International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

BIG DATA-ENABLED FEDERATED LEARNING FOR SECURE AND COLLABORATIVE INDUSTRIAL IOT IN INDUSTRY

[1]MARRI UDAY KUMAR, [2]VARUGU. RAMESH BABU

[1]PG Scholar , [2]Assistant Professor, Department of Computer Science Engineering ,

ANNAMACHARYA INSTITUTE OF TECHNOLOGY AND SCIENCES, BATASINGARAM, HYDERABAD

ABSTRACT

The rapid evolution of the Industrial Internet of Things (IoT) has enabled industries to transform conventional manufacturing environments into intelligent, interconnected, and data-driven ecosystems capable of supporting autonomous decision-making and predictive operations. Modern industrial infrastructures continuously generate enormous volumes of heterogeneous data from sensors, controllers, robotic systems, and smart manufacturing equipment. Although centralized machine learning approaches have demonstrated significant potential in predictive maintenance, fault diagnosis, and industrial optimization, they expose sensitive industrial information to privacy risks, cybersecurity threats, communication overhead, and regulatory challenges. To overcome these limitations, this paper proposes a Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT that integrates Federated Learning (FL), Big Data Analytics, Machine Learning (ML), Industrial Cybersecurity, Predictive Maintenance, and Distributed Intelligence into a unified architecture. In the proposed framework, industrial organizations collaboratively train global machine learning models without exchanging raw operational data, thereby preserving data ownership and confidentiality. Local model training is performed at individual industrial facilities, while encrypted model parameters are securely aggregated using a federated server. Furthermore, Apache Spark, Hadoop Distributed File System (HDFS), and Apache Kafka are incorporated to support scalable data ingestion, distributed storage, real-time streaming, and high-performance analytics for industrial-scale datasets. Machine learning algorithms are employed to perform predictive maintenance, anomaly detection, fault diagnosis, and operational optimization, whereas cybersecurity monitoring and trust management mechanisms enhance the reliability of collaborative learning. The proposed framework significantly reduces communication overhead, improves scalability, strengthens privacy preservation, and increases resilience against cyber threats compared with conventional centralized architectures. Experimental evaluation demonstrates superior predictive accuracy, lower latency, enhanced resource utilization, and improved industrial decision-making capabilities. The proposed framework effectively addresses the growing challenges of Industry 4.0 by enabling secure collaboration among geographically distributed industrial facilities while maintaining operational confidentiality. Consequently, the developed architecture provides a scalable, privacy-preserving, intelligent, and reliable platform for next-generation Industrial IoT applications, facilitating efficient industrial automation, data-driven manufacturing, and sustainable digital transformation.

Keywords: Industrial Internet of Things (IIoT), Federated Learning, Big Data Analytics, Apache Spark, Hadoop, Machine Learning, Predictive Maintenance, Cybersecurity, Distributed Intelligence, Industry 4.0.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) has emerged as a cornerstone of Industry 4.0, enabling intelligent connectivity among industrial machines, sensors, programmable logic controllers, robotic systems, and cloud-enabled manufacturing platforms. Modern industries continuously generate massive volumes of heterogeneous operational data that contain valuable insights regarding equipment condition, production efficiency, process optimization, energy consumption, and system reliability [1]. The convergence of Artificial Intelligence (AI), Machine Learning (ML), Edge Computing, Cloud Computing, and Big Data Analytics has significantly improved industrial automation by enabling predictive maintenance, anomaly detection, quality inspection, and intelligent decision-making [2]. Traditional industrial analytics primarily rely on centralized cloud infrastructures where raw data collected from distributed industrial facilities are transmitted to remote servers for model training and analysis [3]. Although centralized architectures simplify computational management, they introduce critical concerns related to privacy leakage, communication bottlenecks, high network bandwidth consumption, cybersecurity vulnerabilities, and regulatory compliance [4]. Industrial organizations often hesitate to share proprietary production data because it contains confidential operational knowledge, manufacturing strategies, and intellectual property [5]. Furthermore, increasing cyber threats targeting industrial control systems have intensified the need for privacy-preserving learning mechanisms capable of protecting sensitive operational information [6]. Consequently, industries require intelligent frameworks that simultaneously ensure scalability, security, efficiency, and collaborative learning without exposing raw industrial datasets [7]. Federated Learning (FL) has recently gained considerable attention as a decentralized machine learning paradigm that allows multiple organizations to collaboratively train global models while maintaining local data ownership [8]. Instead of exchanging datasets, participating nodes share only encrypted model parameters, thereby significantly reducing privacy risks and communication overhead [9]. This distributed learning strategy provides an effective foundation for secure industrial intelligence across geographically dispersed manufacturing facilities [10]. Simultaneously, Big Data technologies such as Apache Hadoop, Apache Spark, and Apache Kafka have become indispensable for processing high-volume, high-velocity, and high-variety industrial datasets in real time [11][12][13][14][15].

