IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, April 2025

Impact Factor: 7.67

Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection

Niravkumar Prajapati
Independent Researcher
niravprajapati343@gmail.com

Abstract: *Federated Learning's (FL) distributed threat detection technique is a significant advancement in cybersecurity as it preserves privacy while processing data in a decentralized manner. Centralized security systems that rely on raw data collection present two major threats to users because they create regulatory problems in addition to data breaches. FL removes security concerns through its model-building process, allowing different organizations to work together without sharing private data. This document investigates FL's role in cybersecurity through an analysis of malware/ransomware detection, IDS applications, secure threat detection, and network traffic anomaly detection. The paper explores effective privacy-protecting techniques: FL implementations are protected against Byzantine and backdoor attacks using Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), Differential Privacy (DP), and Secure Model Aggregation. FL delivers advantages but encounters challenges mainly related to excessive communication demands as well as performance deterioration under adversarial conditions, and difficulties with system expansion. The research provides an exhaustive analysis of FL-based cybersecurity frameworks while discussing existing applications and security threats together with future developments for these systems and the need for advanced privacy-protecting methods to improve the dependability of FL cybersecurity solutions.*

Keywords: Federated Learning, Privacy-Preserving Cybersecurity, Secure Threat Detection, Intrusion Detection Systems, Differential Privacy, Secure Multi-Party Computation, Anomaly Detection

I. INTRODUCTION

In an era of networks that have expanded drastically, organizations and people face increasing threats to their cybersecurity. Cloud computing, IoT devices, and edge systems have all grown rapidly; This has raised the need for secure detection systems capable of instantly recognizing and thwarting cyber threats. The conventional security systems gather extensive sensitive data at one central location for analysis in their monitoring procedure[1][2]. Federated Learning (FL), which enables distributed computations without disclosing raw data, makes decentralized model training possible. The broad threat detection made possible by FL exposes systems to significant privacy breaches that result in data theft, unauthorized system access, and vulnerabilities for cyberattacks.

The problem of extensive data collection and analysis is critical to threat detection, yet it does pose great privacy challenges. Organizations may be reluctant to disclose sensitive data due to regulatory compliance and a fear of information exposure. Additionally, it leaves the data open to illegal disclosure or data breaches. Even while it might not be feasible to overcome these obstacles, businesses can use FL to local train models and only communicate safe model updates, protecting privacy and enhancing cybersecurity[3].

Federated Learning aims to accomplish decentralized machine learning, which makes it possible to train models using several data sources without sending raw data. In contrast to a centralized strategy, which distributes computing among local devices or nodes, FL uses a single server to gather data from several sources for model training. In this case, only model modifications, such as weights or gradients, are sent to a central server by each device, which trains the model locally using its own private dataset. These changes are combined on the central server to produce a global model,

DOI: 10.48175/IJARSCT-25168

which is then distributed to the devices for iterative improvement. However, in addition to safeguarding data privacy, this approach reduces the delay and expense associated with sending big information. The ability of FL to handle Non-Independent and Identically Distributed (non-IID) data between devices is a critical component. In contrast to centralized systems that presume consistent data distributions, FL operates in settings where participant data might vary greatly, just like in the real world, where a user could have regional patterns or particular preferences[4].

Federated Learning improves threat detection in the field of cybersecurity by combining insights from several datasets across several companies without disclosing private information[5]. This collaboration greatly contributes to the improved model accuracy and robustness by allowing to identify the emerging and sophisticated threats, which would otherwise go undetected with the use of individual data sources. FL ensures that data is protected during the training process by utilizing privacy-preserving strategies, including secure aggregation and differential privacy. Thus, FL is an extremely effective and privacy-aware approach to detect threats in the distributed and dynamic cybersecurity environments[6].

A. Structure of the paper

The structure of this paper is as follows: An overview of cybersecurity federated learning is provided in Section II. In Section III, the methods for protecting privacy in cybersecurity federated learning are examined. Secure threat detection via federated learning is covered in Section IV. After reviewing pertinent case studies and literature in Section V, Section VI offers suggestions for future research.

