Volume 11, Issue 6, June – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

Blockchain-Driven Federated Learning for Secure Industrial Predictive Maintenance

Md Hossain[1]; Nakul Bakchi[2]; Md Imran Hossain[2]; Suman Das[2]; Md Faysal Ahmed[3]

[1]Dept. of Manufacturing Systems Engineering & Management, California State University Northridge, CA, USA
[2]Dept. of Industrial and Systems Engineering, Lamar University, TX, USA
[3] Shaikh Borhanuddin Postgraduate College, Affiliated by National University, Dhaka-1100, Bangladesh

Publication Date: 2026/07/04

Abstract: Factories with similar machines could build better failure-prediction models by sharing data, but most do not want to share their raw records with competitors or a central server. Federated learning (FL) solves this problem by allowing each factory to keep its data locally while training a shared model. However, FL still depends on a central server and does not clearly track contributions. This paper shows a framework that combines FL with a lightweight permissioned ledger. Each factory trains a local model, signs its update, and stores only a hash of the update on the ledger. This provides data integrity, an audit trail, and controlled participation. Using the AI4I 2020 predictive-maintenance dataset across five simulated factories, the framework achieved a ROC-AUC of 0.949, close to the centralized model's 0.974 and much better than a single factory's 0.790. The ledger added only about 6% extra training time and required very little storage. This helps identify and remove malicious participants, making industrial data sharing more secure and trustworthy.

Keywords: *Federated Learning, Blockchain, Predictive Maintenance, Industry 4.0, Industrial AI, Machine Learning Security.*

How to Cite: Md Hossain; Nakul Bakchi; Md Imran Hossain; Suman Das; Md Faysal Ahmed (2026) Blockchain-Driven Federated Learning for Secure Industrial Predictive Maintenance. *International Journal of Innovative Science and Research Technology*, 11(6), 2442-2448. https://doi.org/10.38124/ijisrt/26jun1585

I. INTRODUCTION

Modern factories collect a lot of machine data, such as temperature, torque, rotational speed, and tool wear. This data can be used for predictive maintenance, where a model warns operators before a machine fails. However, a single factory often does not have enough failure examples to train an accurate model because failures are rare. Combining data from multiple factories could improve model performance, but companies are usually unwilling to share raw machine data because it may reveal sensitive information such as production levels and operating processes. The growth of Industry 4.0 has increased the amount of available industrial data and highlighted the need for efficient and sustainable operations [53]. Machine learning is already widely used for fault detection, hazard monitoring, and predictive maintenance in smart manufacturing environments [55-60]. However, the effectiveness of these systems depends on reliable data and trustworthy decision-making processes [54], [61], [62].

Federated learning (FL) helps address this challenge [1]. Instead of sending data to a central server, FL sends the model to each participant. Each factory trains the model using its local data and sends only model updates back to a server, which combines them into a shared model [1], [5]. This approach keeps raw data private and has been applied in many industrial applications [13], [33], [35]. However, FL still has two important limitations. First, it relies on a central server to aggregate updates correctly, creating a single point of failure [6], [66]. Second, FL does not provide a secure record of which participant submitted each update, which can be a concern when organizations do not fully trust one another.

Blockchain technology can help solve these problems, and many studies have combined blockchain with federated learning [8], [12], [18]. A blockchain ledger can provide a tamper-resistant record of updates, control who is allowed to participate, and reduce reliance on a trusted central authority. However, many existing solutions are complex because they use expensive consensus mechanisms, store large amounts of data on-chain, or rely on custom datasets that are difficult to reproduce [9], [15], [16]. On the other hand, many federated predictive-maintenance studies do not use any ledger technology and therefore lack auditability and integrity guarantees [32], [50]. As a result, there is limited understanding

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

of the actual benefits and costs of adding a ledger to federated learning.

This paper aims to provide a practical middle-ground solution. We combine standard federated averaging with a lightweight permissioned ledger and evaluate the framework using a publicly available benchmark dataset. The ledger does not store raw data or model weights. Instead, it stores only a signed hash of each model update, providing integrity, auditability, and access control with minimal overhead.