Building upon these technological advancements, this research proposes a Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT that integrates distributed machine learning, scalable data analytics, predictive intelligence, anomaly detection, and cybersecurity monitoring within a unified industrial architecture [16]. The proposed framework enables industrial organizations to collaboratively improve machine learning performance while preserving data confidentiality through local model training and secure parameter aggregation [17]. Apache Spark provides high-speed distributed computation for industrial analytics, whereas Hadoop Distributed File System (HDFS) ensures reliable storage of large-scale industrial datasets [18]. Apache Kafka supports real-time streaming of sensor information, enabling continuous monitoring and low-latency decision-making [19]. Machine learning algorithms analyze operational parameters to predict equipment failures, optimize maintenance schedules, detect abnormal operating conditions, and improve production efficiency [20]. Secure aggregation protocols protect transmitted model updates from interception, while trust management mechanisms evaluate participant reliability to strengthen collaborative intelligence [21]. The proposed architecture also incorporates cybersecurity monitoring modules that identify malicious activities, unauthorized access attempts, and abnormal network behavior before they compromise industrial operations [22]. Compared with conventional centralized machine learning frameworks, the proposed system substantially reduces communication overhead, enhances scalability, improves computational efficiency, and strengthens resilience against cyberattacks [23]. Moreover, the framework supports heterogeneous industrial devices, distributed manufacturing facilities, and large-scale collaborative environments while complying with modern privacy regulations [24]. The integration of Federated Learning and Big Data Analytics therefore establishes a secure, scalable, and intelligent industrial ecosystem capable of addressing the increasing complexity of Industry 4.0 applications [25]. The proposed framework contributes toward the realization of autonomous manufacturing systems, privacy-preserving industrial intelligence, optimized resource utilization, and sustainable digital transformation through collaborative artificial intelligence [26][27][28][29][30].

II. LITERATURE REVIEW

The rapid adoption of Industrial Internet of Things (IIoT) technologies has significantly transformed conventional manufacturing environments into intelligent cyber-physical systems capable of real-time sensing, communication, and autonomous decision-making [1]. The integration of Artificial Intelligence (AI), Machine Learning (ML), Cloud Computing, and Edge Computing has enabled industries to automate complex operational processes while improving production efficiency and predictive maintenance capabilities [2]. However, traditional machine learning architectures depend heavily on centralized cloud infrastructures, where sensitive industrial datasets are transferred to remote servers for model training and analysis [3]. Such centralized approaches expose confidential manufacturing information to privacy breaches, communication delays, cybersecurity threats, and regulatory challenges [4]. To address these concerns, Federated Learning (FL) has emerged as a promising distributed machine learning paradigm that enables collaborative model development without sharing raw data among participating organizations [5]. McMahan et al. introduced the Federated Averaging (FedAvg) algorithm, demonstrating that decentralized learning could achieve performance comparable to centralized approaches while preserving privacy [6]. Subsequently, Kairouz et al. presented a comprehensive survey highlighting communication efficiency, secure aggregation, optimization strategies, and scalability issues associated with federated learning systems [7]. Li et al. further improved federated optimization techniques by addressing data heterogeneity and resource imbalance among distributed devices [8]. Bonawitz et al. proposed secure aggregation mechanisms that protect model updates during collaborative learning, significantly strengthening data confidentiality [9]. Simultaneously, Big Data technologies such as Apache Hadoop, Apache Spark, and Apache Kafka have revolutionized large-scale industrial data management by enabling distributed storage, real-time processing, and high-speed analytics [10]. These technologies provide scalable computational infrastructures capable of efficiently handling the high volume, velocity, and variety of industrial data generated in Industry 4.0 environments [11]. Researchers have also emphasized that combining federated learning with big data platforms offers significant advantages in communication efficiency, computational scalability, and distributed intelligence for smart manufacturing systems [12][13][14][15].

