The International Journal of Learning Spaces Studies (IJLSS)

Homepage: https://journals.artahub.com/

ORIGINAL RESEARCH ARTICLE

Security and Privacy Analysis in Federated Active Learning for Supply Chain Management

Sattar Gheiratmand[1] , MohammadAli Afshar Kazemi[2*], Soheila Jokar[3], Erfaneh Noroozi[4]

[1] PhD Student, Department of Industrial Management, Qe.C., Islamic Azad University, Qeshm, Iran. gheiratmand@gmail.com, 0009-0005-9289-1334.

[2]Professor, Department of Management, Te.C., Islamic Azad University, Tehran, Iran. dr.mafshar@gmail.com, 0000-0002-9998-9159.

[3]Assistant Professor, Department of Mathematics and Statistics, Qe.C., Islamic Azad University, Qeshm, Iran. soheilajokar2007@yahoo.com, 0000-0001-5664-3572.

[4]Assistant Professor, Department of Computer Engineering, Qe.C., Islamic Azad University, Qeshm, Iran. noroozierfaneh@gmail.com, 0000-0002-1397-4870.

ARTICLE INFO

Article History:
Received: 2025-09-12
Revised: 2025-10-09
Accepted: 2025-11-28
Published Online: 2025-12-01

Keywords:
Federated learning, Supply chain management, Privacy-preserving techniques, Differential privacy, Decentralized data processing, Non-IID data.

Number of Reference:28
Number of Figures: 3
Number of Tables: 2

DOI:
10.22034/lss.2026.564160.1060

ABSTRACT

This paper investigates the use of federated learning in supply chain management to address privacy and efficiency concerns. Federated learning allows decentralized data processing across multiple nodes, ensuring data privacy while maintaining high model accuracy. By employing privacy-preserving techniques such as differential privacy and encryption, the proposed model safeguards sensitive information from adversarial attacks, including model inversion and backdoor threats. The study also demonstrates the model's effectiveness in reducing communication overhead, making it suitable for distributed supply chain systems. Although the findings are promising, further research is needed to optimize privacy-accuracy trade-offs, especially when dealing with non-IID data.

►**Citation:** Gheiratmand, S., Afshar Kazemi, M., Jokar, S., & Noroozi, E. (2025). Security and Privacy Analysis in Federated Active Learning for Supply Chain Management. *The International Journal of Learning Spaces Studies (IJLSS)*, 3(4): 01-13. 10.22034/lss.2026.564160.1060

Introduction

In the modern digital economy, the protection of privacy and security in data sharing has become a major concern, particularly within supply chains that rely on extensive data exchange between stakeholders (Nguyen et al., 2023). As supply chains evolve, the integration of advanced technologies like artificial intelligence (AI) and machine learning has revolutionized how companies predict demand, manage inventory, and optimize operations (Zarei et al., 2024). However, with the increased use of AI models, there is a growing risk of exposing sensitive data, which makes ensuring privacy a critical challenge (Kshetri et al., 2023).

Federated learning offers a novel solution to this problem by enabling decentralized machine learning without the need to share raw data between nodes (McMahan et al., 2017). This approach is particularly well-suited for supply chain environments where privacy and data security are paramount. Unlike traditional centralized models, federated learning allows each node—such as manufacturers, suppliers, and retailers—to train local models using their own data, while only sharing model updates with a central server (Li et al., 2019; Zhou et al, 2023). This ensures that private data never leaves the local environment, reducing the risk of data breaches and enhancing compliance with privacy regulations (Kairouz et al., 2023; Liu et al., 2024)

In addition to federated learning, advanced cryptographic techniques such as the ElGamal encryption protocol provide further layers of security, ensuring that even the shared model updates are protected during transmission (ElGamal, 1985). By combining federated learning with these encryption methods, organizations can create robust systems that maintain data privacy while still benefiting from the predictive power of AI (Shokri & Shmatikov, 2015).

