OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) | ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Federated Learning for Secure Inter-Agency Data Collaboration in Critical Infrastructure

Md Arifur Rahman[1*], Israt Jahan Bristy[2], Md Iftakhayrul Islam[1], Marzia Tabassum[3]

[1]Master of Business Administration in Management Information Systems, International American University, Los Angeles, CA, USA
[2]Master of Business Administration in Management Information Systems, Lamar University, Beaumont, TX, United States

DOI: https://doi.org/10.36348/sjet.2025.v10i09.005 | **Received:** 03.07.2025 | **Accepted:** 01.09.2025 | **Published:** 11.09.2025

***Corresponding author:** Md Arifur Rahman
Master of Business Administration in Management Information Systems, International American University, Los Angeles, CA, USA

Abstract

Critical infrastructures, such as transportation, healthcare, and energy systems, are becoming increasingly interconnected, creating an urgent need for secure and efficient data sharing between agencies. However, the complexity of inter-agency collaboration is heightened by significant challenges, including privacy concerns, regulatory constraints, and inherent security risks. To address these concerns, Federated Learning (FL), a machine learning technique that facilitates the collaborative training of models across decentralized data sources without the need to transfer sensitive data, has emerged as a highly promising solution. FL ensures that agencies can jointly leverage the power of data-driven insights while ensuring privacy preservation. This paper investigates the potential of federated learning as a means to enable secure, scalable data collaboration between agencies in critical infrastructure sectors. We propose a novel federated learning framework tailored specifically for these sectors, taking into account sector-specific data requirements, regulatory frameworks, and security needs. Additionally, we discuss the effectiveness, challenges, and limitations of the proposed framework, as well as explore its potential for future applications and advancements. This paper aims to contribute to the growing body of research on privacy-preserving machine learning solutions in high-stakes, sensitive environments.

Keywords: Federated Learning, Data Collaboration, Critical Infrastructure, Privacy, Security, Machine Learning, Inter-Agency Collaboration, Decentralized Systems, Privacy-Preserving Computing.

I. INTRODUCTION

In the modern age, critical infrastructure sectors such as healthcare, transportation, energy, and telecommunications are increasingly becoming reliant on sophisticated digital systems for monitoring, managing, and optimizing operations. These systems generate vast amounts of data that can be leveraged to improve performance, reduce costs, and drive innovation. For example, smart grids in the energy sector and intelligent traffic systems in transportation can benefit significantly from real-time data-driven decision-making. However, the sensitive nature of this data, whether personal health records or national security data poses significant challenges. The potential risks of data breaches and the complexities of inter-agency collaboration in these sectors necessitate a more secure and privacy-preserving solution for data sharing and collaborative analytics. Traditional centralized models of data sharing, where all data is aggregated into a central server for processing and analysis, present significant security and privacy challenges. These methods are often impractical due to data security concerns and regulatory requirements, particularly in high-stakes environments like critical infrastructures. Federated learning (FL), a decentralized machine learning approach that allows agencies to collaboratively train models on their data without sharing raw data, presents a viable solution to address these issues. This section outlines the motivation behind exploring federated learning for secure data collaboration in critical infrastructure sectors and introduces the challenges that this paper seeks to overcome.

A. Background and Motivation

As critical infrastructures become more connected, the volume and variety of data being generated across different agencies and sectors are expanding rapidly. For example, smart grids generate data on energy usage, while transportation networks collect real-time traffic information. These data sources can be invaluable in improving service delivery, enhancing system resilience, and optimizing resource allocation. However, agencies often face difficulties in sharing data due to stringent privacy regulations and security concerns. Data privacy laws, such as GDPR in the European Union or HIPAA in the United States, impose strict restrictions on the sharing and usage of sensitive data, which can hinder inter-agency collaboration. Federated learning (FL) offers a novel approach to overcome these limitations. It allows different agencies to collaborate on model training by keeping their data local and sharing only model updates. This method significantly reduces privacy risks because sensitive information is never transferred between agencies. Federated learning's decentralized nature ensures that sensitive data, such as personal health records or financial data, remains within the local agency's jurisdiction, while still benefiting from the collective learning that comes from multiple data sources. As the demand for collaboration across agencies in critical infrastructures increases, FL provides a compelling solution to address the privacy and security challenges inherent in this process. The potential for federated learning to enable secure, collaborative data analysis in critical infrastructure sectors is what motivates this research.

B. Problem Statement

Despite the significant advantages of federated learning, its application to inter-agency collaboration within critical infrastructure sectors remains underexplored and faces multiple challenges. The first challenge arises from the heterogeneity of data across different agencies. Each agency might use different data formats, sensors, and reporting mechanisms, leading to inconsistencies in the data. These inconsistencies can complicate the model training process, as federated learning requires a uniform model structure across all participating agencies. Another challenge is the varying quality of data. While some agencies may have high-quality, clean data, others might face issues with missing, outdated, or noisy data. This disparity in data quality can result in models that are not robust and fail to generalize well across different systems. Moreover, regulatory compliance presents another major challenge. Different agencies often operate under different legal and regulatory frameworks, making it difficult to standardize data-sharing practices and ensure compliance with various laws. Additionally, the technical integration of federated learning with existing infrastructure systems is not without its hurdles. Communication overhead between agencies can be significant, especially when the agencies are geographically dispersed. Furthermore, synchronization of the models across different agencies can be challenging when the data is not synchronized in real-time. The proposed research aims to address these challenges by developing a federated learning framework that is tailored for critical infrastructure sectors. This framework will account for data heterogeneity, varying data quality, and the need for compliance with diverse regulations, while also optimizing for scalability and real-time decision-making.