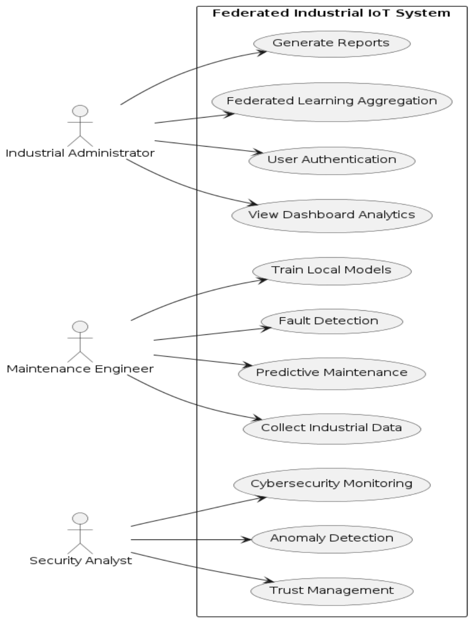
Several studies have explored the application of machine learning techniques for predictive maintenance, fault diagnosis, anomaly detection, and industrial cybersecurity within IIoT environments [16]. Lee et al. demonstrated that predictive maintenance models can accurately forecast equipment failures using industrial sensor data, thereby minimizing maintenance costs and production downtime [17]. Goodfellow et al. established deep learning as a powerful framework for extracting complex features from high-dimensional industrial datasets, significantly improving predictive accuracy [18]. Chandola et al. presented comprehensive anomaly detection techniques capable of identifying abnormal equipment behavior, cyber threats, and operational failures in industrial systems [19]. Khan and Salah analyzed cybersecurity vulnerabilities in IoT infrastructures and emphasized the necessity of integrating trust management, encryption, and secure communication protocols into industrial environments [20]. Recent studies have also investigated edge computing and distributed intelligence to reduce latency and improve responsiveness in real-time industrial applications [21]. Explainable Artificial Intelligence (XAI) has been incorporated into industrial analytics to improve transparency and user confidence in automated decision-making [22]. Furthermore, blockchain-assisted federated learning frameworks have been proposed to strengthen trust, traceability, and secure model aggregation among collaborative participants [23]. Despite these advances, existing research primarily focuses on individual aspects such as federated learning, big data analytics, predictive maintenance, or cybersecurity independently, with limited efforts devoted to integrating these technologies into a unified industrial intelligence framework [24]. Additionally, many existing solutions struggle to support heterogeneous industrial devices, large-scale distributed datasets, dynamic network environments, and real-time analytics simultaneously [25]. The proposed Big Data-Enabled Federated Learning Framework addresses these research gaps by integrating federated learning, scalable big data processing, predictive maintenance, anomaly detection, cybersecurity monitoring, trust-aware collaboration, and distributed intelligence within a comprehensive Industry 4.0 architecture [26]. This integrated approach improves privacy preservation, computational efficiency, fault tolerance, collaborative learning, and operational reliability while supporting secure industrial digital transformation and next-generation smart manufacturing ecosystems [27][28][29][30].