The main contributions are 3-fold. First, we present a simple and reproducible framework that integrates federated predictive maintenance with a lightweight permissioned ledger and clearly explains what information is recorded and why. Second, we evaluate the framework using the AI4I 2020 dataset [51], comparing centralized learning, local-only learning, and federated learning under both balanced and skewed data distributions while measuring the additional ledger overhead. Third, we investigate security aspects by showing how the ledger can detect tampering and prevent unauthorized participation. We also analyze the impact of a malicious factory on model performance and demonstrate how simple defense mechanisms can restore the accuracy of the shared model.

II. RELATED WORK

A. Federated Learning and its Challenges

Federated learning began with federated averaging, which trains a shared model by averaging locally computed updates and cuts communication rounds sharply compared with synchronized training [1]. Later work reduced communication further through compressed updates [2] and dealt with the fact that real clients differ in data and compute. FedProx adds a term that keeps each local model close to the global one and stabilizes training when clients are uneven [3]. SCAFFOLD corrects the drift between clients caused by skewed data [4]. Broad surveys set out the main obstacles of cost, heterogeneity, and privacy [5], catalog open problems [6], and give a systems view of how federated frameworks are built [7]. A common thread is that the central server is trusted, and integrity or audit of the updates is left out of scope.

B. Blockchain-Enabled Federated Learning

A large body of work replaces or supports the central server with a blockchain. BlockFL exchanges and verifies updates through a ledger and studies the effect of block timing on delay [16]. A committee-consensus design stores the model and updates on chain while resisting bad updates at lower cost [15]. Other studies push on scaling decentralized aggregation at the edge [19], on aggregation rules that stay fair and robust when some participants misbehave [21], and on reputation with privacy protection to reward honest behavior [47]. Federated anomaly detection has even been used to hunt threats inside blockchain-based industrial networks [11]. Several surveys map this area, covering the security that blockchain adds to federated learning [17], taxonomies of consensus and aggregation [18], [20], and security reviews across the internet of things [12], [42]. More focused reviews look at aggregation techniques for industrial IoT [43], intrusion detection at the industrial edge [44], open challenges such as poisoning and incentives [45], and integration in mobile settings such as unmanned aerial vehicles [46]. The recurring issue is weight. These systems often assume full consensus, on-chain storage of large updates, or generic benchmarks, which makes them hard to reproduce and to adopt as a simple baseline.

C. Security, Privacy, and Integrity of Updates

Secure aggregation lets a server sum client update without seeing any single one [37]. Differentially private training bounds what an update can leak [38], and recent analysis shows clients can take several local steps and still gain from secure aggregation under a privacy budget [41]. A survey of poisoning attacks lays out the threat model that any open system must face [36]. On the blockchain side, schemes add differential privacy and encryption to on-chain aggregation [10], survey how such systems handle privacy [40], and add traceable, tamper-proof storage of parameters [39]. These methods give strong guarantees, but at a level of compute and complexity beyond a small ledger whose only job is to protect the integrity and provenance of update hashes.

D. Secure Industrial Data Sharing and Predictive Maintenance

The application layer ties these ideas to industry. One-line fuses federated learning with blockchain for industrial data sharing and diagnosis. These works build federated training into the consensus step [8], record updates so they cannot be altered [9], run decentralized transfer learning and domain generalization for machinery faults [28], [29], detect device failures across plants on a shared chain [30], secure fault diagnosis on skewed data [31], select trusted nodes by reputation [22], and hold accuracy on non-IID factory data [23]. A second line uses blockchain on its own for access control and accountability, through fair data exchange [24], lightweight sharing for constrained devices [25], attribute-based encryption [26], token-based authorization [27], trusted data spaces for siloed partners [14], and transparency, security, and efficiency for supply-chain management [56], [65]. A third line applies federated learning to the maintenance pipeline without any ledger, covering remaining-useful-life prediction [32], mixed fault diagnosis [33], transfer learning with prior alignment [34], time-series-aware predictive maintenance [35], and explainable maintenance for Industry 4.0 [50], [64]. The same privacy idea reaches cross-organization settings such as credit records [48] and supply-chain graphs [49]. The ledger-free maintenance works leave out integrity and provenance, while the blockchain works tend to be heavy and tied to private data. Our work sits between them, with plain federated averaging, a small ledger, and a public dataset.

