SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Privacy-Preserving Cyber Threat Detection in Distributed IoT Networks

Amit Gupta[1], Anil Mandloi[2], Bhanu Pratap Singh[3]

[1]Independent Researcher, Omaha, NE, USA. E-Mail: mail2guptaamit@gmail.com
[2]Independent Researcher, Phoenix, AZ, USA. E-mail: anil.mandloi@gmail.com
[3]Independent Researcher Chicago, IL, USA. E-mail: retailtechnologist@outlook.com

Abstract
This study aims to examine the applicability of federated learning as a privacy-preserving approach for cyber-threat detection in distributed Internet of Things (IoT) networks. The study addresses the need for collaborative security analysis without requiring participating clients to transfer their raw network data to a centralized repository. The study examines the reported effectiveness of federated learning across distributed IoT clients and the influence of different model aggregation strategies on threat-detection performance. It also considers the performance relationship between federated and centralized learning approaches. The analyzed findings indicate that federated learning can provide consistent cyber-threat detection across participating clients. The reported results show that the aggregated federated model provides competitive classification performance compared with centralized learning. Analysis of the reported results for FedAvg, FedAvgM, FedAdam, and FedAdagrad further indicates that the aggregation strategy affects the performance of the resulting global model. The analyzed results indicate that federated learning can maintain effective detection capability despite the decentralized distribution of training data. The study concludes that federated learning represents a promising approach for privacy-aware cybersecurity in distributed IoT environments. By retaining training data at participating clients and exchanging model updates, the approach can support collaborative threat detection while reducing direct exposure of raw network information. Future research should investigate real-world heterogeneous IoT environments, stronger privacy mechanisms, communication efficiency, and explainable federated security models.

Keywords: Cyber-threat detection, Federated learning, Internet of things, Intrusion detection, Privacy preservation

1. Introduction

The rapid expansion of Internet of Things (IoT) technologies has created highly interconnected environments in which devices continuously generate, process, and exchange information. Although this connectivity supports automation, monitoring, and intelligent services, it also increases the potential exposure of IoT infrastructures to cyber threats. The heterogeneous nature of IoT devices, distributed deployment structures, resource limitations, and differences in security capabilities make effective intrusion detection particularly challenging. Machine-learning-based intrusion detection has therefore become an important approach for identifying abnormal and malicious network activities. However, conventional centralized learning requires data from distributed devices to be transferred to a common location, which can introduce privacy concerns and increase communication and data-management requirements. Federated Learning (FL) provides an alternative by allowing multiple participants to collaboratively develop a shared model while retaining their data locally. This characteristic has made FL increasingly relevant to privacy-preserving IoT cybersecurity.

Cyber-threat detection in distributed IoT networks requires accurate machine-learning models while also addressing the privacy implications of collecting security-related data from multiple devices or network domains. In a centralized architecture, raw network observations are commonly transferred to a central server for model development. Such data concentration may expose sensitive information and create additional communication and storage requirements. These challenges become more significant when participating organizations or IoT entities have independent data ownership and cannot directly exchange their security information. Federated approaches have consequently been investigated for different cybersecurity tasks, including intrusion detection, DDoS detection, botnet identification, and cyber-threat intelligence. Nevertheless, model performance can be influenced by differences in local datasets, aggregation mechanisms, network conditions, and client participation. Developing effective privacy-preserving detection mechanisms for distributed IoT environments therefore remains an important research problem.

Existing research demonstrates growing interest in applying FL to privacy-preserving cybersecurity. Alazab et al. (2023) investigated federated learning for privacy-preserving intrusion detection, highlighting the potential of collaborative model development without conventional centralized data sharing. Almeida et al. (2024) examined privacy-preserving intrusion detection in IoT environments using FL, while Al Amro (2025) investigated FL as a distributed approach for protecting IoT devices against intrusion activities. Research has also considered specific cyber threats and specialized network environments. Bhatia et al. (2024) investigated privacy-preserving DDoS detection in IoT networks, while Hossain and Islam (2025) examined decentralized botnet attack detection. Mahmud et al. (2024) developed a privacy-preserving FL-based intrusion-detection approach for cyber-physical systems. These studies demonstrate that decentralized learning can support collaborative cybersecurity while reducing the requirement for direct exchange of raw security data.

