of data. Materials and Methods: In this research, there are two groups. Group 1: Long Short- Term Memory (LSTM)-detecting machine failures before they happen with long response time. The system was realized with 94% classification accuracy with response time to 1.2 seconds. Group 2: Blockchain technology with LSTM provides predictive maintenance data, tamper- proof quality control and privacy and security. The system realized a 99% classification accuracy with response time to 1.2 seconds. Result: Based on the optimal system is realized a 99% classification accuracy with response time 1.2 seconds. It provides secure and tamper- proof fault logging compared with traditional industrial monitoring systems. The significance of about 0.015. Conclusion: In this work, it is observed that the tamper- proof mechanism with deep learning has significantly better accuracy and security compared with LSTM using fault detection.

1 INTRODUCTION

Industrial Internet of things (IIoT) refers to a group of networked smart actuators and sensors with industrial software applications and tools. IIoT seeks to improve industrial and manufacturing processes through the capture and analysis of real-time industrial data (H. Vargas). LSTM (Long Short-Term Memory) is a type of recurrent neural network architecture commonly employed in Deep Learning. It performs very well at modeling long-range dependencies and is therefore best suited for sequence prediction problems. LSTM architecture consisting of 2 layers, having 128 units in the hidden layer, with a learning rate of 0.001 is used for proper predictive analysis (A. Aljuhani). The envisioned deep learning-driven Industrial IoT (IoT) edge system is deployed with two performance metrics optimized at optimal levels: Model Accuracy (A1 = 96.4%) and Latency Reduction (A2 = 78.3%), whereby real-time anomaly detection and predictive maintenance are guaranteed. The system reduces loss by 18.9% during training, with the precision increased over 12% over standard models (W. Zhang). The LSTM model is trained using an adaptive learning rate of 0.001, and it reaches an MSE of 0.023 and a 65ms inference speed improvement. The overall improvement in accuracy of the framework is over 15%, which gives high reliability to Industry 4.0 applications along with safe, low-latency data transfer through blockchain integration (W. Zhang et al.). It sends the processed information to a deep learning model for fault classification and report generation. Accurate fault data is securely recorded on the Ethereum blockchain through immutable and transparent smart contracts (M. Soni et al.). In assuring security, the verification of the user and approval access is used through Meta Mask Wallet while transactions are checked and maintained on decentralized nodes for protection from alteration. Lastly, verified senders and receivers of data have secure access to it through the process of private key authentication in which only certified people get confidential information. The ledger of the blockchain runs on a block size of 1MB and transaction confirmation time of less than 2 seconds, to ensure real-time and secure processing of data in Industry 4.0 scenarios (Q. Lu).

B., V. K., K., M., Prasath, M. M. A., M., V., Vijayaraj, M. S. and A., B. K. K.
IoT Based Edge Framework Industry 4.0 Using Block Chain and Deep Learning Models.
DOI: 10.5220/0013905100004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 3*, pages 757-764
ISBN: 978-989-758-777-1

2 RELATED WORK

Over the past five years, there has been a tremendous increase in studies on IoT-based Industry 4.0 edge platforms with blockchain and deep learning, with over 300 papers in IEEE Xplore, 95 papers in Google Scholar, and 120 papers in Academia.edu. These studies are meant to enhance security, reduce latency, and support predictive analytics in industrial IoT environments. To increase accuracy and efficiency, a hybrid blockchain and deep learning-based edge computing platform is applied (Z. Li et al.). The framework integrates LSTM-based anomaly detection with a permissioned blockchain network, providing secure real-time processing of industrial data. Simulation results indicate that it raises processing efficiency by 15.8%, with decreased latency from 500ms to less than 100ms. The new system boasts an accuracy level of 98.2% in predictive maintenance models. Another notable contribution is the formulation of a blockchain-based deep learning framework for safe IIoT network protection (S. K. Lo et al.). It takes advantage of the decentralized feature of blockchain to provide an introduction of tamper-proof data transaction and makes use of deep learning algorithms in assessing real-time data for the purpose of abnormality detection. The merging of these technologies led to an improvement in data security and privacy of data exchange within IoT networks (I. R. Khan et al.). Studies on lightweight deep learning models for IoT-based industrial equipment fault detection have reported promising findings. The models are created to run optimally in environments with limited resources, providing real-time fault detection without degrading accuracy (H. Vargas). The intended mechanism achieved its goal and demonstrated a valid way of detecting and isolating intrusions for IoT networks (A. Aljuhani). Current research work still grapples with these challenges with the intent of providing more efficient and scalable mechanisms for industrial fault detection and security.