II. OVERVIEW OF FEDERATED LEARNING IN CYBERSECURITY

FL is a novel concept that Google just introduced. Google aims to minimise data leaks by using information spread across several devices to build machine learning models. Many entities (such as devices, organisations, or edge nodes) can collaborate to train a shared model without sharing starting data, thanks to FL, a decentralised ML paradigm. There have been recent developments in federated learning that tackle security and statistical concerns. Dispersed mobile user interactions are a key component of federated learning on mobile devices, where issues such as device dependability, unequal data dissemination, and communication costs in a large-scale distribution are crucial for optimisation. Additionally, data is divided by device or user IDs in a horizontal fashion inside the data space[7].

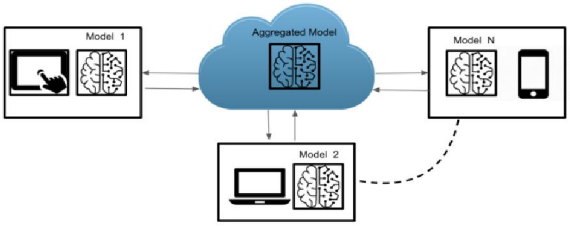

Figure 1: Overview of Federated Learning Across Devices.

The process of FL is shown in Figure 1. It demonstrates how a variety of gadgets, such as cellphones, laptops, and tablets, take part in the training process. The selected devices utilize their local data to train a global model that is sent to them from the server. After training, the devices communicate the updated model parameters back to the server. The global model is improved by the server combining these modifications, and it is subsequently transmitted back to the devices again until it is optimized[8].

A. Key components of FL in Cybersecurity

In FL have a centralized approach to ML where the privacy of data is enhanced, but model training can be trained collaboratively[9]. FL has become an effective method to detect and mitigate cyber threats in distributed environments in cybersecurity. FL in cybersecurity applications consists of mainly:

- **Clients:** Distributed entities that participate in the FL process are referred to as clients. These include sensors, edge devices, or organizational nodes that use their data to train local models. Client applications include firewalls, IDS, and SIEM systems. Clients train the model using local data, and only model updates—not raw data—are transmitted to a central server for compilation.

- **Server:** The central server is responsible for coordinating the FL process. Through techniques like FedAvg, it compiles model updates from several customers. The clients are subsequently sent the revised global model by the server for additional training in later cycles. The organization is responsible for monitoring the interactions among the entities in the FL environment and gathering the knowledge that the FL clients have acquired.
- **Global Model:** The primary server maintains the globally trained ML model. After merging the model updates from several clients, the global model is refined and re-distributed for further training. In cybersecurity, the global model continuously evolves to detect new and emerging threats across different environments.
- **Communication:** An essential feature of FL is communication, which includes the process by which clients and the central server exchange model parameters. It can be carried out via an internal network, intranet, or the Internet and consists of the instruments and equipment that connect servers and parties[10].

B. Federated Learning for Privacy-Preserving Analytics

- Federated Learning resolves these issues with privacy by:
- **Local Data Processing:** To reduce exposure and Data remaining on local devices or servers, increasing the risk of breaches. Because only model modifications (such as gradients) are transmitted rather than private information being transferred to a centralized server, privacy is protected by design.
- **Model Aggregation:** FL combines model updates from several participants via a safe aggregation approach. This method stops attackers from using individual model changes to deduce sensitive information.
- **Differential Privacy and Encryption:** FL may be enhanced using techniques like safe aggregation and differential privacy to better protect privacy.
- **Federated Averaging (FedAvg):** FedAvg is a popular FL method that minimizes communication cost by locally averaging model changes before sending them to the central server in order to protect data privacy.

C. Applications in Security Analytics

In security analytics, FL, in particular, is very beneficial in threat detection improvement, model robustness improvement, and protecting sensitive information. Some specific applications include:

- **Enhancing Threat Detection:** FL may improve the detection of novel threats and anomalies that may not be discernible from a single data source by employing geographically distributed data sources. Organizational collaboration in learning can reveal trends suggestive of malware activity, fraud attempts, or cybersecurity issues.
- **Building Robust Models:** Combining knowledge from several datasets aids in creating security models that are more resilient and broadly applicable. Through knowledge sharing, organizations may cooperatively improve threat detection systems without disclosing private information.
- **Protecting Sensitive Information:** It enables businesses to collaborate on security analytics while maintaining control over sensitive data[11].