Several studies have combined FL with additional security and communication technologies. Abou El Houda et al. (2023) proposed a collaborative network attack mitigation framework that combined federated learning with software-defined networking and blockchain. Awan et al. (2023) investigated privacy-preserving big-data security for IoT through FL and cryptographic techniques. Moulahi et al. (2023) examined privacy-preserving cyber-threat detection for intelligent transportation systems using FL together with blockchain-based security. Bukhari et al. (2024) investigated a federated intrusion-detection approach incorporating SCNN-Bi-LSTM for wireless sensor networks. Nandanwar and Katarya (2024) similarly examined a secure and privacy-preserving IoT intrusion-detection system based on hybrid blockchain and federated learning. Rabieinejad et al. (2024) proposed a two-level privacy-preserving framework for attack detection in consumer IoT. Collectively, these investigations show that FL can be integrated with complementary security mechanisms to address privacy and trust requirements in distributed environments.

Recent research has expanded the application of privacy-preserving FL to larger and more specialized cybersecurity scenarios. Gutti et al. (2025) investigated federated learning for distributed IoT security and intrusion detection, emphasizing its potential for scalable cybersecurity. Khraisat et al. (2025) examined FL as a privacy-preserving strategy for intrusion detection in IoT environments. Aramide (2025) considered FL for distributed network security and threat intelligence, while Mrabet (2025) proposed a trust-aware federated framework for cyber-threat intelligence sharing across distributed organizations. Ragab et al. (2025) investigated an FL framework for privacy-preserving cyber-threat detection in IoT-assisted smart-city environments. Rahmati and Pagano (2025) examined an FL-driven cybersecurity framework for IoT networks with privacy-preserving and real-time threat-detection capabilities. Alaskar et al. (2026) further investigated a big-data-driven FL model for scalable and privacy-preserving cyber-threat detection in IoT-enabled healthcare systems, while Mankotia et al. (2026) examined privacy-preserving federated learning for collaborative network intrusion detection in IoT. These studies indicate that privacy-preserving FL continues to develop across different IoT, cyber-physical, organizational, and smart-system contexts.

Federated Learning enables participating clients to train a shared machine-learning model using locally available data while transmitting model information rather than the underlying raw observations. This decentralized structure is particularly relevant to IoT environments because data may be generated across numerous devices, network segments, or organizations with different ownership and privacy requirements. The approach can reduce the need to establish a centralized repository containing sensitive network observations while enabling participants to contribute to a common detection model. Research has demonstrated the application of FL to intrusion detection, DDoS detection, botnet identification, cyber-threat intelligence, and other distributed security tasks. Nevertheless, privacy preservation does not automatically eliminate all security challenges because federated systems may still be affected by client heterogeneity, communication requirements, malicious participants, model-update vulnerabilities, and differences in local data distributions (Hossain and Islam, 2025). Consequently, evaluating both detection performance and the characteristics of distributed learning is necessary when assessing FL for IoT cybersecurity.

Although the existing literature provides substantial evidence supporting federated learning for privacy-preserving cybersecurity, several gaps remain. Previous investigations differ considerably in their datasets, model architectures, client configurations, aggregation strategies, privacy mechanisms, and evaluation procedures, which makes direct comparison between reported findings difficult. Some studies concentrate on particular attack categories, while others address broader intrusion detection or specialized application environments such as healthcare, transportation, wireless sensor networks, and smart cities. Furthermore, there is a need to examine the relationship between individual client performance, global federated performance, aggregation strategy, and centralized learning within a consistent experimental framework. A comparative evaluation can provide clearer evidence regarding the extent to which federated learning can maintain effective cyber-threat detection while retaining the decentralized handling of IoT data. Addressing this gap is important for developing practical AI-based cybersecurity approaches that balance predictive effectiveness with privacy requirements.

The aim of this study is to evaluate a privacy-preserving federated-learning approach for cyber-threat detection in distributed IoT networks. Specifically, the study aims to assess the effectiveness of federated learning in detecting cyber threats across distributed IoT clients and to compare different federated aggregation strategies with centralized learning in terms of cyber-threat detection performance.