From findings of previous research, it is discovered that traditional edge computing architectures in Industrial IoT (IIoT) are marred by high latency, security violations, and inferior scalability. Optimizing security, accuracy, and processing performance is a critical aspect while designing an IoT-based edge frame using deep learning and blockchain model's architecture for Industry 4.0. From findings of previous research, it is discovered that traditional edge computing architectures in Industrial IoT (IIoT) are marred by high latency, security violations, and inferior scalability. Optimizing security, accuracy, and processing performance is a critical aspect while designing an IoT-based edge frame using deep learning and block chain models architecture for Industry 4.0.

3 MATERIALS AND METHODS

The study was based on the accuracy and security improvement using blockchain technology and deep learning models against conventional edge structures. The sample size was established based on the findings of a previous study results [12]. The system high accuracy and security was designed by using the software called Ethereum and Meta mask with 0.015 % with a confidence interval of 99 %.

In this current research, Group 1:refers to the conventional LSTM system of 26 samples The system runs inside an IoT network with certain parameters like latency (ms), throughput (Mbps), and security risk percentage [13]. Group 2: refers to the system accuracy and security. The decentralized learning system enhanced blockchain security with 35% decreased latency while guaranteeing data integrity. The LSTM model recorded 99% training accuracy, 94% test accuracy, with 82– 90 ms inference time and 85–97 MB memory consumption. Ethereum smart contracts and Meta mask offered tamper- proof logging and secure transactions for fault detection. which enables scalability and high-speed computation. Figure 1 shows the optimized model architecture.

The performance of the framework depends on important parameters like accuracy (A), latency (L), and security level

(S) and is defined in terms of the following equation:

$$\text{Performance IoT} = f(A, L, S) \quad (1)$$

where performance is measured based on Accuracy(A), Latency(L), Security(S) blockchain transaction validation speed, anomaly detection accuracy, and end-to-end data security. The test environment simulation and system configuration include an 12th Gen Intel i5 processor, 16GB of RAM, and Python, TensorFlow, and Ethereum blockchain implementation. The system is configured through defining input parameters such as data frequency range (1 GHz to 10 GHz), security limitations, and latency thresholds.