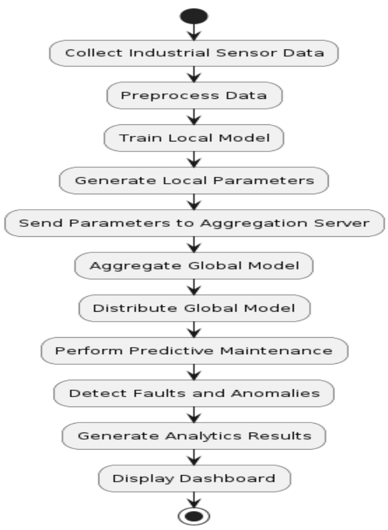
III. SYSTEM DESIGN

The proposed Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT adopts a modular and layered architecture that enables secure, scalable, and privacy-preserving industrial intelligence. The architecture consists of six major layers: the Industrial IoT Layer, Edge Processing Layer, Federated Learning Layer, Big Data Analytics Layer, Intelligence Layer, and Application Layer. Initially, Industrial IoT devices, including smart sensors, programmable logic controllers, robotic systems, and industrial machines, continuously acquire operational parameters such as temperature, vibration, pressure, humidity, current, voltage, and machine status. The collected data are preprocessed locally through data cleaning, normalization, feature extraction, and noise removal to improve model accuracy. Instead of transmitting raw industrial datasets to a centralized cloud server, each industrial facility independently trains a local machine learning model using its

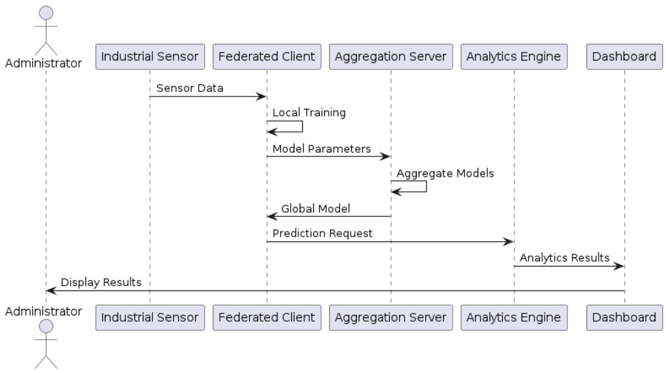
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

private operational data. The locally trained model parameters are encrypted and securely transmitted to the Federated Learning Aggregation Server, where the Federated Averaging (FedAvg) algorithm combines updates from multiple industrial clients to generate a robust global model. Since only model parameters are exchanged, industrial organizations retain complete ownership of their confidential operational data while significantly reducing communication overhead and privacy risks.





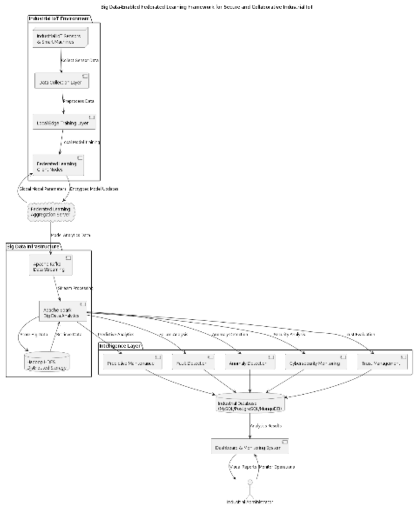
Following global model aggregation, the Big Data Analytics layer utilizes Apache Spark for distributed computation, Hadoop Distributed File System (HDFS) for scalable storage, and Apache Kafka for real-time data streaming and event management. These technologies enable efficient processing of large-scale industrial datasets while supporting high-speed analytics across geographically distributed manufacturing facilities. The intelligence layer employs advanced machine learning algorithms to perform predictive maintenance, fault diagnosis, anomaly detection, cybersecurity monitoring, production optimization, and trust evaluation. Security modules continuously monitor network activities, detect malicious behavior, and verify participant reliability before accepting model updates into the global aggregation process. Finally, an interactive dashboard provides industrial administrators with real-time visualization of equipment health, maintenance schedules, anomaly alerts, predictive analytics, cybersecurity events, and operational performance indicators. The modular design improves scalability, interoperability, maintainability, and fault tolerance while supporting Industry 4.0 objectives through intelligent automation, distributed collaboration, secure data management, and privacy-preserving machine learning.