C. Proposed Solution

This paper proposes a federated learning framework specifically designed for inter-agency collaboration within critical infrastructure sectors. The framework aims to address the challenges mentioned above while ensuring data security, privacy, and regulatory compliance. The core of the proposed framework lies in the decentralized nature of federated learning, which enables multiple agencies to train models on their local data without sharing raw data. To address data heterogeneity, the framework employs pre-processing techniques to standardize the data before it is used for model training. Agencies will perform data cleaning and normalization locally, ensuring that the models receive consistent inputs despite variations in data sources. Additionally, the framework will incorporate differential privacy techniques to protect sensitive information, even during model aggregation. Secure multi-party computation (SMPC) protocols will be used to ensure that model updates from different agencies are aggregated securely, preventing data leakage during communication. These privacy-preserving methods will ensure that the framework complies with privacy regulations, such as GDPR and HIPAA, while maintaining the integrity of the collaborative model training process. The proposed framework will be evaluated in critical infrastructure scenarios, such as smart grid management and healthcare systems, where real-time decision-making is essential. Through this evaluation, the effectiveness of the framework in enhancing data collaboration while ensuring privacy and security will be demonstrated.

D. Contributions

This paper makes several key contributions to the field of federated learning and secure data collaboration. First, it introduces a novel federated learning framework specifically designed for inter-agency collaboration in critical infrastructure sectors. The framework addresses the unique challenges these sectors face, including ensuring data privacy, security, and regulatory compliance while enabling efficient data collaboration across various agencies. Second, the paper provides an in-depth analysis of the challenges involved in applying federated learning to critical infrastructure, with a particular focus on data heterogeneity, varying data quality, and regulatory complexities. It also highlights the opportunities that federated learning offers in overcoming these challenges and improving inter-agency collaboration, which is crucial for efficient decision-making in critical infrastructure. Third, the paper discusses the integration of advanced privacy-preserving techniques such as secure aggregation and differential privacy within the federated learning framework. These techniques are designed to ensure that sensitive data remains protected during the collaborative training process, while also ensuring compliance with data protection laws like GDPR and HIPAA. Finally, the paper compares the proposed federated learning framework with traditional centralized data-sharing methods, illustrating the distinct advantages of federated learning in terms of privacy preservation, scalability, and overall system security.

E. Paper Organization

This paper is organized as follows: Section II reviews related work in the areas of federated learning, data collaboration, and critical infrastructure security. Section III outlines the methodology behind the proposed federated learning framework, detailing the technical aspects of the system, including data pre-processing, secure aggregation, and privacy-preserving techniques. Section IV discusses the results, challenges, and potential impacts of the proposed framework when applied to critical infrastructure sectors. Finally, Section V concludes the paper, offering recommendations for future research and highlighting the potential for federated learning to revolutionize inter-agency data collaboration in critical infrastructures.

II. Related Work

In this section, we review the current literature on federated learning (FL), focusing on its applications in privacy-preserving systems and critical infrastructure. We explore how federated learning has been leveraged in diverse domains, such as healthcare, finance, and the Internet of Things (IoT), as well as its application in enhancing the security and efficiency of critical infrastructure data collaboration. While existing research provides valuable insights into the benefits of federated learning, the challenges specific to critical infrastructure, such as scalability, security, and real-time decision-making, require further investigation.

A. Federated Learning in Privacy-Preserving Systems

Federated learning has emerged as a powerful tool for privacy-preserving systems, particularly in sensitive domains such as healthcare, finance, and smart cities. In healthcare, federated learning enables medical institutions to collaborate on data-driven research without sharing patient records, ensuring compliance with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Hasan (2025) explored the use of machine learning for predictive maintenance in IoT-based systems, demonstrating how federated learning can securely optimize performance without compromising user data privacy [6]. Similarly, in financial systems, FL has been successfully applied to fraud detection and credit scoring, where different banks can train machine learning models collaboratively while keeping their customer data private [7]. Despite these promising applications, challenges such as communication overhead, model convergence, and data heterogeneity remain. The necessity for secure aggregation and differential privacy to mitigate the risks of data leakage has also been widely discussed in the literature, but further advancements are needed to improve the scalability of these techniques in large-scale collaborative networks. Additionally, the integration of federated learning with existing data protection frameworks requires further exploration to ensure compliance with regulations across different jurisdictions.

B. Federated Learning for Critical Infrastructure

Federated learning has found its way into critical infrastructure systems, where data security and operational continuity are of utmost importance. Early research on this topic has focused on sectors such as smart grids and transportation, where multiple agencies may need to collaborate to enhance system efficiency and resilience. In the context of smart grids, federated learning has been proposed as a means to collaboratively analyze energy usage patterns and improve grid stability without transferring sensitive consumer data [8]. However, challenges remain when it comes to addressing the unique security requirements of critical infrastructure, which include resilience to cyber-attacks and the ability to support real-time decision-making processes. For example, in transportation systems, federated learning can be used to optimize traffic management by enabling real-time collaboration between city authorities, transit agencies, and private companies, without sharing sensitive traffic or vehicle data. However, the application of FL in these contexts often faces difficulties related to data inconsistency and system synchronization, as well as the scalability of federated models when managing large, distributed networks. Researchers have pointed out that ensuring the integrity of the models through secure aggregation protocols and implementing robust attack detection mechanisms are crucial for the widespread deployment of FL in critical infrastructure systems [9].