III. PRIVACY-PRESERVING TECHNIQUES IN FEDERATED LEARNING FOR CYBERSECURITY

There are several techniques by which FL improves cybersecurity while maintaining data privacy. In the case of Differential Privacy (DP), model changes are conducted with extra noise to prevent data leaking. Collaborative training is made possible by Secure multi-party computation (SMPC), which conceals individual input. Using homomorphic encryption to compute on encrypted data guarantees confidentiality. Verifying and combining updates in an adversarial secure way is the goal of Secure Model Aggregation. Together, these techniques help FL overcome its

DOI: 10.48175/IJARSCT-25168

privacy and compliance limitations as well as expand the dangers it can detect in cyber threats. Using various privacy-preserving techniques, FL makes sure threat detection is secure and private:

A. Differential Privacy for Protecting Sensitive Data:

In order to assess and restrict the amount of sensitive data that is leaked, adversaries to data/model analysis in FL sometimes use DP as a privacy preservation approach. In order to distort the input or output of user processing and make the findings somewhat resistant to privacy analysis, it uses a randomized method (e.g., adding random sounds or introducing particular random sub-sampling). DP adds statistical noise to the model updates so that attackers cannot reconstruct individual client information while maintaining good model accuracy.

B. Secure Multi-Party Computation (SMPC) in Federated Models:

Multiple parties are involved in SMC security models, which offer security evidence in a precise simulation framework to guarantee that each party recognizes only its input and output, guaranteeing total ignorance. Although having no information is ideal, it sometimes necessitates intricate computations that aren't always feasible, and depending on the circumstance, it could be appropriate to reveal just a fraction of a person's knowledge. Building a security model using SMC might boost capabilities while lowering security requirements. SMPC allows multiple participants to collaboratively train models without disclosing their private information, ensuring secure computations across distributed entities[7].

C. Homomorphic Encryption:

A particular kind of encryption system called homomorphic encryption allows function evaluations over encrypted data while maintaining the function attributes and data structure. Without decryption, homomorphic encryption (HE) methods subject ciphertexts to complex mathematical computations. it is regarded as the best way to implement the SMC protocol as it does not utilize plain text directly while calculating. It allows computations on encrypted data, enabling clients to share encrypted model updates without exposing raw data, thereby preventing potential breaches[12].

D. Secure Model Aggregation and Decentralization for Enhanced Privacy:

Secure Model Aggregation involves cryptographic protocols that enable the server to calculate aggregated model updates without having to obtain the changes from each individual client. Secure multiparty computing and homomorphic encryption are two techniques that guarantee the server only knows the overall result and not the individual contributions. In the case of decentralization in FL, it involves distributing the aggregation process across different nodes or clients, so that a centralized server is no longer necessary. This strategy should improve security and privacy while also making it more difficult for enemies to identify and fix the system. Further, if blockchain technology is applied in FL, it will be integrated into decentralized protocols such as blockchain, ensuring secure aggregation[13][14][15].

IV. FEDERATED LEARNING FOR SECURE THREAT DETECTION

The backdoor attacks embed hidden vulnerabilities into the global model caught into training by malicious participants. The backdoors are present on benign input but undetected and can be exploited on model outputs that are triggered by specific inputs. The goal is to ensure the model works as expected on normal data and behaves in the way the attacker desired on the backdoor samples. Byzantine attacks occur when one or more malicious users intentionally send false or misleading updates to the central server inside the FL system. Figure 2 shows how this interferes with the training process, causing irregular model convergence and decreasing the overall dependability of the system. The integrity and resilience of FL-based cybersecurity solutions depend on addressing these vulnerabilities.