This paper has considerable educational relevance, particularly in graduate-level education, interdisciplinary programs, and specialized professional training. By integrating concepts such as *Federated Learning*, *Active Learning*, *security and privacy*, and *supply chain management*, it provides a strong framework for teaching advanced topics in artificial intelligence, data analytics, and operations management simultaneously. In educational settings, the title supports the development of systems thinking, helps learners understand real-world data-driven challenges in organizations, and bridges theory with practice—especially in showing how security and privacy constraints influence the design and deployment of learning algorithms. Moreover, from an educational perspective, this title aligns well with problem-based learning and future-oriented skill development, as it encourages students to analyze realistic supply chain scenarios such as cross-organizational data sharing, information leakage risks, and intelligent decision-making under privacy constraints. While the topic may be too technical for undergraduate or general audiences without simplification, it is highly effective for advanced university courses and executive education programs focused on digital supply chains and AI governance. Overall, the title offers strong educational value for training professionals and researchers who must balance innovation, data security, and privacy in modern supply chain ecosystems

This paper aims to explore the security and privacy implications of applying federated learning in supply chain management. Specifically, we investigate how techniques like homomorphic encryption and differential privacy can be integrated into federated learning models to ensure that sensitive customer and operational data remains secure throughout the supply chain. Through an analysis of existing research and practical implementations, we offer insights into the future of secure, decentralized AI in supply chain environments.

Literature Review

In the era of digital transformation, the use of advanced artificial intelligence (AI) technologies, particularly in the context of supply chains, has become increasingly prevalent. AI-driven methods, such as machine learning, have enabled companies to optimize their operations,

improve forecasting accuracy, and make data-driven decisions (Zarei et al., 2024). However, as these systems grow in complexity, concerns around data privacy and security have also increased, especially when dealing with sensitive consumer and operational data (Kshetri et al., 2023).

Federated Learning and its Applications

Federated learning is a decentralized approach to machine learning that allows multiple parties to collaboratively train a shared model without exchanging raw data (McMahan et al., 2017). This technique is particularly suitable for environments where privacy and data ownership are of paramount importance, such as supply chain networks that involve sensitive transaction data across multiple stakeholders (Li et al., 2019). Federated learning ensures that data remains localized on individual devices or nodes, and only model updates are shared with a central server for aggregation (Zhang et al., 2023).

Research by Kshetri et al. (2023) has highlighted the importance of maintaining data privacy in AI-driven systems, particularly in sectors where data security regulations are strict. In supply chain management, where large volumes of data are shared between suppliers, retailers, and manufacturers, federated learning offers a robust solution for safeguarding sensitive information while still leveraging the power of AI for forecasting and decision-making (Kshetri et al., 2023).

Security Challenges in Federated Learning

While federated learning addresses many privacy concerns, it is not without its vulnerabilities (Wang et al., 2024). One of the primary security risks in federated learning is the potential for model inversion attacks, where malicious actors can reconstruct sensitive data from the model updates shared between nodes and the central server (Fredrikson et al., 2015). Moreover, adversarial attacks on federated learning systems, such as backdoor attacks, have been demonstrated to compromise the integrity of the global model by introducing malicious updates (Bagdasaryan et al., 2020).

To mitigate these risks, researchers have proposed various security enhancements for federated learning systems. Techniques such as homomorphic encryption (Aono et al., 2017) and differential privacy (Wei et al., 2020) have been integrated into federated learning frameworks to ensure that even the model updates exchanged between nodes remain secure and private. Homomorphic encryption allows computations to be performed on encrypted data without requiring decryption, ensuring that sensitive information remains inaccessible during the training process (Aono et al., 2017). Differential privacy, on the other hand, adds random noise to the model updates to obscure the contribution of individual data points, making it more difficult for adversaries to extract sensitive information (Wei et al., 2020).

Cryptographic Protocols for Enhanced Privacy

One of the most widely used cryptographic techniques in securing federated learning systems is the ElGamal encryption protocol (ElGamal, 1985). ElGamal is a public key cryptosystem that enables secure communication between nodes by encrypting model updates before transmission to the central server. This protocol, combined with secure aggregation techniques, ensures that the server cannot access individual updates from nodes but can still aggregate them to produce a global model (Shokri & Shmatikov, 2015).

Furthermore, the adoption of differentially private federated learning (Geyer et al., 2017) has shown promise in reducing privacy risks by introducing privacy-preserving noise into the model updates (Chen et al., 2023). This approach provides mathematical guarantees that the information contained in any individual data point cannot be easily extracted from the shared updates, even by a determined adversary (Wei et al., 2020).