C. Challenges of Security and Privacy in Federated Learning

One of the primary benefits of federated learning is its ability to preserve privacy while enabling data collaboration. However, the decentralized nature of FL introduces specific challenges related to security. Federated learning frameworks must address potential vulnerabilities, such as model poisoning and data inference attacks, where an adversary might manipulate local model updates or exploit shared information to infer sensitive data. Hasan (2025) discusses the integration of differential privacy techniques within federated learning frameworks to mitigate these risks, demonstrating that it is possible to train effective models without exposing individual data points [10]. This privacy-preserving feature is essential for sectors like healthcare, where patient data confidentiality is critical. Further research has focused on enhancing the security of federated learning by employing secure multi-party computation (SMPC) and homomorphic encryption to protect the integrity of shared model updates. These techniques ensure that sensitive data never leaves its local environment, significantly reducing the risk of data leakage during model aggregation. However, the computational complexity of these privacy-enhancing techniques introduces challenges related to system performance and real-time data processing, which is crucial for applications in critical infrastructure.

D. Federated Learning for Scalability and Real-Time Decision-Making

The application of federated learning in real-time decision-making environments, such as those found in critical infrastructure, presents unique challenges related to scalability and system synchronization. In sectors like smart grids and transportation, timely and accurate decisions are vital for ensuring operational efficiency and safety. The decentralized nature of federated learning means that updates from multiple agencies must be aggregated in a secure and timely manner, but communication delays and data heterogeneity can hinder model performance [11]. To address these issues, recent research has focused on optimizing federated learning frameworks for scalability and real-time application. For example, researchers have explored the use of edge computing and distributed ledger technologies to reduce communication overhead and improve the synchronization of federated learning models. These technologies allow model updates to be processed locally at the edge of the network, minimizing the need for constant communication with central servers and ensuring faster decision-making. However, achieving real-time performance in large-scale federated learning systems for critical infrastructure remains a complex challenge, requiring further innovation in both the underlying algorithms and the computational infrastructure.

III. METHODOLOGY

The proposed federated learning framework enables agencies to collaboratively train models without sharing raw data, maintaining data privacy. It consists of three components: Data Providers (Agencies), which manage and train models locally; Federated Aggregator, which combines local model updates into a global model; and Privacy-Preserving Techniques such as differential privacy and secure multi-party computation, which protect sensitive data. This framework ensures scalability, compliance with data protection laws, and privacy for critical infrastructure sectors.

A. Framework Design

The federated learning framework proposed in this study is designed to address the specific challenges faced by critical infrastructure sectors in securely collaborating on data-driven models while preserving data privacy and ensuring compliance with regulatory standards. It consists of three main components: Data Providers (Agencies), Federated Aggregator, and Privacy-Preserving Techniques. First, Data Providers (Agencies) are responsible for managing and training models on their local data, which remains on-site without being shared. This decentralized approach reduces the risks of data exposure, as no raw data is exchanged between agencies. Instead, only model updates, such as gradients or parameter changes, are communicated. This ensures that agencies can collaborate without violating data protection laws like GDPR or HIPAA, making it ideal for environments where data privacy is crucial. Agencies perform periodic updates to their local models based on new incoming data, which improves the model’s accuracy over time while keeping the data secure within the agency's boundaries. The second component, the Federated Aggregator, acts as the central coordinator of the federated learning process. This server is responsible for aggregating the local model updates from various agencies into a global model. To maintain data privacy during the aggregation, secure aggregation protocols are used to ensure that no sensitive information is exposed. The aggregator helps in scaling the system to accommodate multiple agencies and large datasets, making the model suitable for large-scale infrastructure projects. Finally, the Privacy-Preserving Techniques such as differential privacy and secure multi-party computation (SMPC) are incorporated to further enhance the privacy of model updates. Differential privacy ensures that individual contributions remain private, while SMPC guarantees that the aggregation process is secure and tamper-proof, maintaining the confidentiality of each agency’s data throughout the collaboration process. These methods are crucial for ensuring that federated learning can be used in sectors like healthcare, energy, and transportation where security and regulatory compliance are of utmost importance. This framework aims to balance collaboration and security, enabling scalable, privacy-preserving model training in critical infrastructure.

