

An Intelligent Federated Learning Framework for Privacy-Aware Threat Detection in Secure Cloud Computing Environments

¹Dr Vemuri Sudarsan Rao, ²Dr Kavitha Guda, ³Dr.Macha Sarada

¹Associate Professor, Department of Computer Science and Engineering, Sri Chaitanya Institute of Technology and Research, Khammam, Telangana, India

¹Email: sudharshan.cse2008@gmail.com

²Associate Professor, Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, cheeryal(V), Medchal Dist, Hyderabad, Telangana -501301, India

²Email: kavitharddy.darshan@gmail.com

³Associate Professor, Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), Anurag Engineering College, Kodad, Suryapet, Telangana- 508206, India

³Email: saradaramaraok@gmail.com

ABSTRACT

The widespread adoption of cloud computing has enabled organizations to deliver scalable digital services and manage distributed computing resources efficiently. However, the continuous exchange of sensitive information across cloud infrastructures has intensified concerns regarding data confidentiality, user privacy, and cyber resilience. Conventional machine learning-based security solutions often rely on centralized data collection, which increases the risk of unauthorized data exposure, regulatory non-compliance, and privacy breaches. These limitations highlight the need for collaborative security mechanisms that can learn from distributed data while preserving its confidentiality. This study proposes an intelligent federated learning framework for privacy-aware cloud security that enables multiple cloud participants to jointly develop an effective threat detection model without sharing their raw datasets. The proposed framework performs local model training at each participating node and securely exchanges only encrypted model parameters for global model aggregation. This decentralized learning strategy minimizes data transmission, protects sensitive information from external

disclosure, and strengthens compliance with modern privacy requirements. Machine learning techniques are employed to recognize malicious behaviors, abnormal access patterns, and emerging cyber threats by learning from diverse security events generated across distributed cloud environments. The framework further incorporates secure aggregation and iterative model optimization to improve learning efficiency while maintaining data integrity and model robustness. The effectiveness of the proposed approach is assessed using standard performance metrics, including accuracy, precision, recall, F1-score, and communication efficiency, to evaluate both security performance and collaborative learning capability. Experimental analysis demonstrates that the federated learning framework achieves reliable threat detection while significantly reducing privacy risks associated with centralized data processing. By combining decentralized artificial intelligence, privacy-preserving model training, and collaborative threat intelligence, the proposed framework provides a scalable and secure solution for protecting modern cloud infrastructures against evolving cyber threats without compromising the confidentiality of

organizational data.

Keywords: Federated Learning, Cloud Security, Privacy-Preserving Machine Learning, Distributed Artificial Intelligence, Threat Detection, Secure Aggregation, Cybersecurity, Collaborative Learning, Cloud Computing, Data Privacy.

I. INTRODUCTION

Cloud computing has become an essential part of modern digital infrastructure because it provides flexible storage, scalable processing resources, and convenient access to services. Organizations from different sectors increasingly depend on cloud platforms to manage applications and large volumes of data. This rapid adoption has also expanded the range of security risks faced by cloud environments. Unauthorized access, data leakage, malicious activities, account compromise, and evolving cyberattacks continue to affect the confidentiality and reliability of cloud-based systems. As these threats become more complex, conventional rule-based security mechanisms may struggle to identify new and changing attack patterns.

Machine learning has introduced useful possibilities for strengthening cloud security by learning behavioral patterns from historical data and identifying suspicious activities. However, many traditional learning models depend on collecting information from multiple sources and storing it in a centralized location for training. Such an approach can create additional privacy concerns, particularly when the data contains confidential user records, organizational information, or security-related logs. Transferring sensitive data between different cloud nodes may also increase exposure to interception, misuse, and unauthorized disclosure.

Federated learning provides an alternative method in which a common model can be trained across distributed participants without requiring them to share their original

data. In this approach, each cloud node trains the model locally using its own information. Only the resulting model updates are sent to a coordinating server, where they are combined to improve the global model. The raw data remains within the local environment throughout the training process. This distributed learning strategy makes it possible to gain knowledge from multiple data sources while reducing direct movement of sensitive information.

The proposed Federated Learning Framework for Privacy-Preserving Cloud Security applies this collaborative learning concept to the protection of distributed cloud systems. Participating cloud nodes contribute to the development of a shared threat detection model while retaining control over their private datasets. Secure aggregation is used to combine local model updates and limit unnecessary exposure of individual contributions. The resulting global model can learn from diverse security patterns observed across different cloud environments and can therefore support the detection of suspicious or previously unseen activities.