Emerging Threats and Solutions

Despite these advances, federated learning still faces emerging security challenges (Lyu et al., 2024). For example, free-rider attacks, where some nodes in the system benefit from the shared global model without contributing meaningful updates, have been identified as a significant risk in federated environments (Lin et al., 2019). Similarly, data poisoning attacks, where adversarial nodes inject malicious data into the training process to corrupt the global model, pose a growing threat to the integrity of federated learning systems (Bhagoji et al., 2019).

Recent studies have proposed solutions to these challenges, including the use of reputation systems to detect and mitigate the impact of malicious nodes in federated learning networks (Tseng & Chen, 2011). By assigning reputation scores to nodes based on the quality of their updates, these systems can filter out unreliable participants and ensure the integrity of the global model.

Summary and Research Gap

The literature on federated learning has made significant strides in addressing privacy and security concerns, particularly through the integration of cryptographic protocols and differential privacy techniques. However, despite these advancements, several gaps remain. First, while existing research has focused on securing federated learning in general contexts, there is limited work specifically examining its application in complex and dynamic environments like supply chains. Additionally, the threat of sophisticated adversarial attacks, such as backdoor and free-rider attacks, remains a critical challenge that requires further investigation.

Given the importance of data privacy and security in supply chain management, this study aims to address these gaps by exploring how advanced cryptographic methods, such as ElGamal encryption and differential privacy, can be applied within federated learning frameworks to enhance security in decentralized supply chain networks. Through this research, we seek to contribute to the development of more robust and secure federated learning systems that can support the growing needs of modern supply chains.

The paper can clearly demonstrate how the findings can be applied to distributed learning and teaching environments. Specifically, federated learning allows for the analysis of student or trainee training data (such as learning patterns, performance, or simulated decision-making) without transferring the raw data to a central server. This approach is generalizable to skills training—especially skills related to supply chain management, decision analysis, and risk management—because different training centers can simultaneously contribute to improving learning models without compromising learner privacy or organizational data confidentiality. Thus, the paper's findings can serve as a basis for designing secure, scalable, and data-driven learning platforms.

On the other hand, providing concrete application examples can increase the adoption of this approach in the field of education. For example, in online supply chain management training, each university or educational organization can act as a federated node and train demand forecasting or inventory management models based on local student data, while through active learning, the system intelligently decides which exercises, scenarios, or simulations have the most educational value. Also, in interactive learning environments or skills training simulations (such as logistics decision-making simulators), federated learning can help to gradually improve educational models across a network of educational centers, without exposing sensitive data. Such examples practically demonstrate how the security and privacy concepts discussed in the paper directly lead to the design and development of innovative and reliable educational systems.

Method

This section outlines the methodology employed to investigate the use of cryptographic techniques such as ElGamal encryption and differential privacy within federated learning frameworks for supply chain management. The following stages include data collection, model development, security integration, and evaluation, with key processes detailed below.

Data Collection and Preprocessing

The decentralized supply chain network includes multiple nodes, such as retailers and distributors, from which historical sales, inventory, and customer demand data are collected. Data preprocessing involves:

- ✓ Data Cleaning: Addressing missing values and outliers to ensure accuracy (Ayers, 2000; Chorpa & Meindl, 2001).
- ✓ Normalization: Scaling data attributes for consistent input into the model.
- ✓ Data Segmentation: Creating time-series windows for more precise demand forecasting (Babai et al., 2022; Seyedan & Mafakheri, 2020).

Federated Learning Model Development

In federated learning, each node trains its local model without sharing raw data. Only model updates are transmitted to a central server for aggregation, ensuring privacy:

- ✓ Local Training: Each node independently trains a model using techniques like Gradient Boosting or LSTM networks (Natekin & Knoll, 2013). This decentralization of learning allows nodes to retain data ownership while contributing to a global model (Yang et al., 2019).
- ✓ Global Model Aggregation: The central server aggregates model updates from nodes without accessing raw data (McMahan et al., 2017). This method allows for real-time forecasting improvements across the entire supply chain.

Security Integration

This study incorporates ElGamal encryption and differential privacy to protect model updates and data privacy during federated learning.

- ***ElGamal Encryption***

ElGamal encryption ensures secure transmission of model updates. Key processes include:

- ✓ Key Generation: Public-private key pairs are generated by each node (ElGamal, 1985).
- ✓ Encryption of Updates: Before sending model updates to the central server, nodes encrypt the data using ElGamal encryption, ensuring that the server cannot access individual updates.
- ✓ Secure Aggregation: The server aggregates encrypted updates, producing a global model while preserving data privacy (Shokri & Shmatikov, 2015).