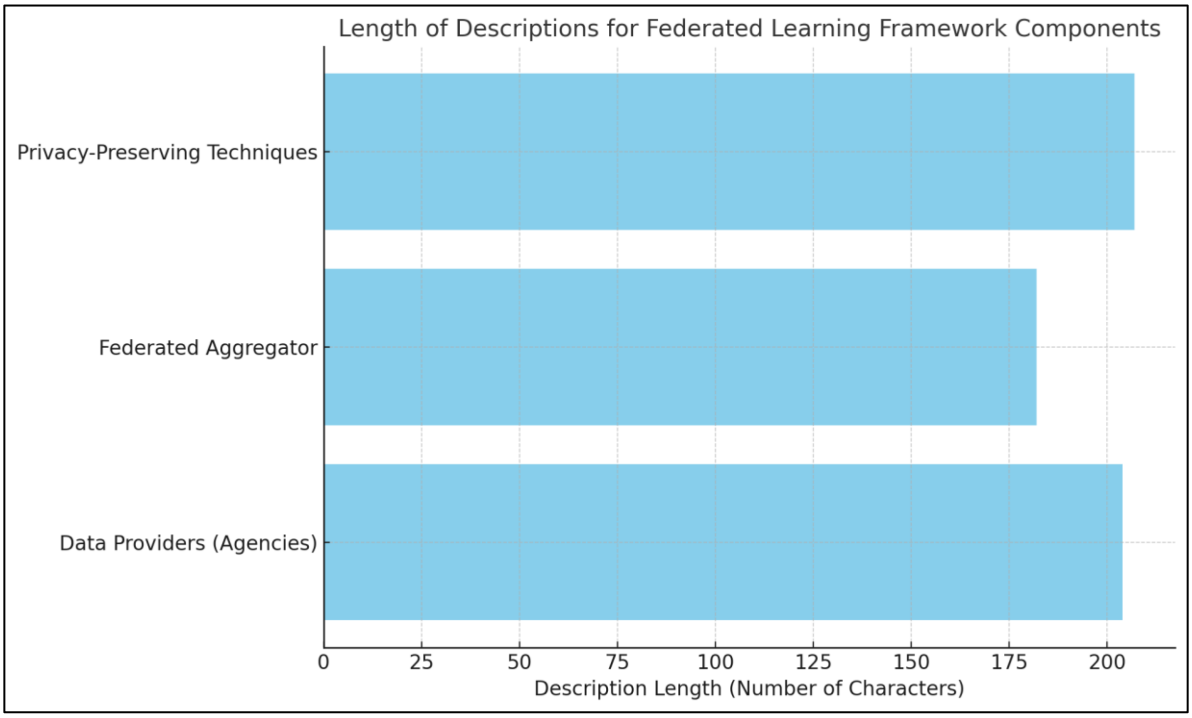

Figure 1: Length of Descriptions for Federated Learning Framework Components

B. Secure Model Aggregation

A core component of federated learning is the aggregation of local model updates into a global model. In traditional machine learning approaches, centralized aggregation of raw data could compromise privacy. In federated learning, secure aggregation protocols ensure that no individual data points are exposed during the model training process. Instead, only the aggregated model updates are shared between the participating agencies and the central aggregator. To ensure secure aggregation, we employ a combination of homomorphic encryption and secure multi-party computation (SMPC). Homomorphic encryption allows the aggregator to perform computations on encrypted model updates without needing to decrypt them, ensuring that the data remains secure at all times. This technique enables the central server to aggregate model updates from different agencies without having access to the underlying data, thereby preventing data leakage. Additionally, SMPC protocols are implemented to ensure that no agency can gain insights into the data held by another agency during the model aggregation process. The SMPC protocols work by splitting the model updates into multiple shares, which are distributed across different parties, ensuring that no single party has complete knowledge of the update. Once the shares are aggregated, the final global model update is reconstructed, preserving the privacy of the data contributors. These secure aggregation techniques are essential to ensuring that federated learning can be applied in privacy-sensitive environments like healthcare, energy, and transportation.

C. Model Evaluation

The evaluation of the federated learning framework is crucial for determining its practicality and effectiveness in real-world applications within critical infrastructure sectors. This process focuses on three primary metrics: Model Accuracy, Communication Efficiency, and Privacy Guarantees, which are essential to assess the overall performance and viability of the framework. First, Model Accuracy is evaluated by comparing the performance of the federated learning model against a baseline model trained with centralized data. The model is tested using datasets from various critical infrastructure domains, such as smart grids, healthcare, and transportation systems. Key metrics include prediction quality, the ability to generalize across different data, and robustness against noisy or incomplete data. The goal is to ensure that federated learning does not compromise model performance despite the decentralized data structure. Second, Communication Efficiency is assessed to measure the overhead caused by transmitting model updates between agencies and the central aggregator. Large and frequent model updates can increase communication costs, so we analyze the time and bandwidth needed for data transmission. To improve efficiency, the framework can reduce the frequency of updates and employ data compression techniques. Lastly, Privacy Guarantees are evaluated to ensure that the privacy-preserving mechanisms remain effective during the aggregation process. Differential privacy and secure aggregation protocols are rigorously tested using adversarial attacks and data inference simulations. The evaluation aims to confirm that sensitive data remains secure and cannot be reconstructed by attackers.