III. PROPOSED METHODOLOGY

A. Scenario and Threat Model

We consider a set of factories that each run similar machines and want a shared model that predicts machine failure. No factory will share raw sensor logs, because those logs expose production and process details. A coordinating server runs the training rounds, but the factories do not fully trust it or each other. We assume most factories are honest while some may be faulty or malicious and may send bad updates. We also assume that anyone with access to the stored

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

updates might try to alter the record after the fact. The goals are to train a useful shared model, to keep raw data local, to make the record of contributions tamper-evident and auditable, and to control who is allowed to join.

B. Framework

Figure 1 shows the design. A round begins when the server pushes the current global model to the factories. A factory then trains on its private data for a few local epochs, hashes the resulting update, signs the hash with its private key, and sends both to the server. The server checks the signature against that factory public key, appends a block carrying the update hash to the ledger, and averages the updates into a new global model. Raw data never leaves a factory. Only model updates are shared, and only their hashes go on the chain.

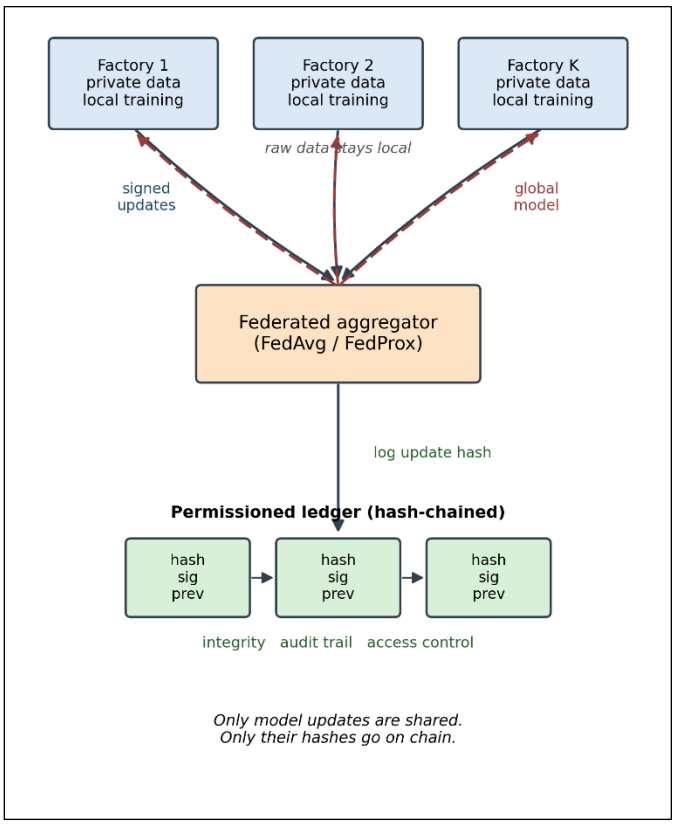

Fig. 1. System Architecture.

C. Federated Training

We use federated averaging as the base method [1]. With K factories, where factory k holds n_k samples and n is the total, the server forms the new global weights as

$$w(t+1) = \sum_k (n_k / n)\, w_k(t+1) \quad (1)$$

where w_k(t+1) is the model returned by factory k. Because failures are rare, each factory trains with a class-weighted loss so the minority failure class is not ignored.

We also test FedProx, which is built for uneven data [3]. Each factory minimizes its local loss F_k plus a term that holds the local model near the global one,

$$\text{minimize } F_k(w) + (\mu / 2) \| w - w(t) \|^2 \quad (2)$$

where mu controls how strongly the local model is pulled back. We use a small mu so the effect is gentle.