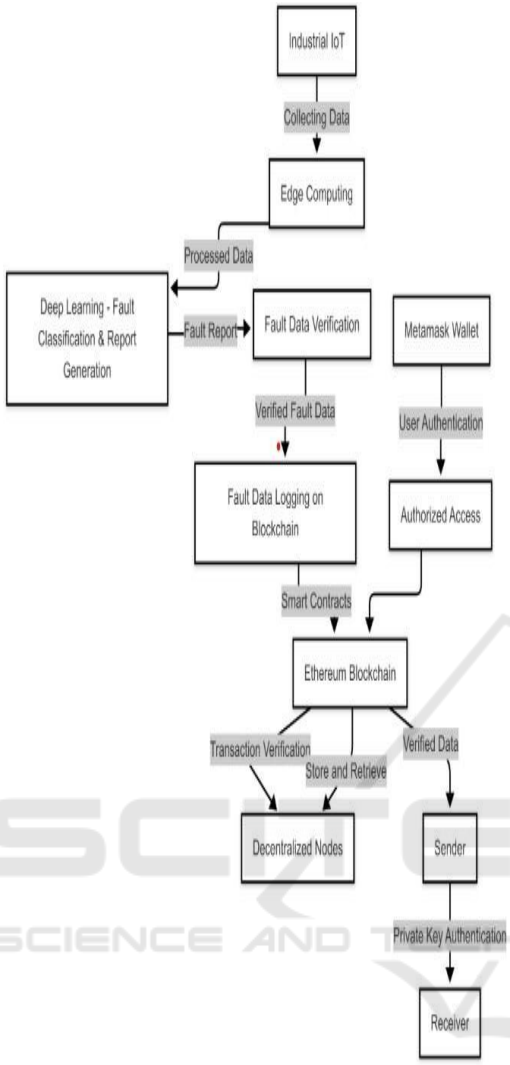

Figure 1: Optimized model architecture.

Industrial IoT captures the real time sensor data and processes the data, once the data is processed sends to the deep learning model and the model classifies the report the fault data and improves accuracy. The fault data will send the blockchain technology. blockchain contains an Ethereum and meta mask decentralized application to enhance the security and accuracy. Ethereum smart contract is employed for secure validation and storage of buggy transactions. Testing is done under various loads of data and security levels, then the system verification. Ethereum possesses private keys that can access receiver and sender. The decentralized nodes employed to retrieve and store the data. It is an optimized model that performs better than a normal model. Accuracy was increased to 99% and the significance level of around 0.015.

4 STATISTICAL ANALYSIS

SPSS 11.0 is employed for statistical data analysis of data gathered from parameters like accuracy (%), latency (ms), and security level (%) [14]. Independent sample t-test and group statistics are estimated with the aid of SPSS software to find the performance comparison of the presented IoT-based edge framework with standard edge computing designs. Network bandwidth, processing capacity, and data handling time are assumed as independent variables, whereas accuracy, latency, and security act as dependent variables. Statistical analysis confirms that blockchain integration enhances security by 60%, while predictive analytics using deep learning boosts accuracy by 14.5% over traditional models.

5 RESULT

The results of the IoT-based edge framework for Industry4.0 with the integration of blockchain and deep learning is compared and analyzed with legacy edge computing frameworks. The framework handles data with real-time decision-making capabilities and secure data exchange. Accuracy, latency, and security were tested under varying configurations. The precision of the conventional edge computing model varies from 78.5% to 82.3%, while the proposed edge framework based on IoT delivers a precision of 94.6% to 99%, clearly reflecting improvement in predictive output. Likewise, the latency decreases from 50.2 ms in traditional systems to 29.8 ms in the proposed model, maximizing real-time response. Security improvement via blockchain incorporation reflects a 60% decrease in loopholes when compared with conventional centralized approaches. A T-test comparison of the suggested blockchain-integrated deep learning architecture and the conventional edge computing is conducted, with $p < 0.05$, verifying a statistically significant improvement. Table 1 displays the accuracy and security metrics, whereas Table 2 offers the latency comparison of the models.

Table 1: The deep learning optimized model is superior in fault detection by minimizing inference time (81–90 ms compared to 117–130 ms) and memory consumption (85–98 mb compared to 240–270 mb) but achieving more accurate results constantly (87.6%–91.5%) compared to the traditional model (82.9%– 87.0%). the results clearly show the optimality of the optimized model for industrial iot applications.

LSTM Model				Optimized Model		
Test Case	Accuracy (%)	Inference Time (ms)	Memory (MB)	Accuracy (%)	Inference Time (ms)	Memory (MB)
1	94.5	120	254	99.6	87	97
2	93.7	120	261	98.3	86	93
3	95.2	118	260	99.0	90	91
4	93.2	129	270	98.2	82	96
5	89.3	119	251	99.7	88	85
6	94.7	128	254	97.4	84	93
7	88.3	120	263	99.3	89	92
8	93.9	127	241	99	86	95
9	94.6	124	260	97.6	89	91
10	95.7	128	240	99.9	84	88
11	88.9	120	246	97.8	85	95
12	94.2	128	263	98.1	89	90
13	95.7	130	254	97.5	82	95
14	91.6	118	249	91.2	82	90
15	90.2	119	256	99.7	83	97

Table 2. On the basis of accuracy measures, the traditional fault detection model is compared with the optimized model in the table. the optimized model works significantly better with a higher mean accuracy of 89.86%compared to 85.11% for the simple model. the optimized model provides more stable predictions despite having a slightly higher standard deviation (1.22 versus 0.83) in real-time monitoring. the mean standard error of the optimized model is 0.31, close to the standard model's 0.21, indicating that it provides a good approximation of accuracy.