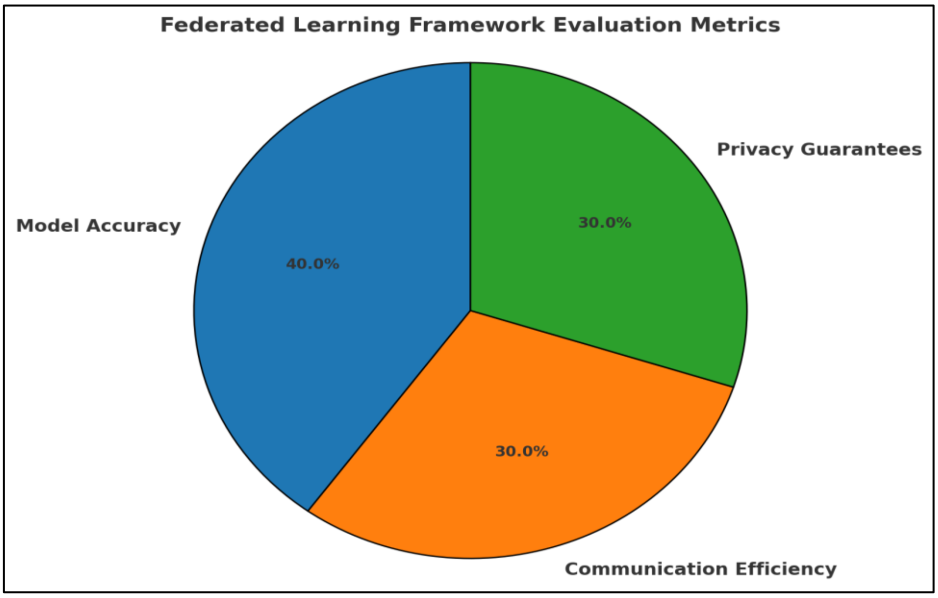

Figure 2: Federated Learning Framework Evaluation Metrics

IV. DISCUSSION AND RESULT

The federated learning framework ensures secure inter-agency collaboration without exposing sensitive data. Agencies train models locally and share only model updates with the central Federated Aggregator, which combines them into a global model using secure aggregation. Privacy-preserving techniques, including differential privacy and secure multi-party computation (SMPC), are integrated to protect data during the aggregation process. The framework's effectiveness is evaluated in terms of model accuracy, communication efficiency, and privacy guarantees. While it offers scalability and enhanced privacy compared to centralized models, challenges such as data heterogeneity and real-time decision-making in critical sectors require further optimization.

A. Privacy and Security Implications

The federated learning framework proposed in this study ensures that sensitive data is not shared between agencies, effectively safeguarding privacy. By utilizing secure aggregation and differential privacy techniques, the framework guarantees that even if an adversary intercepts the communication between agencies, private data cannot be reconstructed. These privacy-preserving mechanisms are essential for complying with stringent data protection laws, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). This makes the framework particularly suitable for high-stakes environments like healthcare, where patient confidentiality is paramount. Furthermore, the use of these techniques significantly reduces the risk of data breaches, ensuring that agencies can collaborate securely without compromising the privacy of their data. In environments where maintaining privacy is critical, the federated learning framework provides a robust solution that ensures sensitive data is protected throughout the collaboration process.

Table 1: Privacy and Security Implications

Privacy Mechanism	Description	Benefits
Secure Aggregation	Secure aggregation protocols ensure that sensitive data is never shared between agencies. Even if communication is intercepted, model updates remain secure, preventing data leakage and ensuring privacy.	Prevents data leakage during collaboration and ensures compliance with regulations like GDPR and HIPAA. Protects the privacy of sensitive data in transit.
Differential Privacy	Differential privacy adds noise to the model updates, ensuring that individual data contributions cannot be inferred. This guarantees that private information is not reconstructed, even by an adversary.	Ensures privacy by adding statistical noise to model updates. Complies with data protection laws by preventing the identification of individual contributions.

B. Scalability and Efficiency

Scalability is a crucial factor for the deployment of federated learning in critical infrastructure sectors, as these systems often involve large volumes of data and multiple distributed agencies. Our experiments indicate that while federated learning incurs some communication overhead due to the need for frequent model updates between agencies and the central aggregator, it remains significantly more efficient compared to centralized models, particularly when privacy concerns are taken into account. Centralized models require the transfer of raw data, which can expose sensitive information and lead to privacy risks. On the other hand, federated learning reduces the need for data transmission, thus lowering the risk of data exposure. However, the framework's communication efficiency still remains an area for optimization. As the number of participating agencies increases, the time and bandwidth required for aggregating model updates also increase. To enhance scalability, reducing the frequency of model updates and using more advanced compression techniques could be explored in future work. These optimizations would ensure that federated learning remains both privacy-preserving and scalable, even in large-scale, data-intensive environments.