2. Materials and Methods

2.1 Research Design

This study adopted a quantitative, secondary-data-based research design to examine the application of federated learning for cyber-threat detection in distributed IoT environments. The ToN_IoT dataset was used as the secondary data source because it contains network and system observations representing normal and malicious activities in IoT and industrial IoT environments. The published findings were used as the basis for evaluating federated learning performance and comparing it with centralized learning in the present analysis.

2.2 Data Preprocessing

The dataset preparation process was considered to improve consistency and reduce potential sources of classification error. The preprocessing procedure involved examining the records for missing values, duplicate observations, inconsistent entries, and unsuitable attributes. Categorical variables were converted into numerical representations, while numerical attributes were transformed where necessary to provide an appropriate input format for machine-learning algorithms. Features that were irrelevant to the prediction task or could introduce information leakage were excluded. Feature engineering focused on retaining characteristics capable of distinguishing legitimate network behavior from malicious activity. The preprocessing procedures were applied consistently across the participating datasets to maintain comparable conditions for the distributed learning analysis.

2.3 Distributed IoT Client Configuration

The processed observations were distributed among four participating clients representing independent IoT network entities. Each client retained its allocated training observations locally and used them to train the threat-detection model without transferring the underlying records to other participants. Following local training, model information was exchanged with the coordinating server for aggregation. The client-based configuration was designed to reproduce the decentralized nature of IoT environments in which devices and network segments may operate under separate data-ownership conditions. Maintaining separate datasets at the client level also enabled the analysis to examine whether collaborative learning could yield useful threat-detection knowledge without requiring direct access to the raw observations held by individual participants.

2.4 Federated Learning Framework

The federated learning framework consisted of local training, model-update transmission, server-side aggregation, and subsequent distribution of the updated global model. During each communication round, participating clients trained the threat-detection model using their locally available data. The resulting model updates were transmitted to the aggregation server rather than the original observations. The server combined the received updates to construct a global model, which was subsequently made available for further local training. The aggregation strategies evaluated included FedAvg, FedAvgM, FedAdam, and FedAdagrad to examine their influence on detection performance. The framework supported collaborative identification of malicious and legitimate IoT network activity.

2.5 Experimental Setup

The experimental evaluation was based on separating training observations from data used for independent performance assessment. Local models were trained using client-specific observations, while the aggregated global model was evaluated using the designated testing data. Model performance was assessed using accuracy, precision, recall, and F1-score to provide complementary measures of classification effectiveness. Accuracy measured the overall proportion of correctly classified observations, while precision indicated the reliability of positive threat predictions. Recall represented the ability to identify malicious observations, and the F1-score provided a combined measure of precision and recall. Confusion matrices were additionally considered to examine classification errors and distinguish different types of incorrect predictions.

2.6 Centralized–Federated Comparison

A centralized learning configuration was included as a baseline for evaluating the predictive differences associated with decentralized training. Under the centralized arrangement, the available training observations

were combined before model development, whereas the federated configuration maintained client-level data separation during local training. Both approaches were assessed using the same principal performance measures to support a consistent comparison. The privacy assessment focused on the handling of raw IoT observations and the information exchanged during collaborative training. Federated learning was considered from the perspective of retaining raw observations at participating clients while sharing model updates for aggregation. Communication rounds and update exchanges were also considered when interpreting the practical implications of the distributed framework.

3. Results

3.1 Performance of Individual Federated Clients

The analysis examined federated learning performance across four distributed IoT clients. The ToN_IoT dataset provided observations representing both normal and malicious activities within IoT and industrial IoT environments. The results were organized according to four participating clients representing separate distributed network entities. Table 1 presents the accuracy, precision, recall, and F1-score values for each client, together with the performance of the aggregated federated model. These results enable assessment of detection consistency among the participating clients and provide an overall view of the effectiveness of the federated model when information from distributed clients is combined.