D. Lightweight Permissioned Ledger

The ledger is a hash-chained list of blocks. Every authorized factory holds an elliptic-curve key pair, and its public key is placed in a registry when it joins. For an update U, the factory computes a SHA-256 hash H(U) and signs it. The server then forms a block that links to the previous block,

$$\text{block hash} = H(\text{index, time, round, id, } H(U), \text{signature, prev hash}) \quad (3)$$

The ledger gives three guarantees. The chain provides integrity, since changing any recorded update breaks the hash links and is caught during validation. For auditability, each block stores the factory id, round, and signature, which together form a complete and non-repudiable trail of contributions. Access control falls out of the registry, because a submission from an unknown key or a bad signature is rejected before any block is added. Since the ledger holds hashes rather than data or weights, it stays small.

E. Defenses Against Malicious Factories

The ledger makes updates tamper-evident and traceable, but it does not by itself stop a factory from sending a harmful update. We pair it with two simple defenses. The first is a robust aggregation rule, the coordinate-wise trimmed mean, which drops the highest and lowest values for each parameter before averaging and so limits the effect of extreme updates. The second uses the ledger directly. Because every update is signed and attributed, a factory whose contributions are linked to a sharp drop in validation performance can be identified and excluded, after which the honest factories aggregate among themselves.

IV. RESULTS

A. Dataset and Preprocessing

We use the AI4I 2020 predictive-maintenance dataset [51], containing 10,000 records with a 3.39% failure rate. Features include product type, temperatures, rotational speed, torque, and tool wear. Two derived features are added: temperature difference and mechanical power. Failure-mode indicators are removed to prevent label leakage. After preprocessing, each record has 10 features. The data is split into 80% training and 20% testing, and features are standardized using training-set statistics.

B. Federated Setup

We simulate five factories. In the balanced (IID) setting, data is evenly distributed among factories. In the skewed (non-IID) setting, failure cases are unevenly distributed, creating failure rates from 0.3% to 12.6%. A small two-hidden-layer MLP is trained for 60 federated rounds, and all methods are evaluated on the same test set.

Table 1. Per-Factory Training Data Under the Two Splits.

Split	Factory	Records	Failures	Rate
IID	1	1600	51	0.032
IID	2	1600	57	0.036
IID	3	1600	62	0.039
IID	4	1600	47	0.029

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

IID	5	1600	54	0.034
non-IID	1	1551	5	0.003
non-IID	2	1769	223	0.126
non-IID	3	1552	6	0.004
non-IID	4	1556	10	0.006
non-IID	5	1572	27	0.017

C. Predictive Performance

Table 2 compares all methods on the test set. Because failures are rare, we treat ROC-AUC as the main measure, since it does not depend on a single decision threshold, and we also report precision, recall, and F1 at the default threshold. Methods marked with a star are centralized and need all raw data pooled in one place.

Table 2. Predictive Performance on the Global Test Set. A Star Marks Centralized Methods that Require Pooled Raw Data.

Method	Acc	Precision	Recall	F1	AUC
Centralized MLP*	0.928	0.302	0.853	0.446	0.974
Random Forest*	0.988	0.940	0.691	0.797	0.964
Logistic Reg.*	0.859	0.178	0.868	0.295	0.934
Local best	0.923	0.271	0.750	0.398	0.905
Local mean	0.923	0.320	0.406	0.217	0.790
FedAvg IID	0.915	0.262	0.824	0.397	0.949
FedProx IID	0.918	0.268	0.824	0.404	0.950
FedAvg n-IID	0.948	0.304	0.412	0.350	0.888
FedProx n-IID	0.946	0.289	0.412	0.339	0.886

D. Effect of Heterogeneity and Scale

Figure 2 reports two sweeps. In the first, we vary the Dirichlet parameter that controls skew. Performance falls smoothly as the data becomes more skewed, with the AUC dropping from 0.949 at near-balanced data to 0.807 at strong skew. FedAvg and FedProx stay close across the whole sweep, and neither holds a consistent edge, with every gap under 0.01 AUC and within the range of run-to-run noise. In the second sweep, we vary the number of factories from three to ten at a fixed level of skew. The AUC stays stable near 0.88, while F1 dips a little as each factory holds less data. The framework does not collapse as more factories join, which matters for real deployments.