DOI: 10.48175/IJARSCT-25168

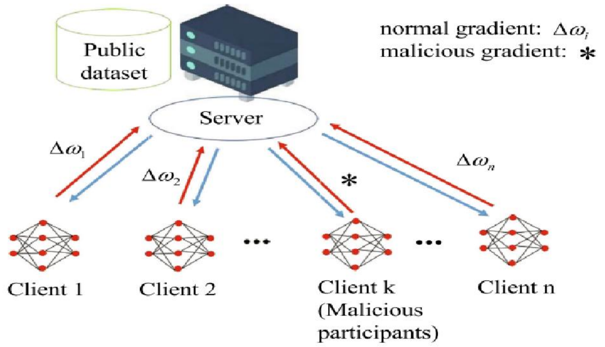

Figure 2: In Byzantine Attacks, There Exist One or More Malicious Federated learning system users (client k) that interfere with training by providing the central server with inaccurate or deceptive updates, resulting to anomalous convergence[16]

A. The Evaluation of FL on Cyber Threat Detection Tasks

Concurrent with their work, they evaluated the effectiveness of FL on SMS spam detection. However, their FL experiment settings are not practical as only two FL clients were deployed, and the spam dataset under evaluation was outdated. Another study on FL-based SMS spam detection only considered three clients. Also, the authors failed to explore security-specific FL scenarios, not to mention to profile the adversarial resistance of FL for SMS spam detection. Besides, federated SVM was applied in Android malware detection in 2020, while an FL-based Android malware detection framework, namely FEDriod, was introduced in 2023. Nevertheless, both studies only took into account a maximum of seven FL clients for training, focusing solely on the efficacy of federated learning rather than its efficiency and resilience to adversaries. In 2023, a dynamic weighted federated averaging strategy was applied to Android malware detection. Besides, the concept of cross-silo FL was applied to threat intelligence sharing across organizations. Still, very few settings were considered when profiling the effectiveness of FL, and no experiments were conducted to understand the adversarial resistance of FL[17].

B. Key Cybersecurity Applications of Federated Learning

FL enhances cybersecurity by enabling decentralized threat detection while preserving privacy. FL allows several entities to collaborate on training models without sharing raw data, unlike traditional models that rely on centralized data collection. By utilizing dispersed intelligence, this method improves IDS, phishing prevention, malware and ransomware detection, and anomaly identification in network data. By detecting threats in real time while maintaining data confidentiality, FL provides a robust, privacy-preserving solution for modern cybersecurity challenges.

Intrusion Detection Systems (IDS):

An IDS monitors network activity to identify network intrusions. The two main types of IDS available today are host-based and network-based. NIDS are designed to detect intrusions by monitoring different network activities, whereas host-based intrusion detection systems (HIDSs) are designed to detect network intrusions in specific hosts. As NIDS can keep an eye on more network targets, it can see more assaults that HIDSs could overlook because HIDSs can't read packet headers. NIDS keeps an eye on the output of packet sniffers. In order to detect a range of IP-based DoS attacks, for instance, NIDS are able to monitor packet headers as they go across the network. Furthermore, NIDS is made to work with certain operating systems and is less reliant on the host's OS as a source of detection. HIDS and NIDS have been combined in some hybrid IDSs and used to detect intrusions [18].

Malware and Ransomware Detection:

Ransomware is a type of malware that prevents people from accessing their own data unless they pay a ransom. An ecosystem of hackers has been fostered by the direct financial implications of this form of virus, which they use as a business model. RaaS is a service that makes it simple and expensive to obtain ransomware programs. Either an outright purchase or a profit-sharing plan might be employed for the price. The fact that criminals cooperate is demonstrated by this. The development and creation of the ransomware code are the responsibilities of one party, while the organization of the infection's or attack campaign's spread is the responsibility of another party. Both parties profit from a successful attack. In the end, this will encourage specialized offenders that will be challenging for law enforcement to track down[19].

Anomaly Detection in Network Traffic:

The two primary methods for detecting anomalies in network data are feature detection and anomaly detection, each of which has advantages and disadvantages of its own. On the other hand, feature detection has a high level of accuracy and quickness of reaction when detecting known attack patterns, especially for predetermined irregularities, and a low false positive rate. However, it is vulnerable to new or undiscovered assaults and requires expensive maintenance due to the regular feature database upgrades. On the other hand, anomaly detection is highly regarded for its strong flexibility and capacity to identify unidentified assaults. It does this by constantly modifying its detection tactics in response to real-time variations in network traffic, therefore thoroughly monitoring all potential assaulting components. Despite these difficulties, this method does need a lot of computational power and has a significant false positive rate. Setting suitable thresholds and anomaly detection settings requires specialized expertise as well. Such methods are constantly being redefined and improved with the advent of ML and DL, which provide network security with both benefits and difficulties[20].