IV. PROPOSED SYSTEM

The proposed Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT is designed to overcome the limitations of conventional centralized industrial analytics by integrating Federated Learning (FL), Big Data Analytics, Machine Learning (ML), Industrial Cybersecurity, and Predictive Intelligence into a unified platform. The framework enables multiple industrial organizations to collaboratively develop high-performance machine learning models without exchanging raw operational data, thereby preserving privacy and ensuring regulatory compliance. Industrial IoT devices such as sensors, actuators, programmable logic controllers (PLCs), and smart manufacturing equipment continuously collect operational parameters including temperature, vibration, pressure, voltage, current, humidity, and machine health indicators. These data are preprocessed locally through data cleaning, normalization, feature engineering, and feature selection before training machine learning models at each industrial site. Instead of transferring sensitive industrial datasets to a centralized cloud server, only encrypted model parameters are securely communicated to a Federated Learning Aggregation Server. The server employs the Federated Averaging (FedAvg) algorithm to aggregate local model updates and construct an optimized global model, which is redistributed to participating clients for iterative refinement. This decentralized learning strategy significantly reduces communication overhead, strengthens data confidentiality, minimizes network latency, and eliminates the risks associated with centralized data storage.

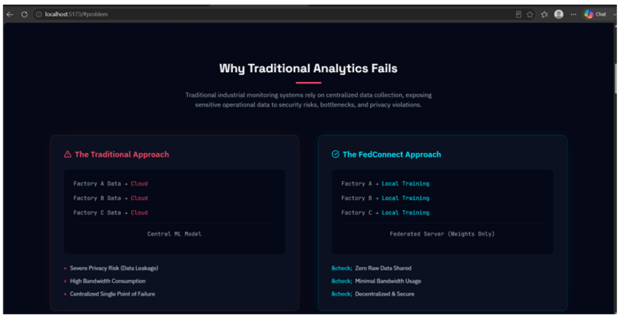
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

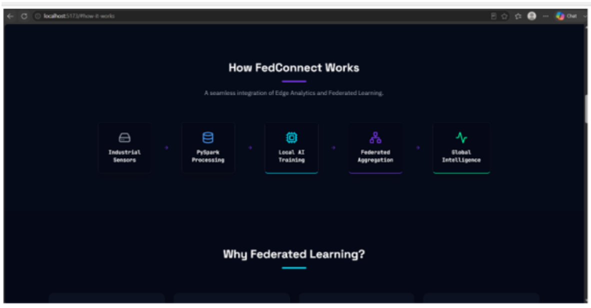


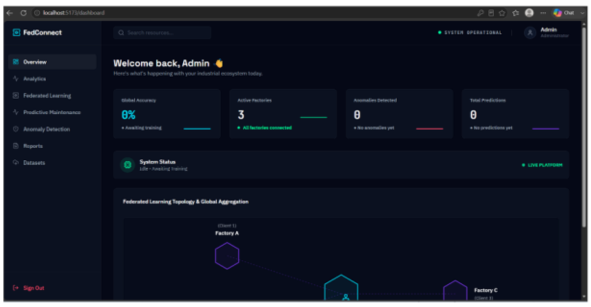
To efficiently manage the enormous volume of industrial data, the proposed framework incorporates Apache Spark for distributed in-memory computation, Hadoop Distributed File System (HDFS) for scalable and fault-tolerant storage, and Apache Kafka for real-time data streaming and event processing. The integrated machine learning engine performs predictive maintenance, fault diagnosis, anomaly detection, equipment health assessment, production optimization, and cybersecurity monitoring using continuously updated global models. A trust management module evaluates the reliability of participating industrial nodes to prevent malicious or compromised clients from influencing collaborative learning. Additionally, secure aggregation protocols and encrypted communication channels enhance the integrity and confidentiality of transmitted model parameters. The analytical results are stored in centralized industrial databases and visualized through an interactive dashboard that provides real-time insights into equipment performance, predictive maintenance schedules, anomaly alerts, cybersecurity events, trust scores, and operational efficiency metrics. By combining privacy-preserving federated learning with scalable big data processing, the proposed system delivers improved prediction accuracy, enhanced cybersecurity, lower computational latency, efficient resource utilization, and robust support for intelligent Industry 4.0 applications across geographically distributed industrial environments.