The main purpose of this work is to create a balance between intelligent threat detection and data privacy. Instead of relying on centralized data collection, the framework supports collaborative security intelligence while preserving the confidentiality of local information. Such an approach can improve scalability, reduce privacy risks, and encourage cooperation among distributed cloud environments. The proposed system therefore offers a suitable foundation for developing adaptive and privacy-aware security solutions for modern cloud infrastructures.

II. LITERATURE SURVEY

1. Title: Achieving Security and Privacy in Federated Learning Systems: Survey, Research Challenges and Future Directions

Authors: Alberto Blanco-Justicia, Josep

Domingo-Ferrer, Sergio Martínez, David Sánchez, Adrian Flanagan, and Kuan Eeik Tan

Abstract: This study examines the major security and privacy concerns associated with federated learning systems. Although federated learning avoids direct transfer of local datasets, the exchange of model parameters may still reveal sensitive information. The authors discuss threats such as model poisoning, inference attacks, and malicious client participation. Different protection mechanisms are reviewed to understand their ability to preserve private information without reducing learning performance. The work also points out that achieving privacy and security at the same time remains a difficult challenge. It provides useful research directions for developing federated systems that are resistant to attacks while maintaining the confidentiality of participating users.

2. Title: From Distributed Machine Learning to Federated Learning: In the View of Data Privacy and Security

Authors: Sheng Shen, Tianqing Zhu, Di Wu, Wei Wang, and Wanlei Zhou

Abstract: The authors study the transition from conventional distributed machine learning toward federated learning from a privacy and security perspective. The work explains how local devices can participate in collaborative model development while retaining their original information. It reviews important privacy mechanisms, including differential privacy, secure aggregation, and secure multiparty computation. The study also identifies possible attacks against federated systems and discusses how adversaries may exploit model updates. The findings indicate that federated learning provides a strong foundation for distributed intelligence, but additional protection is required to secure the complete learning process.

3. Title: Privacy-Preserving Aggregation

in Federated Learning: A Survey

Authors: Ziyao Liu, Jiale Guo, Wenzhuo Yang, Jiani Fan, Kwok-Yan Lam, and Jun Zhao

Abstract: This research focuses on privacy-preserving aggregation, which is one of the central security operations in federated learning. The study reviews methods that allow a central coordinator to combine model updates without directly exposing the contribution of individual clients. Different aggregation protocols are compared in terms of privacy, computational cost, communication requirements, and practical limitations. The authors also examine available federated learning frameworks that support privacy-aware aggregation. The work shows that secure aggregation can significantly reduce information leakage, although scalability and system efficiency remain important concerns in large distributed environments.

4. Title: Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Internet of Things Systems

Authors: S. A. Mahmud et al.

Abstract: This study introduces a federated learning approach for detecting intrusions across diverse IoT environments while keeping sensitive records on local devices. Instead of transferring raw network traffic to a centralized server, participating nodes train local models and share only learned parameters. The framework applies the Federated Averaging algorithm to combine local knowledge and repeatedly improve a global detection model. The research demonstrates the usefulness of collaborative learning for identifying cyber threats without depending on centralized data collection. This approach is particularly relevant to cloud-connected systems where privacy, distributed data ownership, and security monitoring must operate together.

5. Title: NIDS-FGPA: A Federated Learning Network Intrusion Detection

Algorithm Based on Gradient Similarity and Paillier Encryption

Authors: J. M. Wang et al.

Abstract: The study proposes a network intrusion detection method that combines federated learning with secure model aggregation. A gradient-similarity strategy is introduced to improve the way updates from distributed clients are combined. Paillier homomorphic encryption is also used to protect information exchanged during collaborative training. The framework attempts to address two important concerns: maintaining the confidentiality of participant updates and reducing the influence of unsuitable local models. The results suggest that combining intelligent aggregation with encryption can strengthen privacy-aware intrusion detection in distributed network environments.

6. Title: Federated Learning with SCNN-Bi-LSTM for Enhanced Intrusion Detection in Wireless Sensor Networks

Authors: S. M. S. Bukhari et al.

Abstract: This research presents a hybrid deep learning approach that combines a stacked convolutional neural network with a bidirectional long short-term memory model. Federated learning is used to enable sensor nodes to train collaboratively without exposing their private datasets. The convolutional layers extract important traffic characteristics, while the bidirectional recurrent component learns sequential attack patterns. By keeping data at individual nodes, the proposed approach reduces privacy risks associated with centralized training. The work indicates that deep learning and federated collaboration can jointly improve threat recognition in distributed and resource-sensitive network environments.