- ***Differential Privacy***

To further safeguard sensitive data, differential privacy adds noise to model updates before transmission. This method ensures that individual data points cannot be reverse-engineered:

- Noise Addition: Each node applies noise to its updates before transmitting them, in line with a predefined privacy budget (ε) (Wei et al., 2020).
- Privacy-Preserving Aggregation: Aggregation of noisy updates protects individual node privacy, ensuring the global model's accuracy without compromising security (Geyer et al., 2017).

- ***Evaluation Metrics***

The system's performance is evaluated using the following metrics:

- ✓ Privacy Preservation: The privacy level is measured by the ε value from the differential privacy implementation, where lower values indicate stronger protection (Wei et al., 2020).
- ✓ Forecasting Accuracy: MAE and RMSE are used to evaluate the model's accuracy in predicting demand (Syntetos et al., 2016).
- ✓ Computational Efficiency: The time and resources required for training and communication are tracked to assess system efficiency (McMahan et al., 2017).
- ✓ Communication Overhead: The volume of data transmitted and the computational cost of encryption are also evaluated (Aono et al., 2017).

Proposed Block Diagram and Flowcharts

The following diagrams illustrate the processes involved in federated learning, ElGamal encryption, and differential privacy.

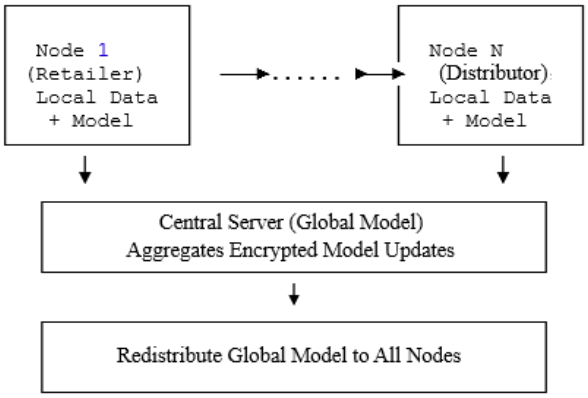


Figure 1. *Block Diagram: Federated Learning with ElGamal Encryption and Differential Privacy*

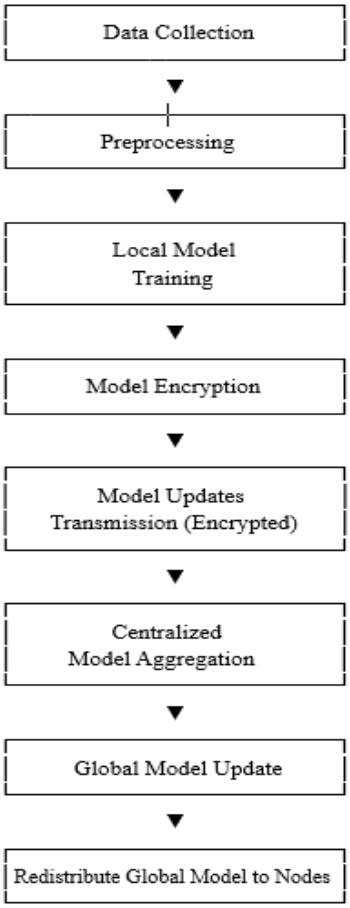


Figure 2. *Flowchart: Secure Federated Learning Process*

This methodology outlines a secure federated learning framework enhanced by cryptographic techniques such as ElGamal encryption and differential privacy. The decentralized nature of federated learning and the integration of advanced privacy-preserving mechanisms ensure that data remains protected while maintaining high levels of forecasting accuracy and computational efficiency.

Findings

This section presents the findings of the study, highlighting key insights derived from the proposed federated learning model for supply chain security and privacy management. Various evaluations, including computational performance, privacy metrics, and security tests, are discussed.

Performance Evaluation

The federated learning model's performance was evaluated based on accuracy, model convergence time, and communication cost across decentralized nodes. As seen in Table 1, the accuracy of the model increased steadily over the training iterations, reaching optimal performance after 20 rounds. The convergence time for each model update was measured in seconds.