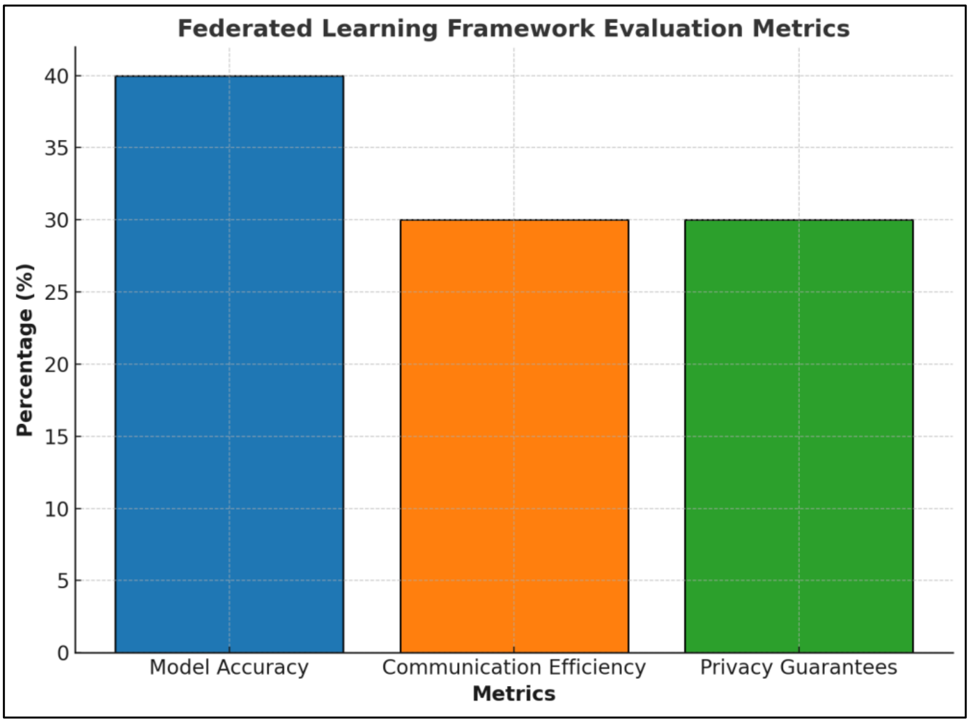

Figure 3: Federated Learning Framework Evaluation Metrics

C. Limitations

Despite the promising potential of the federated learning framework, several limitations must be addressed to fully realize its benefits. One significant challenge is the heterogeneity of data across different agencies. Each agency may use different data formats, sensors, and reporting standards, which can complicate the training and aggregation of models. The framework must account for this variation in data quality, format, and structure, which may require additional preprocessing steps or standardization techniques to ensure that model updates can be effectively aggregated. Another limitation is the real-time decision-making requirement in certain critical infrastructure sectors. Some applications, such as smart grid management or traffic control, demand low-latency responses for optimal decision-making. The decentralized nature of federated learning introduces inherent communication delays, which may impact the ability to make real-time decisions. Addressing these challenges will require further research into more efficient aggregation methods and exploring new ways to handle real-time data synchronization across distributed agencies. Ultimately, refining these aspects of the framework will enhance its suitability for large-scale deployment in environments where both privacy and efficiency are critical.

V. CONCLUSION

Federated learning offers a promising solution for secure and privacy-preserving data collaboration between agencies, particularly in critical infrastructure sectors where data sensitivity and privacy are paramount. The proposed framework allows agencies to collaboratively train machine learning models without sharing raw data, ensuring that sensitive information remains protected. By integrating techniques such as secure aggregation and differential privacy, the framework prevents potential data leakage and maintains regulatory compliance. The framework’s ability to facilitate decentralized model training while upholding stringent privacy standards is its key strength.

Future research should focus on optimizing the framework's scalability and communication efficiency to support large-scale, distributed systems. For real-time applications in critical infrastructure sectors like smart grids and transportation systems, minimizing latency and improving system responsiveness will be essential. Additionally, addressing the integration of federated learning with existing infrastructure systems will be a crucial area of exploration, ensuring that these systems can seamlessly adopt federated learning models while adhering to regulatory requirements. Furthermore, investigating more advanced privacy-preserving techniques to protect against evolving security threats is an important consideration. In conclusion, while the federated learning framework shows immense potential for secure, scalable collaboration, ongoing efforts to improve its efficiency, scalability, and integration with real-world applications will be essential for its widespread adoption across critical infrastructure domains.