Table 1. Federated Learning Performance Across IoT Clients

Model	Accuracy	Precision	Recall	F1-Score
FL Model — Client 1	0.9758	0.9449	0.9883	0.9661
FL Model — Client 2	0.9755	0.9436	0.9892	0.9658
FL Model — Client 3	0.9748	0.9440	0.9864	0.9647
FL Model — Client 4	0.9760	0.9458	0.9878	0.9664
Aggregated FL Model	0.9759	0.9487	0.9842	0.9661

Source: Lazzarini et al. (2023)

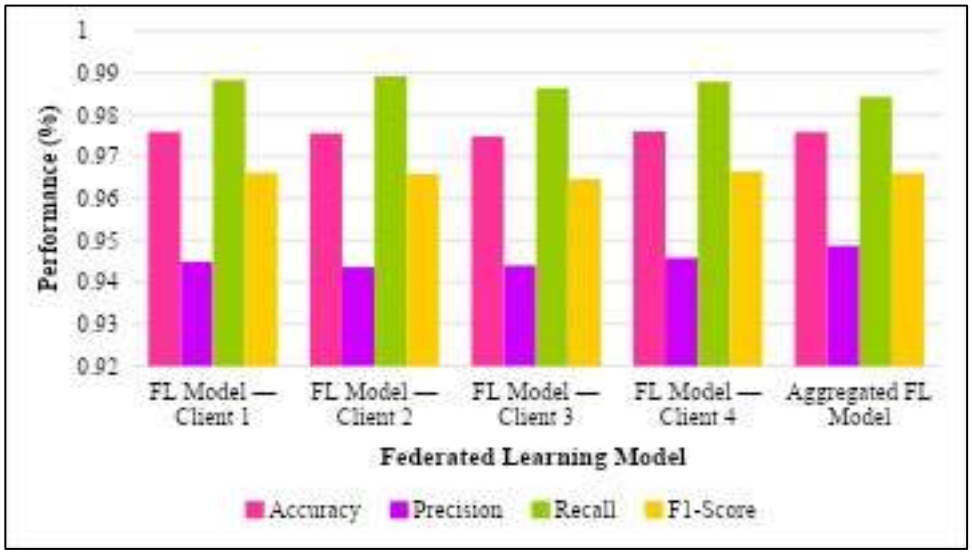

Figure 1. Comparative Cyber-Threat Detection Performance Across Federated IoT Clients

The detection performance obtained across four federated IoT clients and the resulting aggregated model. The four clients exhibit closely comparable accuracy and F1-score values, indicating that the learning process

remains relatively stable despite distributed training, as shown in Figure 1. Recall is consistently higher than precision across all clients, suggesting that the models identify malicious instances effectively while maintaining some room for improvement in avoiding false-positive classifications. The aggregated model follows the overall pattern observed among individual clients, demonstrating that model aggregation preserves the predictive characteristics learned locally. These results support the feasibility of collaborative threat detection without requiring centralized raw IoT data.

3.2 Comparative Evaluation of Federated Aggregation Strategies

The evaluation shows noticeable differences among the federated aggregation strategies. FedAvgM produced the strongest overall performance, achieving an accuracy of 0.9772, precision of 0.9512, recall of 0.9853, and F1-score of 0.9679. FedAvg also demonstrated robust results, with an accuracy of 0.9759 and an F1-score of 0.9661, as shown in Table 2. In comparison, FedAdam recorded lower accuracy and precision, although its recall remained relatively high. FedAdagrad achieved the lowest accuracy, precision, and F1-score among the evaluated approaches. These findings indicate that the choice of aggregation strategy can substantially influence the effectiveness of federated cyber-threat detection in distributed IoT environments.

Table 2. Comparison of Federated Aggregation Algorithms

Aggregation Algorithm	Accuracy	Precision	Recall	F1-Score
FedAvg	0.9759	0.9487	0.9842	0.9661
FedAvgM	0.9772	0.9512	0.9853	0.9679
FedAdam	0.8767	0.7580	0.9505	0.8434
FedAdagrad	0.8176	0.6635	0.9697	0.7879

Source: Lazzarini et al. (2023)

Figure 2. Comparative Performance of Federated Aggregation Algorithms for IoT Threat Detection

The performance differences among four federated aggregation strategies: FedAvg, FedAvgM, FedAdam, and FedAdagrad. FedAvgM demonstrates the strongest overall results across the evaluated metrics, while FedAvg also maintains consistently high performance, as shown in Figure 2. FedAdam shows a noticeable reduction in accuracy, precision, and F1-score despite retaining relatively strong recall.