V. LITERATURE REVIEW

In this section, conduct a literature review on the use of Federated Learning (FL) to protect cybersecurity privacy in general and secure threat detection in particular. The paper reviews FL-based cybersecurity frameworks, focuses on best practices, new challenges and advancements. Table I provides a summary of the reviewed studies for ease of reading.

Zhou et al. (2022) for edge computing a brand-new privacy-preserving FL scheme (PFLF) is suggested. For every piece of data in PFLF, the application server and client contribute noise. To safeguard customers' privacy, it create a flexible arrangement process that counts the best training hours for them. They show that PFLF provides privacy assurances for both clients and servers during the whole training procedure. Client privacy may be safeguarded against privacy leaks in distributed machine learning, commonly referred to as federated learning. Edge computing may be made even more convenient by utilizing FL to preserve edge clients' privacy[21].

Li et al. (2024) created a PFLS against poisoning attacks to eliminate the impact of model poisoning attacks on the privacy of participants. More specifically, a dynamic adaptive defense technique is created that may identify the malevolent actors and lessen the impact of hostile gradients. To safeguard the anonymity of participants, a multidimensional homomorphic encryption technique is combined with a hierarchical aggregation design. The security analysis shows that the PFLS scheme is able to keep the private of FL participants [22].

O'Connor and Elfouly (2024) in the present, FL is used to create a new cybersecurity architecture that increases the smart distribution grids' resistance to cyberattacks. Because of FL, data analysis may be carried out cooperatively by several grid nodes without jeopardizing data privacy or disclosing sensitive information that could be intercepted and jeopardize the smart distribution grid as a whole[23].

Suneetha and Kesavan (2024) This review discusses the new development of privacy-preserving communication in machine learning, namely in the domains of secure multi-party computation for cyber threat detection (SMPC), federated learning, and differential privacy (DP). It also contributes to cybersecurity threat monitoring using privacy privacy-preserving framework in distributed systems like IoT and industrial networks. The study of privacy-preserving communication shows that FL can be combined with DP and SMPC to achieve data privacy preservation while the deduction accuracy of detecting cyber threats can be well-maintained[24].

Moumni, Châabane and Drira (2023) examine ML models that have been implemented and shown on an open dataset to show how effective FL frameworks based on ML are at protecting privacy. They demonstrate through extensive tests and analyses the notable privacy attained by using local model training, aggregated model updates, and decentralized data. Through the use of FL, it present a viable approach to anomaly detection privacy preservation that permits efficient analysis of smart meter data[25].

Ghimire and Rawat (2022) emphasize security above all else, but it also covers several techniques to address FL's performance issues (accuracy, latency, resource limitations, etc.) that might compromise the general security and usefulness of the IoT. To forecast how this new paradigm will evolve in the future, it reviews the main research projects, challenges, and trends in this area. This article will provide readers with a more thorough understanding of cybersecurity for Florida, including different security risks and defenses[26].

Table I provides the summary of related work based on Federated Learning for Privacy-Preserving Cybersecurity, including key findings, Approaches, challenges, Study on, and Limitations.

Table 1: Summary of literature review based on Federated Learning for Privacy-Preserving Cybersecurity