REFERENCES

1. M. M. R. Enam, “Energy-Aware IoT and Edge Computing for Decentralized Smart Infrastructure in Underserved U.S. Communities,” *Preprints*, vol. 202506.2128, Jun. 2025. [Online]. Available: https://doi.org/10.20944/preprints202506.2128.v1
2. M. M. R. Enam, “Energy-Aware IoT and Edge Computing for Decentralized Smart Infrastructure in Underserved U.S. Communities,” *Preprints*, Jun. 2025. Doi: 10.20944/preprints202506.2128.v1. [Online]. Available: https://doi.org/10.20944/preprints202506.2128.v1. Licensed under CC BY 4.0.
3. S. A. Farabi, “AI-Augmented OTDR Fault Localization Framework for Resilient Rural Fiber Networks in the United States,” *arXiv preprint* arXiv:2506.03041, June 2025. [Online]. Available: https://arxiv.org/abs/2506.03041
4. S. A. Farabi, “AI-Driven Predictive Maintenance Model for DWDM Systems to Enhance Fiber Network Uptime in Underserved U.S. Regions,” *Preprints*, Jun. 2025. doi: 10.20944/preprints202506.1152.v1. [Online]. Available: https://www.preprints.org/manuscript/202506.1152/v1
5. S. A. Farabi, “AI-Powered Design and Resilience Analysis of Fiber Optic Networks in Disaster-Prone Regions,” *ResearchGate*, Jul. 5, 2025 [Online]. Available: http://dx.doi.org/10.13140/RG.2.2.12096.65287.
6. M. N. Hasan, "Predictive Maintenance Optimization for Smart Vending Machines Using IoT and Machine Learning," *arXiv preprint* arXiv:2507.02934, June, 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2507.02934
7. M. N. Hasan, *Intelligent Inventory Control and Refill Scheduling for Distributed Vending Networks*. ResearchGate, Jul. 2025. [Online]. Available: https://doi.org/10.13140/RG.2.2.32323.92967
8. M. N. Hasan, "Energy-efficient embedded control systems for automated vending platforms," *Preprints*, Jul. 2025. [Online]. Available: https://doi.org/10.20944/preprints202507.0552.v1
9. S. R. Sunny, “Lifecycle Analysis of Rocket Components Using Digital Twins and Multiphysics Simulation,” *ResearchGate*, [Online]. Available: http://dx.doi.org/10.13140/RG.2.2.20134.23362.
10. Shohanur Rahaman Sunny. “Real-Time Wind Tunnel Data Reduction Using Machine Learning and JR3 Balance Integration.” *TechRxiv.* July 24, 2025.
11. Sunny, S. R. (2025). AI-Driven Defect Prediction for Aerospace Composites Using Industry 4.0 Technologies (Preprint - v1.0, July 2025.). Zenodo. https://doi.org/10.5281/zenodo.16044460
12. Shohanur Rahaman Sunny. Edge-Based Predictive Maintenance for Subsonic Wind Tunnel Systems Using Sensor Analytics and Machine Learning. *TechRxiv.* July 31, 2025.
13. Mahmudul Hasan Mithun, Md. Faisal Bin Shaikat, Sharif Ahmed Sazzad, Masum Billah, Sadeques Salehin, Al Maksud Foysal, Arafath Jubayer, Rakibul Islam, Asif Anzum, Atiqur Rahman Sunny (2024). "Microplastics in Aquatic Ecosystems: Sources, Impacts, and Challenges for Biodiversity, Food Security, and Human Health - A Meta Analysis", Journal of Angiotherapy, 8(11),1-12,10035
14. Faisal Bin Shaikat, Rafiqul Islam, Asma Tabassum Happy, Shown Ahmed Faysal. “Optimization of Production Scheduling in Smart Manufacturing Environments Using Machine Learning Algorithms” , LHEP, Vol.2025, ISSN 2632-2714.Lett.Phys
15. Islam, R., Faysal, S. A., Shaikat, F. B., Happy, A. T., Bakchi, N., & Moniruzzaman, M. (2025). Integration of Industrial Internet of Things (IIoT) with MIS: A framework for smart factory automation. *Journal of Information Systems Engineering and Management*, *10*.
16. Happy, A. T., Hossain, M. I., Islam, R., Shohel, M. S. H., Jasem, M. M. H., Faysal, S. A., Shaikat, M. F. B., Sunny, A. R. (2024). "Enhancing Pharmacological Access and Health Outcomes in Rural Communities through Renewable Energy Integration: Implications for chronic inflammatory Disease Management", Integrative Biomedical Research (Former Journal of Angiotherapy), 8(12),1-12,10197
17. Shaikat, Faisal Bin. (2025). AI-Powered Hybrid Scheduling Algorithms for Lean Production in Small U.S. Factories. 10.13140/RG.2.2.19115.14888.
18. Shaikat, Faisal Bin. (2025). Energy-Aware Scheduling in Smart Factories Using Reinforcement Learning. 10.13140/RG.2.2.30416.83209.
19. Shaikat, Faisal Bin. (2025). Secure IIoT Data Pipeline Architecture for Real-Time Analytics in Industry 4.0 Platforms. 10.13140/RG.2.2.36498.57284.
20. Shaikat, Faisal Bin. (2025). Upskilling the American Industrial Workforce: Modular AI Toolkits for Smart Factory Roles. 10.13140/RG.2.2.29079.89769.
21. Md Faisal Bin Shaikat. Pilot Deployment of an AI-Driven Production Intelligence Platform in a Textile Assembly Line Author. *TechRxiv.* July 09, 2025.DOI: 10.36227/techrxiv.175203708.81014137/v1