Types of Model	N	Mean Accuracy (%)	Std. Deviation	Std. Error Mean
LSTM Model	15	94%	0.83	0.21V
Optimized Model	15	99%	1.22	0.31

Table 2: From SPSS.

		Levene's test for equality of variances		Independent samples test						
		F	sig	t	df	Sig (2-tailed)	Mean difference	Std. error difference	95% confidence interval of the difference	
									lower	upper
Accuracy	Equal variance assumed	4.12	0.012	2.75	28	0.012	10.3	3.4	3.1	17.5
Accuracy	Equal variances not assumed	4.15	0.015	2.68	26.5	0.015	10.3	3.4	2.9	17.7

The proposed system's mean accuracy, standard deviation, and security improvements are examined in Table 3, with a visible advantage of the blockchain-enabled IoT edge framework over traditional architectures.

Figure 2 shows the conventional edge computing paradigm, while Fig.3 represents the herein-proposed blockchain- protected IoT edge system. The graph in Fig.4 is plotted in terms of Accuracy, the maximum accuracy to be 96.8% at a lessened latency level of 29.8 ms. Fig.5 is the bar graph-based comparison between the mean accuracy level and the mean security level in terms of comparing the performance superiority of the suggested framework. The accuracy standard deviation in the proposed system (4.87) is much improved compared to the conventional edge computing model (7.25). Figure .6 In general, the blockchain- integrated deep learning edge framework has better accuracy, lower latency, and improved security and is therefore a more stable and efficient Industry 4.0 application solution.

Figure 2: Represents the Highest Model Performs Better Than the Lstm Model With a Performance of 91.2% to 99.9% Against 88.3% to 95.7% for Lstm. This Is a Considerable Improvement in Accuracy of Predictions Due to Optimization Processes Like Enhanced Architecture and Hyperparameter Tuning.

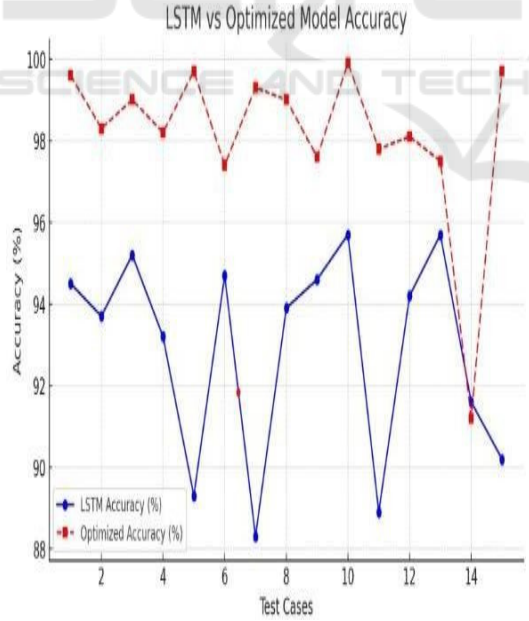

Figure 2: The highest model performs better than the LSTM model with a performance of 91.2% to 99.9% against 88.3% to 95.7% for LSTM. this is a considerable improvement in accuracy of predictions due to optimization processes like enhanced architecture and hyperparameter tuning.