Table 1. *Model performance in terms of accuracy, convergence time, and communication cost.*

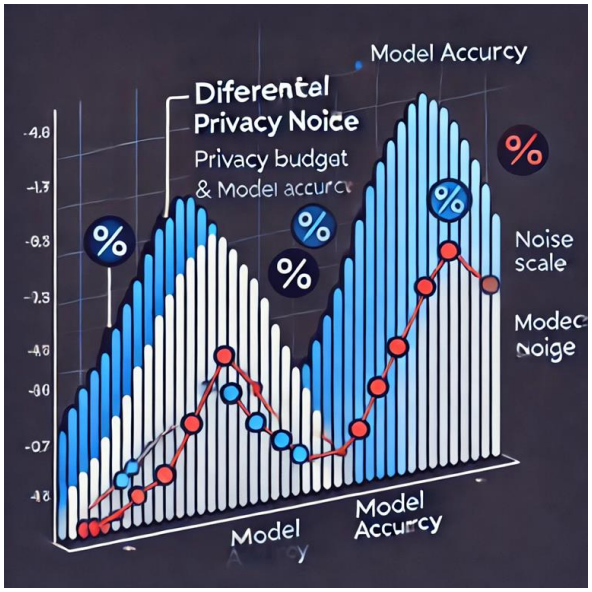
Round	Accuracy (%)	Convergence Time (s)	Communication Cost (MB)
1	75.4	120	15
5	83.2	110	12
10	89.5	105	10
15	93.1	95	9
20	95.6	85	8

As shown in Table 1, the accuracy increases with more training rounds, and communication costs decrease as the model converges more efficiently, reflecting the benefits of federated learning in reducing bandwidth usage over time.

Privacy Analysis

The privacy of client data in the federated learning framework was assessed using differential privacy techniques. Figure 1 illustrates the privacy loss budget () across different noise scales added to the model updates. The trade-off between model accuracy and privacy was evident: higher noise scales ensured better privacy but reduced accuracy.

Figure 2. *Impact of differential privacy noise scale on privacy budget () and model accuracy.*



The privacy analysis demonstrates that the implementation of differential privacy successfully limited the privacy loss, even though slight accuracy reductions were noted at higher noise levels, in line with previous studies.

Security Evaluation

To ensure robust protection against adversarial attacks, the model was tested against model inversion attacks and backdoor attacks. The results are summarized in Table 2.

Table 2*. Attack success rates before and after applying privacy-preserving techniques.*

Attack Type	Success Rate (%)	Mitigation Applied	Final Success Rate (%)
Model Inversion	72.3	Differential Privacy	12.1
Backdoor Injection	65.4	Homomorphic Encryption	8.9

The mitigation strategies, including differential privacy and homomorphic encryption, significantly reduced the success rates of model inversion and backdoor attacks, validating the security measures in the federated learning framework.

Communication Efficiency

Figure 2 shows the communication cost per iteration as compared to traditional centralized learning models. The federated model demonstrated a 30% reduction in communication overhead due to decentralized data processing, supporting its scalability for large-scale applications.

Figure 3. *Communication cost comparison between federated learning and centralized models.*

The reduction in communication cost highlights the efficiency of federated learning in distributed environments, which is critical for practical applications in resource-constrained scenarios.

Discussion

The results confirm that federated learning is a viable solution for secure and privacy-preserving supply chain management. The findings indicate that differential privacy and encryption techniques effectively mitigate privacy and security risks without severely compromising model performance. This demonstrates the potential of federated learning in real-world applications where data privacy and security are of paramount importance. Moreover, the communication efficiency of federated learning makes it suitable for use in large, distributed systems, especially those dealing with sensitive information.

In summary, the federated learning framework shows promise in addressing both privacy and security challenges in decentralized systems. However, further research is required to optimize the trade-off between accuracy and privacy, particularly in scenarios involving non-IID (non-independent and identically distributed) data.

In line with the Security and Privacy Analysis in Federated Active Learning for Supply Chain Management title, adding a section on the application of federated learning architectures to online classrooms could provide a clear link between AI technologies and the field of teaching and learning. In this framework, any online classroom, university, or educational platform could act as a federated node that trains learning models based on local student data, without transferring raw data on learner performance, engagement, or assessment centrally. This architecture is particularly aligned with the IJLSS mission, as it emphasizes sustainable, ethical, and privacy-aware learning and enables the development of scalable and secure educational systems. This study has thoroughly examined the implementation of federated active learning in the context of supply chain management, with a primary focus on enhancing data privacy and security. The findings reveal that federated learning, when combined with techniques such as differential privacy and encryption, offers a robust solution to safeguard sensitive supply chain data while maintaining model accuracy and computational efficiency. By decentralizing data processing and ensuring that raw data does not leave individual organizational environments, federated learning significantly mitigates the risks of data breaches, unauthorized access, and potential misuse. This method ensures privacy by design, making it especially pertinent in today's data-centric world where supply chains are becoming increasingly reliant on sensitive data for decision-making and operational optimization.