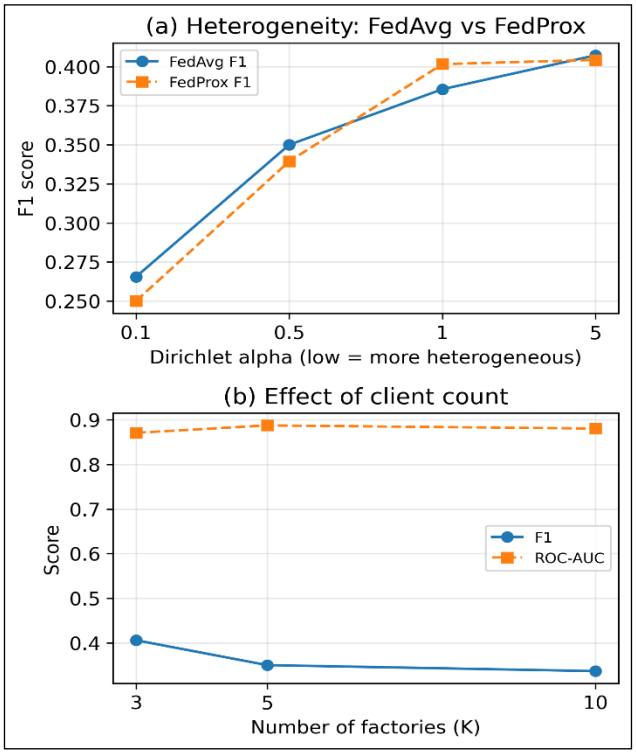

Fig. 2. Effect of Data Heterogeneity (Dirichlet Alpha) and of the Number of Factories.

E. Ledger Overhead

We measured the ledger cost during a full run that logged 300 updates, one per factory per round. Hashing an update took about 0.007 milliseconds, signing took about 0.40 milliseconds, and verifying a signature took about 1.40 milliseconds. Together the ledger work came to 0.54 seconds, about 5.9 percent of the 9.11 seconds of training in this single-process setup. The full chain of 300 blocks used about 103 kilobytes, or roughly 0.34 kilobytes per block, because only hashes and signatures are stored. The cost is small.

V. CONCLUSION

We presented a simple framework that joins federated learning with a lightweight permissioned ledger for secure predictive maintenance across factories. The ledger records only signed hashes of model updates, which gives integrity, auditability, and access control without storing data or weights. On the public AI4I 2020 dataset, federated learning reached an AUC of 0.949 on balanced data, close to a centralized model and well above any single factory trained alone, while the ledger added about 6 percent to training time and only kilobytes of storage. Security tests confirmed that tampering and unauthorized access are caught, and a poisoning study showed that one malicious factory can break plain averaging while a robust aggregation rule and ledger-based exclusion both recover the model.

REFERENCES

[1]. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Aguera y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. 20th Int. Conf. Artificial Intelligence and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