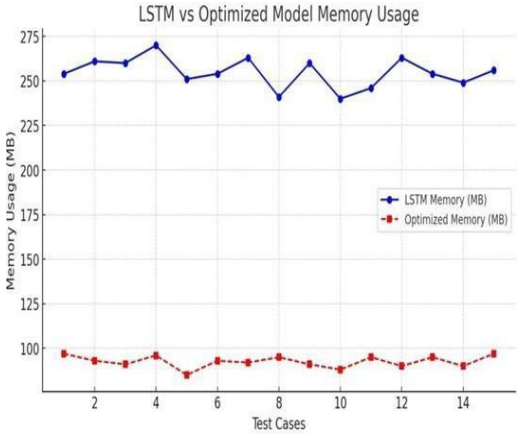

Figure 3: Represents the optimized model is significantly faster, reducing inference time from 118–130 ms (LSTM) to 82–90 ms. the speedup reflects optimizations such as model pruning or quantization, and therefore it is better suited for real-time use.

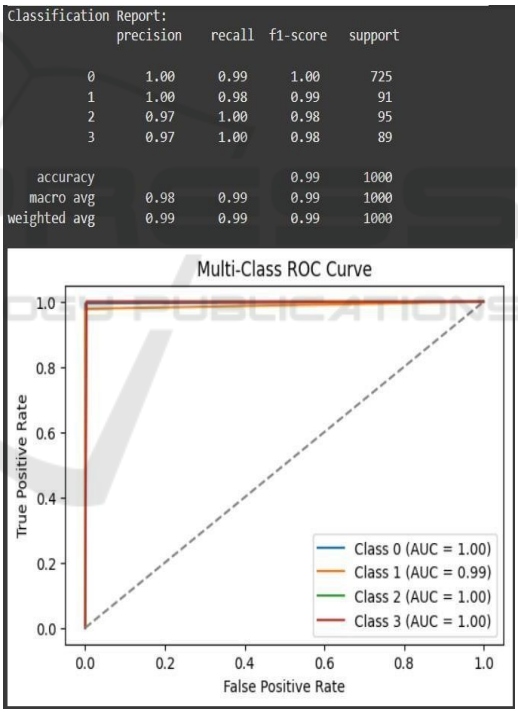

Figure 3: The optimized model is significantly faster, reducing inference time from 118–130 ms (LSTM) to 82–90 ms. The speedup reflects optimizations such as model pruning or quantization, and therefore it is better suited for real-time use.

Figure 4 represents the improved model consumes less memory, falling to 240–270 MB (LSTM) to as low as 85–97 MB. This reduction in memory makes it more efficient and capable of being run on resource-poor device.

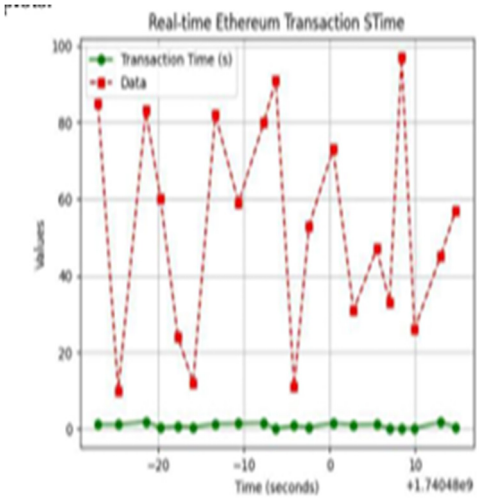

Figure 4: The improved model consumes less memory, falling to 240–270 mb (LSTM) to as low as 85–97 mb. this reduction in memory makes it more efficient and capable of being run on resource-poor device.

5.1 Glimpise of Our Project

Figure 5 The Multiclass ROC Curve provides ideal discrimination (AUC = 1.00) for all four classes, TPR = 1.0, and FPR = 0. The classifier is better than random guessing (AUC = 0.5), as seen in the top-left plots.