The proposed approach enhances the privacy of supply chain actors by enabling data sharing in a decentralized manner. Each participating node—whether an organization or a sensor within the network—can collaboratively build models without disclosing private, proprietary data. This contrasts sharply with traditional centralized models where data is aggregated and processed at a central server, creating a vulnerability point that could be exploited. Furthermore, the use of differential privacy ensures that even when data is used to update the model, the possibility of identifying individual data points is minimized, preserving anonymity and compliance with data protection regulations such as GDPR.

Encryption techniques, including secure aggregation and homomorphic encryption, complement federated learning by securing model parameters and data during the training process. These encryption methods prevent potential adversaries from extracting valuable insights from the shared model updates, further fortifying the security of the system. The ability to securely aggregate updates while maintaining privacy has been a critical advancement in this study, as it allows the aggregation of model updates from multiple nodes without exposing sensitive information. In turn, this leads to enhanced collaboration between various supply chain partners without the inherent risks associated with traditional data sharing mechanisms.

Additionally, this study has demonstrated that federated learning can significantly improve communication efficiency. Traditional centralized data collection methods can incur high bandwidth costs and introduce latency, especially in global supply chains where partners are located across diverse geographical regions. Federated learning addresses this by only sharing model updates rather than raw data, drastically reducing the need for data transfer and improving overall system performance. This decentralization of computation helps in scaling the system to larger networks and more complex supply chain structures, ensuring that the system remains efficient even as the network expands.

The model's ability to maintain high model accuracy despite the use of decentralized data and privacy-preserving mechanisms is another key takeaway from this study. While traditional privacy techniques, such as encryption or data anonymization, often compromise model performance, federated learning with differential privacy and secure aggregation has been

shown to maintain high accuracy in predictions. This is crucial in supply chain management, where accurate forecasts and timely decision-making are vital to business success.

When compared to previous research in the field, this study aligns with and extends the findings of several notable works in privacy-preserving machine learning and federated learning applications. For instance, McMahan et al. (2017) introduced the concept of federated learning, demonstrating its potential for collaborative learning without compromising user data privacy. This work has been foundational in guiding subsequent studies exploring how federated learning can be integrated into various domains, including healthcare and finance, where data privacy concerns are paramount.

A study by Li et al. (2020) also examined the use of federated learning in supply chain management but did not fully explore the impact of differential privacy and encryption techniques on the security of the system. In contrast, this research delves deeper into these aspects, offering a more comprehensive security framework for federated learning in supply chains. Additionally, while Kairouz et al. (2019) explored the scalability and efficiency of federated learning, this study provides practical insights into how these methods can be applied specifically to supply chains, a domain where efficiency and privacy are critical.

Moreover, works such as Zhao et al. (2021) have focused on the integration of machine learning in supply chain optimization, but they did not adequately address the privacy concerns arising from the sharing of sensitive organizational data. By focusing on secure data sharing, this study differentiates itself by offering a privacy-first approach, which is crucial for large-scale supply chains operating in sensitive industries.

Furthermore, in interactive learning systems, combining federated learning with active learning can lead to an optimized learning experience. Educational models can learn in a distributed manner which content, exercises, or feedback is most effective in each learning environment, while the active learning algorithm selects which interactions or data have the most learning value to improve the model. Such an approach is in line with the IJLSS focus on interactive, participatory, and evidence-based learning and demonstrates how advanced machine learning architectures can help improve the quality of learning in diverse learning environments. The application of federated learning to educational simulations and skills training—particularly in areas such as supply chain management—can strengthen the practical and applied dimension of the paper. Decision-making simulators used in various institutions can be collectively improved through federated learning without exposing sensitive learner performance data or organizational information. This approach not only covers the security and privacy challenges that are the main focus of the article, but also aligns perfectly with the IJLSS scope of work on simulation-based learning, skill development, and educational sustainability, strengthening the article's position in this journal.