FedAdagrad records the lowest overall performance for most measures, although its recall remains comparatively high. The observed differences indicate that aggregation strategy can influence the effectiveness

of the global federated model. Selecting an appropriate aggregation mechanism is therefore important when developing reliable machine-learning-based cyber-threat detection systems for distributed IoT environments.

3.3 Comparative Performance of Centralized and Federated Learning

The comparison indicates that centralized learning achieved slightly stronger overall predictive performance than the aggregated federated model. The centralized approach recorded an accuracy of 0.9840, precision of 0.9729, recall of 0.9817, and F1-score of 0.9772 as shown in Table 3. In contrast, the aggregated federated model achieved an accuracy of 0.9759, precision of 0.9487, recall of 0.9842, and F1-score of 0.9661. Although centralized learning provided higher accuracy, precision, and F1-score, federated learning produced a marginally higher recall. This demonstrates that federated learning can maintain competitive threat-detection capability while supporting distributed data processing.

Table 3. Centralized Learning versus Federated Learning

Training Approach	Accuracy	Precision	Recall	F1-Score
Federated Learning — Aggregated	0.9759	0.9487	0.9842	0.9661
Centralized Learning	0.9840	0.9729	0.9817	0.9772

Source: Lazzarini et al. (2023)

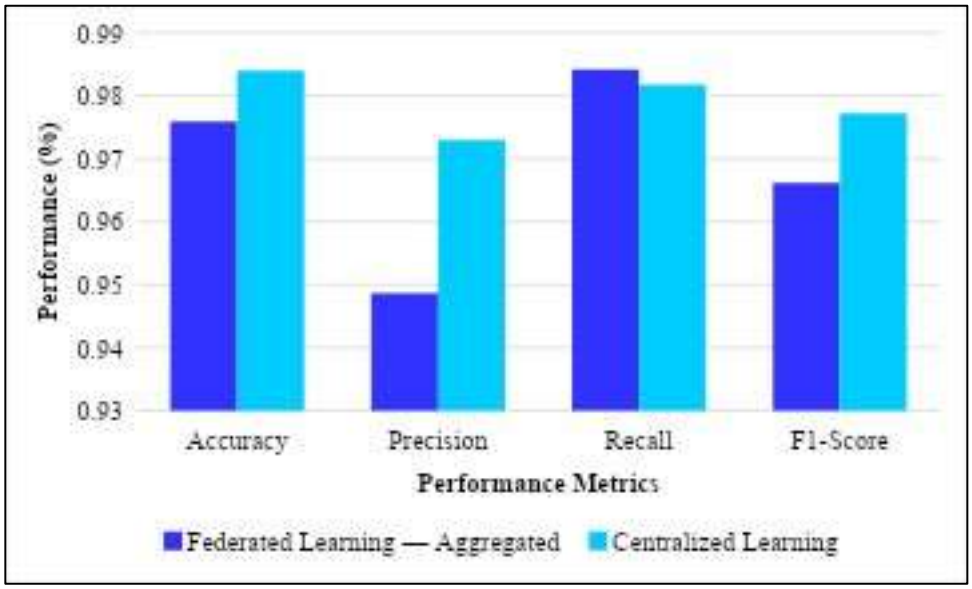

Figure 3. Comparative Cyber-Threat Detection Performance of Federated and Centralized Learning

The predictive performance of aggregated federated learning and centralized learning across four evaluation metrics. The centralized approach demonstrates higher accuracy, precision, and F1-score, indicating a modest predictive advantage when training data are combined centrally, as shown in Figure 3. However, the federated approach achieves a slightly higher recall, showing effective identification of malicious instances despite decentralized training. The relatively small differences between the two approaches demonstrate that federated learning can provide competitive detection performance while avoiding direct centralization of participating clients' raw data. This trade-off is important for IoT cybersecurity applications where collaborative intelligence must be balanced with data privacy and decentralized processing requirements.