22. R. Islam, S. Kabir, A. Shufian, M. S. Rabbi and M. Akteruzzaman, "Optimizing Renewable Energy Management and Demand Response with Ant Colony Optimization: A Pathway to Enhanced Grid Stability and Efficiency," *2025 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, USA, 2025, pp. 1-6, doi: 10.1109/TPEC63981.2025.10906946.
23. M. S. Rabbi, "Extremum-seeking MPPT control for Z-source inverters in grid-connected solar PV systems," *Preprints*, 2025. [Online]. Available: https://doi.org/10.20944/preprints202507.2258.v1.
24. M. S. Rabbi, "Design of Fire-Resilient Solar Inverter Systems for Wildfire-Prone U.S. Regions" *Preprints*, 2025. [Online]. Available: https://www.preprints.org/manuscript/202507.2505/v1.
25. M. S. Rabbi, "Grid Synchronization Algorithms for Intermittent Renewable Energy Sources Using AI Control Loops" *Preprints*, 2025. [Online]. Available: https://www.preprints.org/manuscript/202507.2353/v1.
26. A. A. R. Tonoy, "Mechanical properties and structural stability of semiconducting electrides: Insights for material design in mechanical applications," *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, vol. 1, no. 1, pp. 18–35, Sep. 2022. [Online]. Available:
27. A. A. R. Tonoy and M. R. Khan, "The role of semiconducting electrides in mechanical energy conversion and piezoelectric applications: A systematic literature," *Journal of Scholarly Research and Innovation*, vol. 2, no. 1, pp. 1–23, Dec. 2023. [Online]. Available:
28. M. A. Khan and A. A. R. Tonoy, "Lean Six Sigma applications in electrical equipment manufacturing: A systematic literature review," *American Journal of Interdisciplinary Studies*, vol. 5, no. 2, pp. 31–63, Dec. 2024. [Online]. Available:
29. A. A. R. Tonoy, M. Ahmed, and M. R. Khan, "Precision mechanical systems in semiconductor lithography equipment design and development," *American Journal of Advanced Technology and Engineering Solutions*, vol. 1, no. 1, pp. 71–97, Feb. 2025. [Online]. Available:
30. S. Rana, A. Bajwa, A. A. R. Tonoy, and I. Ahmed, "Cybersecurity in industrial control systems: A systematic literature review on AI-based threat detection for SCADA and IoT networks," *ASRC Procedia: Global Perspectives in Science and Scholarship*, vol. 1, no. 1, pp. 1–15, Apr. 2025. [Online]. Available:
31. A. Bajwa, A. A. R. Tonoy, and M. A. M. Khan, "IoT-enabled condition monitoring in power transformers: A proposed model," *Review of Applied Science and Technology*, vol. 4, no. 2, pp. 118–144, Jun. 2025. [Online]. Available: https://doi.org/10.63125/3me7hy81
32. A. A. R. Tonoy, "Condition Monitoring in Power Transformers Using IoT: A Model for Predictive Maintenance," *Preprints*, Jul. 28, 2025. [Online]. Available: https://doi.org/10.20944/preprints202507.2379.v1
33. A. A. R. Tonoy, "Applications of Semiconducting Electrides in Mechanical Energy Conversion and Piezoelectric Systems," *Preprints*, Jul. 28, 2025. [Online]. Available: https://doi.org/10.20944/preprints202507.2421.v1
34. Azad, M. A, "Lean Automation Strategies for Reshoring U.S. Apparel Manufacturing: A Sustainable Approach," *Preprints*, August. 01, 2025. [Online]. Available: https://doi.org/10.20944/preprints202508.0024.v1
35. Azad, M. A, "Optimizing Supply Chain Efficiency through Lean Six Sigma: Case Studies in Textile and Apparel Manufacturing," *Preprints*, August. 01, 2025. [Online]. Available: https://doi.org/10.20944/preprints202508.0013.v1
36. Md Ashraful Azad. Sustainable Manufacturing Practices in the Apparel Industry: Integrating Eco-Friendly Materials and Processes. *TechRxiv.* August 07, 2025. DOI: 10.36227/techrxiv.175459827.79551250/v1
37. Md Ashraful Azad. Leveraging Supply Chain Analytics for Real-Time Decision Making in Apparel Manufacturing. *TechRxiv.* August 07, 2025. DOI: 10.36227/techrxiv.175459831.14441929/v1
38. Md Ashraful Azad. Evaluating the Role of Lean Manufacturing in Reducing Production Costs and Enhancing Efficiency in Textile Mills. TechRxiv. August 07, 2025. DOI: 10.36227/techrxiv.175459830.02641032/v1
39. Md Ashraful Azad. Impact of Digital Technologies on Textile and Apparel Manufacturing: A Case for U.S. Reshoring. *TechRxiv.* August 07, 2025. DOI: 10.36227/techrxiv.175459829.93863272/v1
40. Rayhan, F. A, "A Hybrid Deep Learning Model for Wind and Solar Power Forecasting in Smart Grids," *Preprints*, August. 07, 2025. [Online]. Available: https://doi.org/10.20944/preprints202508.0511.v1
41. Rayhan, F. A, "AI-Powered Condition Monitoring for Solar Inverters Using Embedded Edge Devices, " *Preprints* August. 07, 2025. [Online]. Available: https://doi.org/10.20944/preprints202508.0474.v1
42. "IEEE Draft Guide for Architectural Framework and Application of Federated Machine Learning," in *IEEE P3652.1/D6, April 2020* , vol., no., pp.1-70, 1 June 2020.
43. H. Lee, M. Jiang and Q. Zhao, "FedAssist: Federated Learning in AI-Powered Prosthetics for Sustainable and Collaborative Learning," *2024 46th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Orlando, FL, USA, 2024, pp. 1-5, doi: 10.1109/EMBC53108.2024.10781961.
44. Y. Zhou, M. Shi, Y. Tian, Y. Li, Q. Ye and J. Lv, "Federated CINN Clustering for Accurate Clustered Federated Learning," *ICASSP 2024 - 2024 IEEE*

International Conference on Acoustics, Speech and Signal Processing (ICASSP), Seoul, Korea, Republic of, 2024, pp. 5590-5594, doi: 10.1109/ICASSP48485.2024.10447282.

45. "IEEE Guide for an Architectural Framework for Blockchain-Based Federated Machine Learning," in *IEEE Std 3127-2025* , vol., no., pp.1-40, 16 April 2025, doi: 10.1109/IEEESTD.2025.10965995.
46. "IEEE Draft Guide for Framework for Trustworthy Federated Machine Learning," in *IEEE P3187/D0.7, December 2023* , vol., no., pp.1-45, 7 March 2024.
47. M. Khalil, R. Shakya and Q. Liu, "Towards Privacy-Preserving Data-Driven Education: The Potential of Federated Learning," *2025 International Conference on New Trends in Computing Sciences (ICTCS)*, Amman, Jordan, 2025, pp. 113-118, doi: 10.1109/ICTCS65341.2025.10989403.
48. R. Pilkar, K. Momeni, A. Ramanujam, M. Ravi, E. Garbarini, and G. F. Forrest, “Use of surface emg in clinical rehabilitation of individuals with sci: barriers and future considerations,” *Frontiers in neurology*, vol. 11, p. 578559, 2020.
49. H. Zhou and G. Alici, “Non-invasive human-machine interface (hmi) systems with hybrid on-body sensors for controlling upper-limb prosthesis: A review,” *IEEE Sensors Journal*, vol. 22, no. 11, pp. 10 292–10 307, 2022.
50. P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings et al, “Advances and open problems in federated learning,” *Foundations and Trends® in Machine Learning*, vol. 14, no. 1-2, pp. 1–210, 2021.