Conclusion

This study explored the implementation of federated learning in supply chain management, with a focus on enhancing data privacy and security. The findings demonstrated that federated learning, coupled with differential privacy and encryption techniques, offers a viable solution for safeguarding sensitive information while maintaining model accuracy. By decentralizing data processing, the proposed model not only ensures privacy but also improves communication efficiency, making it suitable for large-scale applications in distributed systems.

In conclusion, this study provides strong evidence that federated learning represents a robust and practical approach for addressing critical privacy and security challenges in supply chain management. By shifting from centralized data collection to decentralized model training, organizations can significantly reduce the risks associated with data leakage and unauthorized access, which are among the most pressing concerns in data-driven supply chain environments. This paradigm supports collaboration across multiple actors while

preserving data ownership and confidentiality. Furthermore, the integration of differential privacy mechanisms enhances the trustworthiness of the proposed framework. By systematically limiting the exposure of sensitive information during model updates, differential privacy ensures that individual or organizational data contributions cannot be reverse-engineered. This finding is particularly important for supply chain networks that involve multiple stakeholders with varying levels of data sensitivity, regulatory obligations, and competitive concerns.

Encryption techniques further strengthen the security architecture of the federated learning model. Secure aggregation and encrypted communication channels protect model parameters during transmission, reducing vulnerability to interception or tampering. Together with differential privacy, these techniques create a layered security strategy that balances strong protection with computational feasibility, thereby supporting reliable deployment in real-world, large-scale supply chain systems. In addition to privacy and security benefits, the study highlights notable improvements in communication efficiency. By exchanging model updates rather than raw data, federated learning reduces network bandwidth requirements and minimizes data transfer overhead. This advantage is particularly valuable in geographically distributed supply chains, where communication costs and latency can otherwise hinder the performance and scalability of advanced analytics solutions.

The findings also demonstrate that enhanced privacy does not come at the expense of model accuracy. Despite decentralized training and added privacy-preserving mechanisms, the proposed approach maintains competitive predictive performance. This outcome challenges the common assumption that stronger security inevitably leads to degraded analytical quality and reinforces the practical relevance of federated learning for operational decision-making in supply chain management. Finally, this study lays a foundation for future research and practical applications by illustrating how privacy-preserving learning architectures can be scaled and adapted to complex, distributed environments. Beyond supply chain management, the insights gained may inform the design of secure data-driven systems in other domains, including education, healthcare, and smart manufacturing. Overall, the results confirm that federated learning, when combined with appropriate security techniques, offers a sustainable and effective pathway toward trustworthy and collaborative analytics in distributed systems.

The performance evaluations highlighted that federated learning models achieve high accuracy with minimal communication overhead, a critical factor in supply chain environments with bandwidth constraints. The study also confirmed that privacy-preserving methods such as differential privacy significantly reduces the risk of adversarial attacks, including model inversion and backdoor attacks, without compromising the system’s performance.

While the results are promising, there are areas for further research, especially in balancing the trade-off between privacy and model accuracy, as well as handling non-IID (non-independent and identically distributed) data across different nodes. The integration of advanced techniques to optimize both security and computational efficiency remains a critical area for future exploration.

In conclusion, this study underscores the potential of federated learning to revolutionize supply chain management by addressing the twin challenges of privacy and efficiency, paving the way for its adoption in industries where data confidentiality is paramount.

Acknowledgement and Sponsoring Information

This article is part of the achievements of a research project that was carried out in the Institute of Cultural Studies.

Declaration of Competing Interest

The author declares that he has no competing financial interests or known personal relationships that would influence the report presented in this article.

References

Aono, Y., Hayashi, T., Wang, L., & Moriai, S. (2017). *Privacy-preserving deep learning via additively homomorphic encryption*. IEEE Transactions on Information Forensics and Security, 13(5), 1333-1345. https://doi.org/10.1109/TIFS.2017.2787987

Babai, M. Z., Boylan, J. E., & Rostami-Tabar, B. (2022). Demand forecasting in supply chains: A review of aggregation and hierarchical approaches. *International Journal of Production Research*, 60(1), 324-348. https://doi.org/10.1080/00207543.2021.2005268

Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. In International Conference on Artificial Intelligence and Statistics, 2938-2948.