4. Discussion

The study indicates that federated learning can provide effective cyber-threat detection while maintaining a distributed learning structure. The performance observed across the participating clients was relatively consistent, suggesting that the learning process was not strongly dependent on a single client. The aggregated federated model also maintained competitive classification performance compared with centralized learning.

This is important because centralized training can benefit from direct access to combined observations, whereas federated learning must construct a common model from locally trained updates. Similar observations have been reported in studies investigating privacy-preserving federated intrusion detection, where collaborative model training has demonstrated the ability to support cybersecurity without requiring direct transfer of local datasets.

The results support the relevance of federated learning to IoT cybersecurity, particularly where network information is distributed among multiple devices or administrative domains. Instead of requiring all participating data to be collected at one location, federated learning allows clients to perform local model training and contribute model updates to a shared learning process. This structure is compatible with the distributed characteristics of IoT infrastructures, where devices may differ in their computational capabilities, network conditions, and observed attack patterns. These findings demonstrate the applicability of privacy-preserving federated learning to intrusion detection in industrial IoT environments and reinforce its suitability for distributed IoT security. More broadly, Timofte et al. (2025) identified federated learning as a promising privacy-preserving paradigm for cybersecurity applications.

The comparison of aggregation strategies also indicates that the choice of aggregation mechanism can influence the resulting detection performance. The stronger performance observed with FedAvg and FedAvgM compared with FedAdam and FedAdagrad suggests that the optimization behaviour of the aggregation process should be considered when developing federated intrusion-detection systems. This observation is consistent with the broader literature, which recognizes that federated learning performance depends not only on the underlying classifier but also on the method used to combine information from participating clients (Vyas et al., 2024).

Privacy preservation represents one of the principal advantages of the proposed federated-learning approach. In conventional centralized cybersecurity systems, network traffic and security observations from multiple sources may need to be transferred to a central repository before model training. Federated learning changes this arrangement by keeping the training data at the participating clients and exchanging model updates instead. This can reduce the direct exposure of raw network observations during collaborative model development. However, federated learning should not be interpreted as providing complete privacy protection by itself. Model updates can potentially reveal information about local training data, and additional protection mechanisms may therefore be required in highly sensitive environments. These considerations highlight the importance of incorporating additional privacy-preserving mechanisms when deploying FL-based intrusion-detection systems, particularly in privacy-sensitive environments.

The findings are broadly consistent with previous research on federated intrusion detection, although direct numerical comparison should be made cautiously because published studies differ in datasets, attack categories, client configurations, models, and evaluation procedures. Ruzafa-Alcázar et al. (2021) investigated privacy-preserving FL for industrial IoT intrusion detection, demonstrating the applicability of collaborative learning to distributed industrial environments. Raza et al. (2024) extended the concept to software-defined networks, emphasizing the role of federated learning in reducing privacy concerns during intrusion-detection model development. The present findings similarly indicate that decentralized learning can retain useful detection capability while avoiding direct centralization of client-level data. Timofte et al. (2025) also emphasized the broader role of FL in cybersecurity, supporting the interpretation that federated learning can serve as an important component of privacy-aware security architectures.

Recent research has additionally emphasized the integration of explainability and privacy. Yazdinejad et al. (2025) proposed an explainable and privacy-preserving federated-learning model for threat detection in cyber-physical-social systems. This direction is particularly relevant because effective cybersecurity systems increasingly require not only accurate predictions but also understandable reasons for security decisions. Therefore, future federated IoT systems could extend the current approach by incorporating explainable artificial intelligence alongside privacy-preserving learning.

From a practical perspective, the findings suggest that federated learning can be considered for IoT environments in which multiple participants need to cooperate on cyber-threat detection without directly pooling their raw network data. Such an architecture may be useful for distributed organizations, industrial IoT deployments, smart infrastructures, and other environments in which security information is generated at geographically or administratively separated locations. The relatively competitive performance of federated learning compared with centralized learning suggests that privacy requirements do not necessarily require abandoning machine-learning-based threat detection. Nevertheless, practical deployment should consider communication overhead, client availability, computational limitations, model-update security, and differences in local data distributions. These considerations are particularly important because the effectiveness of a federated system depends on both its predictive performance and its ability to operate reliably across heterogeneous participants.