Statistics (AISTATS), PMLR vol. 54, 2017, pp. 1273-1282.
[2]. J. Konecny, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," in NIPS Workshop on Private Multi-Party Machine Learning, arXiv:1610.05492, 2016.
[3]. T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated Optimization in Heterogeneous Networks," in Proc. Machine Learning and Systems 2 (MLSys), 2020.
[4]. S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "SCAFFOLD: Stochastic Controlled Averaging for Federated Learning," in Proc. 37th Int. Conf. Machine Learning (ICML), PMLR vol. 119, 2020, pp. 5132-5143.
[5]. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50-60, 2020.
[6]. P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, vol. 14, no. 1-2, pp. 1-210, 2021.
[7]. Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," IEEE Trans. Knowledge and Data Engineering, vol. 35, no. 4, pp. 3347-3366, 2023.
[8]. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," IEEE Trans. Industrial Informatics, vol. 16, no. 6, pp. 4177-4186, 2020.
[9]. G. Xu, Z. Zhou, J. Dong, L. Zhang, and X. Song, "A Blockchain-Based Federated Learning Scheme for Data Sharing in Industrial Internet of Things," IEEE Internet of Things Journal, 2023.
[10]. B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT," IEEE Trans. Industrial Informatics, 2022.
[11]. A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block Hunter: Federated Learning for Cyber Threat Hunting in Blockchain-Based IIoT Networks," IEEE Trans. Industrial Informatics, 2022.
[12]. Y. Jiang, B. Ma, X. Wang, G. Yu, P. Yu, Z. Wang, W. Ni, and R. P. Liu, "Blockchained Federated Learning for Internet of Things: A Comprehensive Survey," ACM Computing Surveys, vol. 56, no. 10, art. 258, 2024.
[13]. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated Learning for Industrial Internet of Things in Future Industries," IEEE Wireless Communications, 2021.
[14]. B. Farahani and A. K. Monsefi, "Smart and collaborative industrial IoT: A federated learning and data space approach," Digital Communications and Networks, 2023.
[15]. Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus," IEEE Network, vol. 35, no. 1, pp. 234-241, 2021.
[16]. H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained On-Device Federated Learning," IEEE Communications Letters, vol. 24, no. 6, pp. 1279-1283, 2020.
[17]. D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, and K.-C. Li, "Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey," Soft Computing, 2021.
[18]. Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood, "Blockchain-enabled Federated Learning: A Survey," ACM Computing Surveys, 2022.
[19]. S. Ren, E. Kim, and C. Lee, "A scalable blockchain-enabled federated learning architecture for edge computing," PLOS ONE, 2024.
[20]. W. Ning, Y. Zhu, C. Song, H. Li, L. Zhu, J. Xie, T. Chen, T. Xu, X. Xu, and J. Gao, "Blockchain-Based Federated Learning: A Survey and New Perspectives," Applied Sciences, 2024.
[21]. B. Du, H. Wang, Y. Li, J. Zhao, Y. Ma, and R. Huang, "Fair and Robust Federated Learning via Decentralized and Adaptive Aggregation based on Blockchain," ACM Trans. Sensor Networks, 2024.
[22]. Z. Zhou, Y. Tian, J. Xiong, J. Ma, and C. Peng, "Blockchain-Enabled Secure and Trusted Federated Data Sharing in IIoT," IEEE Trans. Industrial Informatics, 2023.
[23]. Q. Wang, H. Dong, Y. Huang, Z. Liu, and Y. Gou, "Blockchain-Enabled Federated Learning for Privacy-Preserving Non-IID Data Sharing in Industrial Internet," Computers, Materials and Continua, 2024.
[24]. J. Sengupta, S. Ruj, and S. Das Bit, "FairShare: Blockchain Enabled Fair, Accountable and Secure Data Sharing for Industrial IoT," IEEE Trans. Network and Service Management, 2023.
[25]. J. Tan, J. Shi, J. Wan, H.-N. Dai, J. Jin, and R. Zhang, "Blockchain-Based Data Security and Sharing for Resource-Constrained Devices in Manufacturing IoT," IEEE Internet of Things Journal, 2024.
[26]. W. Tong, L. Yang, Z. Li, X. Jin, and L. Tan, "Enhancing Security and Flexibility in the Industrial Internet of Things: Blockchain-Based Data Sharing and Privacy Protection," Sensors, 2024.
[27]. W. Wang, H. Huang, Z. Yin, T. R. Gadekallu, M. Alazab, and C. Su, "Smart contract token-based privacy-preserving access control system for industrial Internet of Things," Digital Communications and Networks, 2023.
[28]. W. Zhang, Z. Wang, and X. Li, "Blockchain-based decentralized federated transfer learning methodology for collaborative machinery fault diagnosis," Reliability Engineering and System Safety, 2023.
[29]. S. Zhang, P. Jiang, X. Li, C. Yin, and X. V. Wang, "A blockchain-empowered secure federated domain generalization framework for machinery fault diagnosis," Advanced Engineering Informatics, 2024.
[30]. W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-Based