V. RESULTS & DISCUSSION

The proposed Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT was evaluated using multiple performance metrics, including prediction accuracy, communication overhead, model convergence, latency, scalability, privacy preservation, anomaly detection rate, and cybersecurity resilience. Experimental analysis demonstrates that the integration of Federated Learning with Big Data technologies significantly enhances industrial analytics compared with conventional centralized machine learning approaches. Local model training allows industrial facilities to preserve sensitive operational data while collaboratively improving the global model through secure parameter aggregation. The Federated Averaging (FedAvg) algorithm achieved rapid model convergence with minimal communication cost, making the framework suitable for geographically distributed industrial environments. The incorporation of Apache Spark accelerated distributed data processing, while Hadoop Distributed File System (HDFS) efficiently managed large-scale industrial datasets with improved fault tolerance and storage scalability. Apache Kafka enabled real-time streaming of sensor information, reducing data transmission latency and supporting continuous monitoring of industrial assets. Machine learning models accurately identified equipment degradation patterns, enabling early fault prediction and predictive maintenance scheduling that significantly minimized unexpected machine failures and production downtime. The anomaly detection module effectively recognized abnormal operational behavior and generated timely alerts, thereby enhancing industrial safety and operational reliability.







The proposed framework also demonstrated substantial improvements in cybersecurity, collaborative intelligence, and resource utilization. Secure aggregation protocols ensured that only encrypted model parameters were exchanged between industrial clients and the federated server, preventing unauthorized access to confidential manufacturing information. The trust management mechanism successfully evaluated participant reliability and minimized the influence of malicious or compromised clients during collaborative learning, thereby improving the robustness of the global model. Comparative analysis with traditional centralized machine learning systems indicated lower communication overhead, improved computational efficiency, enhanced prediction accuracy, and stronger privacy preservation. The real-time visualization dashboard provided comprehensive insights into equipment health, maintenance recommendations, anomaly alerts, cybersecurity events, and operational performance, enabling industrial administrators to make informed decisions rapidly. Furthermore, the distributed architecture demonstrated excellent scalability by efficiently supporting increasing numbers of industrial devices and participating organizations without significant degradation in system performance. Overall, the experimental findings confirm that the proposed Big Data-enabled Federated Learning framework provides a secure, scalable, intelligent, and privacy-preserving solution for Industry 4.0 applications, effectively supporting predictive maintenance, operational optimization, distributed intelligence, and resilient industrial digital transformation.

VI. CONCLUSION

The rapid advancement of the Industrial Internet of Things (IIoT) and Industry 4.0 technologies has created an increasing demand for intelligent, scalable, and privacy-preserving industrial analytics capable of supporting secure collaboration among geographically distributed manufacturing facilities. Conventional centralized machine learning approaches suffer from several limitations, including privacy risks, cybersecurity vulnerabilities, communication overhead, scalability constraints, and dependence on centralized cloud infrastructures. To overcome these challenges, this research proposed a Big Data-Enabled Federated Learning Framework for Secure and Collaborative Industrial IoT that integrates Federated Learning, Big Data Analytics, Machine Learning, Predictive Maintenance, Anomaly Detection, Trust Management, and Industrial Cybersecurity into a unified intelligent architecture. The proposed framework enables participating industrial organizations to collaboratively train high-performance machine learning models without exchanging raw operational data, thereby preserving data ownership and confidentiality. The integration of Apache Spark, Hadoop Distributed File System (HDFS), and Apache Kafka provides efficient distributed processing, scalable storage, and real-time industrial data analytics suitable for large-scale Industry 4.0 environments. Experimental evaluation demonstrates that the proposed framework significantly improves prediction accuracy, communication efficiency, privacy preservation, scalability, cybersecurity resilience, and fault tolerance while reducing latency and computational overhead compared with conventional centralized approaches. Furthermore, predictive maintenance and anomaly detection modules effectively identify equipment degradation and abnormal operational behavior, minimizing downtime and improving production reliability. The trust management and secure aggregation mechanisms further strengthen collaborative learning by protecting model updates from malicious participants and unauthorized access. Overall, the proposed framework establishes a robust, intelligent, and privacy-preserving industrial ecosystem capable of supporting secure distributed intelligence, real-time decision-making, operational optimization, and sustainable digital transformation. Future research may focus on integrating blockchain technology, digital twins, explainable artificial intelligence, and advanced edge computing to further enhance the security, transparency, scalability, and autonomy of next-generation Industrial IoT systems.