7. Title: Federated Learning for Cybersecurity: A Privacy-Preserving Approach for Intrusion Detection and Malware Classification

Authors: E. M. Timofte et al.

Abstract: The authors develop a federated cybersecurity framework for intrusion detection and malware classification. The proposed approach allows decentralized participants to improve a common security model while their original datasets remain within their local environments. The study considers the need to maintain useful detection performance while reducing communication overhead and protecting data privacy. Its findings show that federated learning can support collaborative cyber defence across distributed systems. The work is closely related to cloud security because it demonstrates how multiple independent nodes can contribute to shared threat intelligence without centralizing sensitive information.

III. EXISTING SYSTEM

In the existing cloud security environment, most threat detection systems follow a centralized learning process. Security-related information, including network traffic records, access logs, user activities, and attack details, is collected from different cloud sources and moved to one central server. The machine learning model is then trained using the combined dataset. Although this method allows the model to learn from a large amount of information, it also creates a major privacy concern because sensitive records must leave their original location.

Centralized data storage can become an attractive target for attackers. If the central server is compromised, a large collection of private and organizational information may be exposed at once. Data transfer between cloud nodes and the main server can also increase the chance of leakage or unauthorized interception. In many cases, organizations may be unwilling to share their security logs because these records can contain confidential details about internal systems, users, and network behaviour.

Another limitation is that conventional cloud security models often depend on data

gathered from a single environment. As a result, the trained model may perform well on familiar attacks but may fail when it encounters threat patterns from other cloud platforms. Differences in data distribution, infrastructure, and user behaviour can further reduce detection accuracy. Existing approaches also require frequent movement of large datasets, which increases communication cost and creates additional storage requirements.

Therefore, the existing system faces difficulties in maintaining both effective threat detection and data privacy. The dependence on centralized data collection increases security risks and restricts collaboration between independent cloud environments. These limitations create a need for a distributed learning approach in which cloud nodes can jointly improve a security model without sharing their original sensitive data.

IV. PROPOSED SYSTEM

The proposed system introduces a federated learning framework to improve cloud security without collecting sensitive information in a central location. In this framework, several cloud nodes take part in the learning process while keeping their original datasets within their own environments. Each node trains a local security model using its network traffic, access records, or other available security data. Instead of sending raw information to the central server, only the learned model updates are shared. These updates are combined through a secure aggregation process to build an improved global model, which is then returned to the participating nodes for further training. This process continues for several communication rounds, allowing the model to learn from diverse attack patterns observed across different cloud environments. The proposed approach reduces direct data exposure, limits unnecessary data transfer, and supports

collaborative threat detection among independent cloud systems. By combining local learning, secure model aggregation, and global knowledge sharing, the system aims to detect suspicious activities more effectively while preserving the confidentiality of cloud data.

V. SYSTEM ARCHITECTURE

The system architecture presents a federated learning environment developed to strengthen cloud security while keeping sensitive information private. The framework consists of several independent cloud nodes, a central aggregation server, a global model distribution mechanism, security applications, and an administrative monitoring interface. Unlike conventional centralized approaches, the proposed architecture does not require the participating cloud nodes to transfer their original datasets to a common storage location.

Each cloud node maintains its own private dataset, which may include network traffic details, login activities, access logs, and security events. Local model training is performed separately at every node using the data available within that particular environment. Since the original records remain inside the corresponding cloud node, confidential information is not directly exposed during the collaborative learning process. After local training, only the learned model updates are prepared for transmission. The generated model updates are encrypted before being sent to the central aggregation server. Updates received from Cloud Node 1, Cloud Node 2, and other participating nodes are combined through a secure aggregation process. The aggregation server does not access the raw datasets of individual participants. Instead, it brings together the useful knowledge learned by the local models and uses the combined updates to construct an improved global model.

Once the global model is created, it is distributed back to all participating cloud

nodes. Each node receives the updated model and can use it as the basis for the next local training cycle. This repeated exchange allows knowledge gained from different cloud environments to contribute to the overall learning process. As a result, a threat pattern identified at one node can indirectly help other nodes improve their security capabilities without exposing the data from which the pattern was learned.