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

Federated Learning for Device Failure Detection in Industrial IoT," IEEE Internet of Things Journal, 2021.
[31]. Y. Xiao, H. Shao, J. Lin, Z. Huo, and B. Liu, "BCE-FL: A Secure and Privacy-Preserving Federated Learning System for Device Fault Diagnosis Under Non-IID Condition in IIoT," IEEE Internet of Things Journal, 2024.
[32]. Y. Qin, J. Yang, J. Zhou, H. Pu, X. Zhang, and Y. Mao, "Dynamic weighted federated remaining useful life prediction approach for rotating machinery," Mechanical Systems and Signal Processing, 2023.
[33]. M. Mehta, S. Chen, H. Tang, and C. Shao, "A federated learning approach to mixed fault diagnosis in rotating machinery," Journal of Manufacturing Systems, 2023.
[34]. W. Zhang and X. Li, "Data privacy preserving federated transfer learning in machinery fault diagnostics using prior distributions," Structural Health Monitoring, 2022.
[35]. J. Ahn, Y. Lee, N. Kim, C. Park, and J. Jeong, "Federated Learning for Predictive Maintenance and Anomaly Detection Using Time Series Data Distribution Shifts in Manufacturing Processes," Sensors, 2023.
[36]. G. Xia, J. Chen, C. Yu, and J. Ma, "Poisoning Attacks in Federated Learning: A Survey," IEEE Access, 2023.
[37]. K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security (CCS), 2017.
[38]. M. Abadi, A. Chu, I. J. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with Differential Privacy," in Proc. 2016 ACM SIGSAC Conf. Computer and Communications Security (CCS), 2016, pp. 308-318.
[39]. J. Chen, J. Xue, Y. Wang, L. Huang, T. Baker, and Z. Zhou, "Privacy-Preserving and Traceable Federated Learning for data sharing in industrial IoT applications," Expert Systems with Applications, 2023.
[40]. K. M. Sameera, S. Nicolazzo, M. Arazzi, A. Nocera, K. A. Rafidha Rehiman, P. Vinod, and M. Conti, "Privacy-preserving in Blockchain-based Federated Learning systems," Computer Communications, 2024.
[41]. M. A. Heikkila, "On Using Secure Aggregation in Differentially Private Federated Learning with Multiple Local Steps," Transactions on Machine Learning Research (TMLR), 2025.
[42]. W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey," ACM Computing Surveys, 2023.
[43]. M. Shawkat, A. El-desoky, Z. H. Ali, and M. Salem, "Blockchain and federated learning based on aggregation techniques for industrial IoT: A contemporary survey," Peer-to-Peer Networking and Applications, 2025.
[44]. 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 Networks, vol. 152, art. 103320, 2024.
[45]. J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions," ACM Computing Surveys, vol. 55, no. 11, art. 240, 2023.
[46]. H. Alaya, A. Ben Letaifa, and A. Rachedi, "State of the art and taxonomy survey on federated learning and blockchain integration in UAV applications," The Journal of Supercomputing, 2025.
[47]. Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1817-1829, 2021.
[48]. F. Yang, Y. Qiao, M. Z. Abedin, and C. Huang, "Privacy-Preserved Credit Data Sharing Integrating Blockchain and Federated Learning for Industrial 4.0," IEEE Trans. Industrial Informatics, vol. 18, no. 12, pp. 8755-8764, 2022.
[49]. X. Tang, Y. Wang, X. Liu, X. Yuan, C. Fan, Y. Hu, and Q. Miao, "Federated graph neural network for privacy-preserved supply chain data sharing," Applied Soft Computing, vol. 168, art. 112475, 2025.
[50]. H. M. H. A. Alshkeili, S. J. Almheiri, and M. A. Khan, "Privacy-Preserving Interpretability: An Explainable Federated Learning Model for Predictive Maintenance in Sustainable Manufacturing and Industry 4.0," AI, vol. 6, no. 6, art. 117, 2025.
[51]. S. Matzka, "Explainable Artificial Intelligence for Predictive Maintenance Applications," in Proc. 2020 Third Int. Conf. Artificial Intelligence for Industries (AI4I), 2020, pp. 69-74, doi: 10.1109/AI4I49448.2020.00023.
[52]. M. Hossain and M. B. Uddin, "Digital twins in additive manufacturing," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 2, pp. 909-918, 2024.
[53]. M. B. Uddin, M. Hossain, and S. Das, "Advancing manufacturing sustainability with industry 4.0 technologies," International Journal of Science and Research Archive, vol. 6, no. 1, pp. 358-366, 2022.
[54]. M. O. Bouraima, M. H. Suvo, M. J. Islam, M. B. N. Shahin, and D. Nandy, "AI-Driven Data Reliability for Decision-Making in Advanced Manufacturing and Supply Chain Systems," International Journal of Industrial Engineering Research and Development (IJIERD), vol. 14, no. 2, pp. 45-58, 2023. doi: 10.34218/IJIERD_14_02_004.
[55]. J. Shekh, M. B. N. Shahin, M. J. Islam, M. H. Suvo, and D. Nandy, "ML Framework for Predictive Hazard Monitoring in Smart Manufacturing Environments," International Journal of Scientific Research in Science, Engineering and Technology, vol. 11, no. 6, pp. 583-592, 2024. doi: 10.32628/IJSRSET2512553.
[56]. Y. A. Bipasha, "Blockchain technology in supply chain management: transparency, security, and efficiency challenges," International Journal of Science and Research Archive, vol. 10, no. 1, pp. 1186-1196, 2023.
[57]. M. R. Islam, “System Dynamics of Leadership Influence in Sustainable Supply Chains,” World Journal of Advanced Engineering Technology and Sciences, vol. 17, no. 03, pp. 509–514, 2025, doi: 10.30574/wjaets.2025.17.3.1584.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1585