Reference	**Study On**	**Approach**	**Key Findings**	**Challenges**	**Limitations**
Zhou et al. (2022)	Privacy-preserving FL for edge computing	A Privacy-preserving Federated Learning Framework (PFLF) was put out that incorporates noise addition and flexible training methods.	Enhanced privacy through noise addition and optimal training time allocation, ensuring data security across training phases.	Balancing privacy and performance in edge environments.	Increased communication overhead due to added noise and extra processing
Li et al. (2024)	Defense against poisoning attacks in FL	Developed a Privacy-preserving FL Scheme (PFLS) with dynamic adaptive defense and multidimensional homomorphic encryption.	Improved resilience to model poisoning attacks while preserving participant privacy through hierarchical aggregation.	Identifying malicious gradients without impacting model convergence.	Higher computational cost due to homomorphic encryption.
O'Connor and Elfouly (2024)	Cybersecurity in smart distribution grids	FL was used to analyze data collaboratively and privately across several grid nodes.	Enhanced resilience to cyber-attacks in smart grids without exposing sensitive node-level data.	Managing synchronization and latency across grid nodes.	Requires robust communication infrastructure for real-time performance.
Suneetha and Kesavan (2024)	Privacy-preserving communication in FL	FL in conjunction with Secure Multi-Party Computation (SMPC) and Differential Privacy (DP) for the identification of cyberthreats.	Achieved privacy preservation while maintaining high threat detection accuracy across IoT and industrial networks.	Balancing accuracy and privacy trade-offs.	Increased complexity due to integrating multiple privacy mechanisms.
Moumni, Châabane and Drira (2023)	Privacy-preserving anomaly detection	Explored FL models on smart meter data, leveraging decentralized data and local model training.	Demonstrated significant privacy benefits through decentralized data processing and aggregated model updates.	Ensuring consistent model accuracy across heterogeneous datasets.	Requires robust aggregation techniques for diverse data patterns.
Ghimire and Rawat	Security challenges in	Surveyed FL's performance issues and	Provided insights into FL's dual role in	Addressing resource	Lack of standardized

(2022)	FL for IoT	security challenges, focusing on accuracy, latency, and resource constraints.	enhancing cybersecurity and facing security threats, discussing countermeasures for attacks.	limitations in IoT environments.	security protocols for FL in IoT environments.

VI. CONCLUSION AND FUTURE WORK

Federated learning has become a popular cybersecurity strategy that protects privacy by facilitating cooperative threat detection without disclosing private information. This study looked at FL's main applications, including as IDS, malware and ransomware detection, and network traffic anomaly detection, highlighting how it may enhance security while maintaining data confidentiality. Furthermore, it was suggested that privacy-preserving strategies like Secure Model Aggregation, HE, and Differential Privacy on SMPC are crucial defenses against adversarial assaults like Byzantine and backdoor attacks. While FL offers significant advantages, challenges such as scalability, adversarial robustness, and communication overhead remain critical concerns.

Future research should focus on enhancing FL's resilience against adversarial threats, improving communication efficiency, and developing decentralized aggregation techniques to reduce reliance on a central server. The application of combining edge-based security frameworks, self-learning FL models, and blockchain technology may further boost FL in cybersecurity.

REFERENCES

[1] Ritesh Verma, "Cybersecurity Challenges In The Era Of Digital Transformation," *J. Informatic, Educ. Manag.*, pp. 178–186, Feb. 2024, doi: 10.25215/9392917848.20.

[2] A. V. Hazarika and M. Shah, "Distributed quantum computing models : Study of architectures and models for the distribution of quantum computing tasks across multiple quantum nodes," *Int. J. Sci. Res. Arch.*, vol. 13, no. 02, pp. 3719–3723, 2024, [Online]. Available: https://ijsra.net/sites/default/files/IJSRA-2024-2602.pdf

[3] V. V. Vegesna, "Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities," *Int. J. Mach. Learn. …*, vol. 5, no. 4, pp. 1–8, 2023.

[4] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated Learning: Navigating the Landscape of Collaborative Intelligence," *Electronics*, vol. 13, no. 23, p. 4744, Nov. 2024, doi: 10.3390/electronics13234744.

[5] P. Katari, "Decentralized Cybersecurity : Implementing Federated Learning in Threat Intelligence Networks Decentralized Cybersecurity : Implementing Federated Learning in Threat Intelligence Networks," *J. Informatics Educ. Res.*, vol. 1, no. 3, pp. 29–40, 2021.

[6] A. Khraisat, A. Alazab, S. Singh, T. Jan, and A. Jr. Gomez, "Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions," *ACM Comput. Surv.*, vol. 57, no. 1, pp. 1–38, Jan. 2024, doi: 10.1145/3687124.

[7] S. Bharati, M. R. H. Mondal, P. Podder, and V. B. S. Prasath, "Federated learning: Applications, challenges and future directions," *Int. J. Hybrid Intell. Syst.*, vol. 18, no. 1–2, pp. 19–35, May 2022, doi: 10.3233/HIS-220006.

[8] P. M. Mammen, "Federated Learning: Opportunities and Challenges," pp. 1–5, 2021.