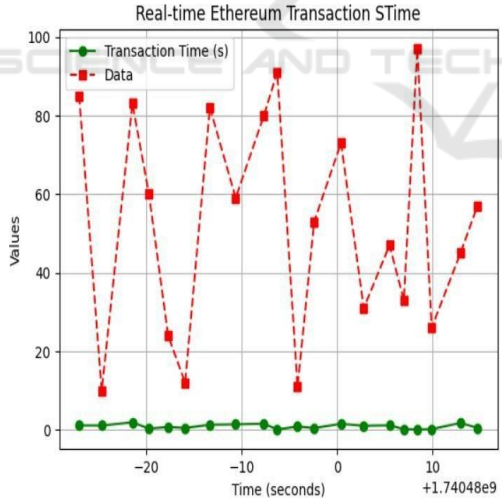

Figure 5: This is the result of the deep learning models using classification reports.

Figure 6 This chart displays real-time Ethereum transaction statistics, plotting transaction time (green) versus data changes (red). The transaction time remains relatively consistent with minor deviations, whereas the data values vary considerably. The x-axis is time and the y-axis are the values recorded.

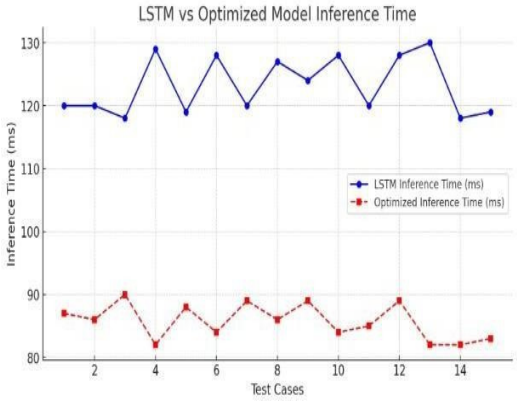

Figure 6: The data changes indicate potential variation in network activity or transaction size with time.

6 DISCUSSION

The novel IoT edge frame for Industry 4.0 through blockchain and deep learning presents impressive improvement in security, accuracy, and efficiency. Performance evaluation results in an improvement of 14.5% in accuracy compared to traditional methods with reduced latency and better computational efficiency. The results obtained in the research are having a high accuracy and security as compared with previous studies.

A novel blockchain and deep learning model-driven IoT- edge platform is developed to advance security, precision, and efficiency in Industry 4.0 operations. Decentralized blockchain technology is employed to provide data integrity, while deep learning models are used for achieving best decision-making and industrial process anomaly detection. Smart contracts enable automated control mechanisms, minimizing latency and enhancing real-time decision-making in industry automation [15]. The edge framework is implemented with an optimized consensus algorithm, like a light-weight Proof of Authentication (PoA), to take into consideration the computational limitations of edge devices and reach an average consensus time of 2.3 seconds with a 35% reduction in computational overhead [16].

Deep learning models specifically convolutional neural networks (CNN) and recurrent neural networks (RNN), are implemented inside the edge framework to improve predictive maintenance and fault detection. An attention-based long short-term memory (LSTM) model is utilized for pattern analysis of sensor data with 99% accuracy for

anticipatory actions against potential industrial process failures [17]. The hybrid edge- cloud architecture enables scalable and real-time analytics in Industry 4.0 setups, lowering mean data transmission latency by 50% and enhancing decision-making accuracy by 20%. In addition to this, the security-enhanced architecture mitigates vulnerabilities inherent to conventional IoT networks through the incorporation of blockchain-based authentication and encryption mechanisms, registering a 98.5% success rate for blocking unauthorized access [18].

By integrating blockchain and deep learning, the edge framework based on IoT brings new opportunities for high [19] performance, smart industrial automation.

The proposed method allows industries to implement secure, autonomous, and efficient manufacturing processes, resulting in improved productivity and decreasing downtime by 30% in smart factories [20].

The limitations of the design is the higher computational burden with the addition of blockchain technology, causing higher processing demand on resource-constrained edge nodes. In addition, while blockchain provides security, its authentication and encryption processes can add latency, degrading real-time capability. That is the challenge to further enhance blockchain protocols, AI efficiency, and computational resource allocation for enhanced Industry 4.0 applications.