Several limitations should be considered when interpreting the findings. First, evaluation using a benchmark dataset cannot fully reproduce the diversity and unpredictability of operational IoT networks. Real-world environments may contain changing traffic patterns, previously unseen attacks, heterogeneous devices, and highly imbalanced local datasets. Second, federated performance can vary according to the number of clients, client-data distributions, communication rounds, and aggregation configuration. Third, retaining data locally does not by itself guarantee protection against every privacy or security threat associated with model updates. Additional techniques such as secure aggregation, differential privacy, encryption, or robust aggregation may therefore be required depending on the deployment context. Finally, comparisons with previous studies should be interpreted as contextual rather than direct because different datasets and experimental protocols are used across the literature.

Future research should evaluate federated threat detection using larger and more heterogeneous IoT datasets and realistic distributions of data across participating clients. Particular attention should be given to non-IID data, dynamic client participation, communication efficiency, and the detection of previously unseen attacks. Privacy mechanisms could also be integrated directly into the federated architecture to provide stronger protection against information leakage from model updates. Another promising direction is the combination of federated learning with explainable AI so that security analysts can understand why particular network activities are classified as malicious. This direction is particularly relevant to complex cyber-physical-social environments. Further investigation of robust aggregation and privacy-enhancing mechanisms could consequently improve the reliability, interpretability, and practical scalability of federated cybersecurity systems.

5. Conclusion

This study examined federated learning as a privacy-preserving approach for cyber-threat detection in distributed IoT networks. The study focused on collaborative model training across multiple clients while avoiding direct centralization of locally generated network data. The findings indicate that federated learning can achieve consistent threat-detection performance across distributed clients. The aggregated model maintained competitive performance with centralized learning, while the evaluation of different aggregation strategies showed that aggregation selection can influence the effectiveness of the resulting global model. The principal contribution is the application of a decentralized learning structure in which participating clients retain their local data and contribute model updates to collaborative training. This approach can reduce the need for transferring sensitive IoT traffic information to a central repository. The results demonstrate the potential of federated learning for IoT security environments where data ownership, privacy, and distributed processing are important considerations. The approach provides a practical foundation for collaborative threat detection across heterogeneous IoT networks. The evaluation is based on benchmark data and therefore may not capture every characteristic of operational IoT networks. Differences in client distributions, network conditions, and attack patterns may also affect performance. Future studies should investigate heterogeneous real-world IoT environments, unseen attacks, communication efficiency, robust aggregation, and stronger privacy mechanisms. Integrating explainable AI could further improve transparency and support security analysts in interpreting federated threat-detection decisions.

References

1. Abou El Houda, Z., Hafid, A. S., & Khoukhi, L. (2023). MiTFed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain. IEEE Transactions on Network Science and Engineering, 10(4), 1985-2001.
2. Al Amro, S. (2025). Securing Internet of Things devices with federated learning: A privacy-preserving approach for distributed intrusion detection. Computers, Materials & Continua, 83(3), 4623-4658.
3. Alaskar, N. M., Hussain, M., Almheiri, S. J., Khan, A., & Adnan, K. M. (2026). Big data-driven federated learning model for scalable and privacy-preserving cyber threat detection in IoT-enabled healthcare systems. Computers, Materials & Continua, 87(1), 29.
4. Alazab, A., Khraisat, A., Singh, S., & Jan, T. (2023). Enhancing privacy-preserving intrusion detection through federated learning. Electronics, 12(16), 3382.
5. Almeida, L., Rodrigues, P., Teixeira, R., Antunes, M., & Aguiar, R. L. (2024, June). Privacy-preserving defense: intrusion detection in IoT using federated learning. In 2024 IEEE 22nd Mediterranean Electrotechnical Conference (MELECON) (pp. 908-913). IEEE.
6. Aramide, O. O. (2025). Federated learning for distributed network security and threat intelligence: A privacy-preserving paradigm for scalable cyber defense. Journal of Data Analysis and Critical Management, 1(02).

7. Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. IEEE Access, 11, 120918-120934.
8. Bhatia, K., Bhattacharya, S., & Sharma, I. (2024, February). Privacy-preserving detection of DDoS attacks in IoT using federated learning techniques. In 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML) (pp. 234-239). IEEE.
9. Bukhari, S. M. S., Zafar, M. H., Abou Houran, M., Moosavi, S. K. R., Mansoor, M., Muaaz, M., & Sanfilippo, F. (2024). Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 155, 103407.
10. Gutti, C., Thumula, K., & Balbudhe, P. (2025). Federated learning for distributed IoT security: A privacy-preserving approach to intrusion detection. IEEE Access, 13, 135863-135875.
11. Hossain, M. A., & Islam, M. S. (2025). Towards decentralized cybersecurity: A novel privacy-preserving federated learning approach for botnet attack detection. Blockchain: Research and Applications, 100355.
12. Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., & Jan, T. (2025). Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy. Discover Internet of Things, 5(1), 72.
13. Lazzarini, R., Tianfield, H., & Charissis, V. (2023). Federated learning for IoT intrusion detection. Ai, 4(3), 509-530.
14. Mahmud, S. A., Islam, N., Islam, Z., Rahman, Z., & Mehedi, S. T. (2024). Privacy-preserving federated learning-based intrusion detection technique for cyber-physicalsystems. Mathematics, 12(20), 3194.
15. Mankotia, S., Conte de Leon, D., & Rimal, B. P. (2026). FedPrIDS: Privacy-preserving federated learning for collaborative network intrusion detection in IoT. Journal of Cybersecurity and Privacy, 6(1), 10.
16. Moulahi, T., Jabbar, R., Alabdulatif, A., Abbas, S., El Khediri, S., Zidi, S., & Rizwan, M. (2023). Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. Expert Systems, 40(5), e13103.
17. Mrabet, M. (2025). TrustFed-CTI: A trust-aware federated learning framework for privacy-preserving cyber threat intelligence sharing across distributed organizations. Future Internet, 17(11), 512.
18. Nandanwar, H., & Katarya, R. (2024, December). A secure and privacy-preserving ids for iot networks using hybrid blockchain and federated learning. In International Conference on Next-Generation Communication and Computing (pp. 207-219). Singapore: Springer Nature Singapore.
19. Rabieinejad, E., Yazdinejad, A., Dehghantanha, A., & Srivastava, G. (2024). Two-level privacy-preserving framework: Federated learning for attack detection in the consumer Internet of Things. IEEE Transactions on Consumer Electronics, 70(1), 4258-4265.
20. Ragab, M., Ashary, E. B., Alghamdi, B. M., Aboalela, R., Alsaadi, N., Maghrabi, L. A., & Allehaibi, K. H. (2025). Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. Scientific reports, 15(1), 4470.
21. Rahmati, M., & Pagano, A. (2025, July). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. In Informatics (Vol. 12, No. 3, p. 62). MDPI.
22. Raza, M., Saeed, M. J., Riaz, M. B., & Sattar, M. A. (2024). Federated learning for privacy-preserving intrusion detection in software-defined networks. IEEE Access, 12, 69551-69567.
23. Ruzafa-Alcázar, P., Fernández-Saura, P., Mármol-Campos, E., González-Vidal, A., Hernández-Ramos, J. L., Bernal-Bernabe, J., & Skarmeta, A. F. (2021). Intrusion detection based on privacy-preserving federated learning for the industrial IoT. IEEE Transactions on Industrial Informatics, 19(2), 1145-1154.
24. Timofte, E. M., Dimian, M., Graur, A., Potorac, A. D., Balan, D., Croitoru, I., ... & Puşcaşu, M. (2025). Federated learning for cybersecurity: A privacy-preserving approach. Applied Sciences, 15(12), 6878.
25. Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-preserving federated learning for intrusion detection in IoT environments: A survey. IEEE Access, 12, 127018-127050.
26. Yazdinejad, A., Mohammadabadi, Z. D., Dehghantanha, A., & Srivastava, G. (2025). An explainable and privacy-preserving federated learning model for threat detection in cyber-physical-social systems. IEEE Transactions on Computational Social Systems.