[9] M. Moshawrab, M. Adda, A. Bouzouane, H. Ibrahim, and A. Raad, "Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives," *Electronics*, vol. 12, no. 10, p. 2287, May 2023, doi: 10.3390/electronics12102287.

[10] I. Kholod *et al.*, "Open-Source Federated Learning Frameworks for IoT: A Comparative Review and Analysis," *Sensors*, vol. 21, no. 1, p. 167, Dec. 2020, doi: 10.3390/s21010167.

[11] F. Olaoye and A. Egon, "Federated Learning for Privacy-Preserving Security Analytics," *EasyChair*, pp. 1–12, 2024.

[12] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-Preserving Aggregation in Federated Learning: A Survey," *IEEE Trans. Big Data*, vol. 14, no. 8, pp. 1–20, 2024, doi: 10.1109/TBDATA.2022.3190835.

[13] M. S. Akaash Vishal Hazarika, "Blockchain-based Distributed AI Models: Trust in AI model sharing," *Int. J. Sci. Res. Arch.*, vol. 13, no. 2, pp. 3493–3498, 2024.

[14] W. E. Mbonu, C. Maple, and G. Epiphaniou, "An End-Process Blockchain-Based Secure Aggregation Mechanism Using Federated Machine Learning," *Electronics*, vol. 12, no. 21, p. 4543, Nov. 2023, doi: 10.3390/electronics12214543.

[15] C. Hu, H. H. Liang, X. M. Han, B. A. Liu, D. Z. Cheng, and D. Wang, "Spread: Decentralized Model Aggregation for Scalable Federated Learning," in *Proceedings of the 51st International Conference on Parallel Processing*, Aug. 2022, pp. 1–12. doi: 10.1145/3545008.3545030.

[16] Y. Feng *et al.*, "A survey of security threats in federated learning," *Complex Intell. Syst.*, vol. 11, no. 2, p. 165, Feb. 2025, doi: 10.1007/s40747-024-01664-0.

[17] Y. Bi, Y. Li, X. Feng, and X. Mi, "Enabling Privacy-Preserving Cyber Threat Detection with Federated Learning," pp. 1–21, 2024.

[18] M. Aljanabi, Mohd Arfian Ismail, Raed Abdulkareem Hasan, and Junaida Sulaiman, "Intrusion Detection: A Review," *Mesopotamian J. CyberSecurity*, pp. 1–4, Jan. 2021, doi: 10.58496/MJCS/2021/001.

[19] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–146, 2019.

[20] K. Lu, "Network Anomaly Traffic Analysis," *Acad. J. Sci. Technol.*, vol. 10, no. 3, pp. 65–68, Apr. 2024, doi: 10.54097/8as0rg31.

[21] H. Zhou, G. Yang, H. Dai, and G. Liu, "PFLF: Privacy-Preserving Federated Learning Framework for Edge Computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1905–1918, 2022, doi: 10.1109/TIFS.2022.3174394.

[22] X. Li, M. Wen, S. He, R. Lu, and L. Wang, "A Privacy-Preserving Federated Learning Scheme Against Poisoning Attacks in Smart Grid," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16805–16816, May 2024, doi: 10.1109/JIOT.2024.3365142.

[23] O. O'Connor and T. Elfouly, "Federated Learning: A Paradigm Shift in Cybersecurity for Smart Grids," in *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Jul. 2024, pp. 821–824. doi: 10.1109/ISVLSI61997.2024.00163.

[24] B. Suneetha and R. Kesavan, "A Survey on Privacy-Preserving Communication Frameworks in Machine Learning for Cybersecurity Threat Detection," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, Dec. 2024, pp. 1354–1359. doi: 10.1109/ICUIS64676.2024.10866308.

[25] N. Moumni, F. Châabane, and F. Drira, "Privacy-Preserving Anomaly Detection in Smart Meter Data Via Federated Learning," in *2023 International Conference on Cyberworlds (CW)*, Oct. 2023, pp. 516–517. doi: 10.1109/CW58918.2023.00093.

[26] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, Jun. 2022, doi: 10.1109/JIOT.2022.3150363.

DOI: 10.48175/IJARSCT-25168