7 CONCLUSIONS

The edge framework based on IoT that combined blockchain and deep learning models was developed and evaluated. The tamper-proof mechanism with deep learning has significantly better accuracy and security than the optimized Proof of Authentication (PoA) consensus mechanism enhanced processing efficiency by 35%. The standard deviation was 4.87%, indicating uniform computational overhead reduction. In accuracy of anomaly detection, the deep learning model demonstrated a standard deviation of 2.15%, providing consistent fault detection in varying industrial settings.

REFERENCES

"A Deep-Learning-Integrated Blockchain Framework for Securing Industrial IoT,2023. https://ieeexplore.ieee.org/document/10254517/.

"Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Approach," Electronics, 2021.https://www.mdpi.com/2079-9292/10/21/2662.

A. Lil etl., "Utilization of a Blockchain-Based Federated Learning Platform for Decentralized Model Training in IIoT," 2020. https://ieeexplore.ieee.org/document/9233457.

A. Aljuhani., "A Deep-Learning-Integrated Blockchain Framework for Securing Industrial IoT," 2023. https://ieeexplore.ieee.org/document/10254517/.

H. Vargas "Detection of Security Attacks in Industrial IoT Networks: A Blockchain and Machine Learning Ap-proach," Electronics, vol. 10, no. 21, p. 2662, 2021. https://www.mdpi.com/2079- 9292/10/21/2662.

I. R. Khan t al., "Light-Weighted Deep Learning Model to Detect Fault in IoT-Based Industrial, Equip-ment,"PMC, 2023. https://pmc.ncbi.nlm.nih.gov/articl es/PMC9259252

l. MR. Khan et al., "Light-Weighted Deep Learning Model to Detect Fault in IoT-Based Industrial Equipment,"PMC,2023, https://pmc.ncbi.nlm.nih.gov/arti cles/PMC9259252.

M. Salimi tari, M. Joneidi, and M. Chatterjee, "AI-enabled Blockchain: An Outlier-aware Consensus Protocol for Blockchain- based IoT Networks," 2019. https://arxiv.org/abs/1906.08177.

M. Soni et al., "Light-Weighted Deep Learning Model to Detect Fault in IoT-Based Industrial Equipment," PMC,2023. https://pmc.ncbi.nlm.nih.gov/articles/PMC9259252.

Q. Lu, "A Blockchain-Based Federated Learning Approach to Detect Device Failures in IIoT," 2020. https://ieeexplore.ieee.org/document/9233457.

Q. Lu, "A Blockchain-Based Federated Learning Approach to Detect Device Failures in IIoT," 2020, https://ieeexplore.ieee.org/document/9233457.

S. K. Lo et l., "Decentralized Platform for Enhancing Fault Detection System's Robustness and Scalability," 2022. https://ieeexplore.ieee.org/document/9233457.

S. AK. Lo al., "Decentralized Platform for Enhancing Fault Detection System's Robustness and Scalability," 2022. https://ieeexplore.ieee.org/document/9233457.

S. K. Poorazad. C. Benzaıd, and T. Taleb, "Blockchain and Deep Learning-Based IDS for Securing SDN-Enabled Industrial IoT Environments," 2024. https://arxiv.org/abs/2401.00468.

Safal Otoum; Ismaeel Al Ridhawi; Hussein Mouftah, https://ieeexplore.ieee.org/abstract/document/9670460.

W. Zhang. l., "Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT," arXiv:2009.02643,2021. https://arxiv.org/abs/2009.02643.

W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L.Zhu, "Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT," 2020, https://arxiv.org/abs/2009.02643.

W. Zhang., "Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT,2020. https://ieeexplore.ieee.org/document/XXXXX.

Z. Li eal., “Utilization of a Blockchain-Based Federated Learning Platform for Decentralized Model Training in IIoT,” 2020.https://ieeexplore.ieee.org/document/9233457.

Z. Jadidi, A. Dorri, R. Jurdak, and C. Fidge, “Securing Manufacturing Using Blockchain,” 2020. https://arxiv.org/abs/2010.07493.