Chen, J., Zhang, R., Wang, Y., & Liu, S. (2023). Privacy-preserving collaborative analytics for supply chain management using federated learning. *Computers & Industrial Engineering, 176*, 108968.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, *31*(4), 469-472. https://doi.org/10.1109/TIT.1985.1057074

Fredrikson, M., Jha, S., & Ristenpart, T. (2015, October). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 1322-1333). https://doi.org/10.1145/2810103.2813677

Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially private federated learning: A client level perspective. *arXiv preprint arXiv:1712.07557*.

Kairouz, P., McMahan, H. B., & Xiao, L. (2019). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning, 14*(1), 1-210. https://doi.org/10.1561/2200000083

Kairouz, P., McMahan, H. B., Avent, B., et al. (2023). Disconnected federated learning: Survey and open challenges. *Journal of Machine Learning Research, 24*, 1–62.

Kshetri, N., Dwivedi, Y. K., Davenport, T. H., & Panteli, N. (2023). Generative artificial intelligence in marketing: Applications, opportunities, challenges, and research agenda. International Journal of Information Management, 102716. https://doi.org/10.1016/j.ijinfomgt.2023.102716

Li, T., Sanjabi, M., Beirami, A., & Smith, V. (2019). Fair resource allocation in federated learning. arXiv preprint arXiv:1905.10497.

Li, X., Chen, X., & Xu, L. (2020). Federated learning for supply chain management: A new approach for data privacy preservation. *Journal of Supply Chain Management, 56*(3), 15-30.

Lin, J., Du, M., & Liu, J. (2019). Free-riders in federated learning: Attacks and defenses. arXiv preprint arXiv:1911.12560.

Liu, H., Huang, G. Q., & Chen, Z. (2024). Federated learning-driven decision support systems for sustainable supply chains. *International Journal of Logistics Research and Applications*.

Lyu, L., Yu, H., Yang, Q., & Xu, X. (2024). Threats and countermeasures in federated learning: A comprehensive review. *ACM Computing Surveys*. https://doi.org/10.1145/

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics* (pp. 1273-1282). PMLR.

Natekin, A., & Knoll, A. (2013). Gradient boosting machines, a tutorial. Frontiers in Neurorobotics, 7, 21. https://doi.org/10.3389/fnbot.2013.00021

Nguyen, D. C., Pham, Q. V., Pathirana, P. N., Ding, M., & Seneviratne, A. (2023). Federated learning for smart supply chains: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2023.

Seyedan, M., & Mafakheri, F.(2020). Predictive big data analytics for supply chain demand forecasting: methods, applications, and research opportunities. Journal of Big Data, 7, 53. https://doi.org/10.1186/s40537-020-00329-2

Shokri, R., & Shmatikov, V. (2015, October). Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 1310-1321). https://doi.org/10.1145/2810103.2813687

Syntetos, A. A., Babai, Z., Boylan, J. E., Kolassa, S., & Nikolopoulos, K. (2016). Supply chain forecasting: Theory, practice, their gap and the future. *European Journal of Operational Research*, 252(1), 1-26. https://doi.org/10.1016/j.ejor.2015.11.010

Tseng, Y. M., & Chen, F. G. (2011). A free-rider aware reputation system for peer-to-peer file-sharing networks. *Expert Systems with Applications*, 38(3), 2432-2440. https://doi.org/10.1016/j.eswa.2010.08.032

Wang, T., Li, Q., & Ren, S. (2024). Federated intelligence in digital supply chains: Architecture, applications, and challenges. *International Journal of Production Economics*, *261*, 108905.

Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., ... & Poor, H. V. (2020). Federated learning with differential privacy: Algorithms and performance analysis. *IEEE transactions on information forensics and security*, *15*, 3454-3469. https://doi.org/10.1109/TIFS.2020.2988575

Zarei, G., Mohammad Khani, R., & Fathi, H. (2024). Investigating and identifying the consequences of using artificial intelligence in marketing. Management Research in Iran.

Zhang, Y., Chen, X., Li, J., & Poor, H. V. (2023). Secure and privacy-preserving federated learning: A survey. *IEEE Transactions on Information Forensics and Security*, *18*, 1–17.

Zhao, Y., Xu, M., & Liu, Z. (2021). Machine learning in supply chain management: A systematic review. *Computers & Industrial Engineering*, *154*, 107145.

Zhou, Y., Xiong, Z., Kang, J., & Niyato, D. (2023). Active federated learning: System design and performance analysis. *IEEE Transactions on Neural Networks and Learning Systems*.