[58]. M. R. Islam, "Digital Leadership and Circular Economy Performance in Sustainable Supply Chains," World Journal of Advanced Engineering Technology and Sciences, vol. 17, no. 03, pp. 503–508, 2025, doi: 10.30574/wjaets.2025.17.3.1583.
[59]. M. R. Islam, "Circular economy leadership for sustainable industrial transformation: A holistic framework for resilient and resource-efficient growth," World Journal of Advanced Engineering Technology and Sciences, vol. 17, no. 03, pp. 253–262, 2025, doi: 10.30574/wjaets.2025.17.3.1540.
[60]. Y. A. Bipasha, M. R. Islam, and M. F. Ahmed, "A blockchain and machine learning framework for secure and transparent digital supply chain management," International Journal of Innovative Science and Research Technology, vol. 11, no. 3, pp. 945–952, Mar. 2026, doi: 10.38124/IJISRT/26MAR767.
[61]. M. R. Islam and A. Halim, "Developing a challenge-driven project management framework for sustainable development: An MCDM-based evaluation and prioritization approach," International Journal of Science and Research Archive, vol. 18, no. 01, pp. 177–187, 2026, doi: 10.30574/ijsra.2026.18.1.0027.
[62]. M. B. Uddin, M. R. Islam, M. N. Uddin, and A. Halim, "Next-generation plastic recycling: Breakthrough developments and the path toward a circular economy," World Journal of Advanced Engineering Technology and Sciences, vol. 16, no. 01, pp. 513–527, 2025, doi: 10.30574/wjaets.2025.16.1.1237.
[63]. R. A. Elbarouni, "A review of AI-driven seismic interpretation, digital twin technology and intelligent reservoir characterization for hydrocarbon exploration," World Journal of Advanced Engineering Technology and Sciences, vol. 09, no. 01, pp. 513–519, 2023, doi: 10.30574/wjaets.2023.9.1.0147.
[64]. R. A. Elbarouni, "AI-driven digital twin framework for real-time seismic reservoir monitoring and predictive hydrocarbon production optimization," World Journal of Advanced Engineering Technology and Sciences, vol. 11, no. 02, pp. 712–720, 2024, doi: 10.30574/wjaets.2024.11.2.0122.
[65]. R. A. Elbarouni, "Advanced 3D seismic interpretation techniques for accurate subsurface structural mapping and reservoir characterization," International Journal of Science and Research Archive, vol. 18, no. 03, pp. 992–1002, 2026, doi: 10.30574/ijsra.2026.18.3.0539.
[66]. R. A. Elbarouni, "Seismic attribute-based fault detection and structural mapping in 3D seismic data for hydrocarbon exploration," World Journal of Advanced Engineering Technology and Sciences, vol. 18, no. 03, pp. 320–329, 2026, doi: 10.30574/wjaets.2026.18.3.0166.