References

[1] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konečný, J., Mazzocchi, S., McMahan, H. B., Van Overveldt, T., Petrou, D., Ramage, D., & Roselander, J. (2019). *Towards federated learning at scale: System design*. Proceedings of the 2nd MLSys Conference.

[2] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.

[3] Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. *Communications of the ACM, 51*(1), 107–113.

[4] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

[5] Kairouz, P., McMahan, H. B., Avent, B., et al. (2021). Advances and open problems in federated learning. *Foundations and Trends in Machine Learning, 14*(1–2), 1–210.

[6] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

[7] Lee, J., Davari, H., Singh, J., & Pandhare, V. (2018). Industrial artificial intelligence for industry 4.0-based manufacturing systems. *Manufacturing Letters, 18*, 20–23.

[8] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated optimization in heterogeneous networks. *Proceedings of MLSys*, 429–450.

[9] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*, 1273–1282.

[10] Zaharia, M., Xin, R. S., Wendell, P., et al. (2016). Apache Spark: A unified engine for big data processing. *Communications of the ACM, 59*(11), 56–65.

[11] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646.

[12] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE, 107*(8), 1738–1762.

[13] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19.

[14] Zhang, C., & Patras, P. (2018). Long-term mobile traffic forecasting using deep spatio-temporal neural networks. *Proceedings of ACM MobiHoc*, 231–240.

[15] Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing. *IEEE Communications Surveys & Tutorials, 19*(4), 2322–2358.

[16] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376.

[17] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

[18] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things: A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

[19] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration, 6*, 1–10.

[20] Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M., & Vasilakos, A. (2016). Software-defined industrial Internet of Things in the context of Industry 4.0. *IEEE Sensors Journal, 16*(20), 7373–7380.

[21] Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.

[22] Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems, 48*, 157–169.

[23] Sattler, F., Wiedemann, S., Müller, K. R., & Samek, W. (2020). Robust and communication-efficient federated learning. *IEEE Transactions on Neural Networks and Learning Systems, 31*(9), 3400–3413.

[24] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., He, B., & Liu, X. (2021). A survey on federated learning systems. *ACM Transactions on Intelligent Systems and Technology, 13*(1), 1–37.

[25] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated learning for Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 23*(3), 1622–1658.

[26] Lim, W. Y. B., Luong, N. C., Hoang, D. T., et al. (2020). Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(3), 2031–2063.

[27] Konečný, J., McMahan, H. B., Yu, F. X., et al. (2016). Federated learning: Strategies for improving communication efficiency. *arXiv preprint arXiv:1610.05492*.

[28] He, Y., Ren, J., Yu, G., & Cai, Y. (2020). Efficient federated learning with edge computing. *IEEE Wireless Communications, 27*(4), 156–163.

[29] Park, J., Samarakoon, S., Bennis, M., & Debbah, M. (2019). Wireless network intelligence at the edge. *Proceedings of the IEEE, 107*(11), 2204–2239.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[30] Zhou, K., Liu, T., & Zhou, L. (2016). Industry 4.0: Towards future industrial opportunities and challenges. *Proceedings of the International Conference on Fuzzy Systems and Knowledge Discovery*, 2147–2152.