The trained global model supports several security operations, including threat detection, anomaly detection, attack prediction, security alert generation, and analytical reporting. Detected security events are made available to the security analyst or system administrator through the monitoring interface. The administrator can review alerts and reports, observe suspicious activities, and take suitable action when a potential threat is identified.

Overall, the architecture combines private local training, encrypted model exchange, secure aggregation, and collaborative threat intelligence within a single framework. Its key strength is that raw data never needs to be shared among the participating cloud environments. This design helps reduce privacy risks while allowing multiple nodes to jointly build a more informed and adaptive cloud security model.

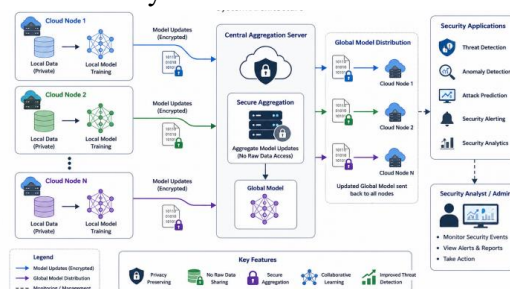


Fig 5.1: System Architecture

VI. IMPLEMENTATION

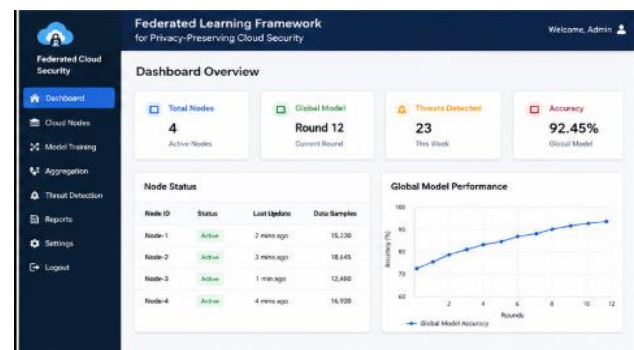


Fig 6.1: Dashboard

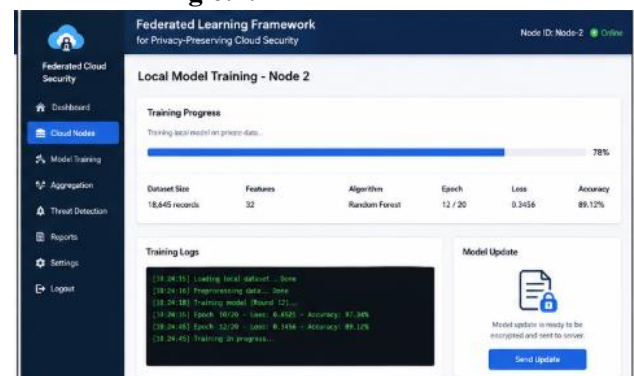


Fig 6.2: Model Training



Fig 6.3: Secure Aggregation Server

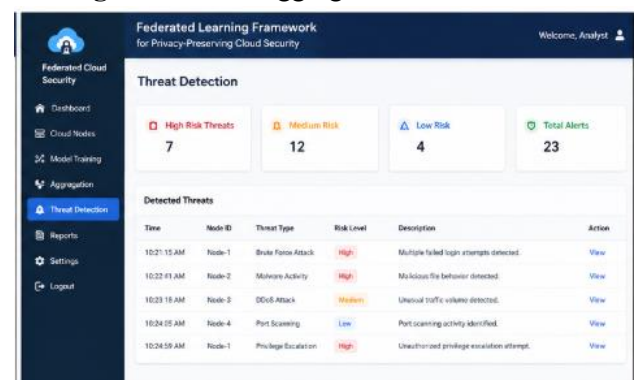


Fig 6.4: Threat Detection Results

VII. CONCLUSION

The proposed Federated Learning Framework for Privacy-Preserving Cloud Security offers a practical way to improve threat detection without requiring sensitive information to be collected at a central location. By training models directly within individual cloud nodes and exchanging only learned updates, the framework keeps raw data under local control throughout the learning process. Secure aggregation combines knowledge from multiple participants and produces a global model capable of recognizing diverse security threats. The developed system supports activities such as anomaly identification, attack detection, security alerting, and continuous monitoring while reducing the privacy risks associated with conventional centralized learning. Overall, the framework shows that collaborative intelligence and data confidentiality can work together to build a more adaptive and privacy-aware security mechanism for distributed cloud environments.

VIII. FUTURE SCOPE

In the future, the proposed framework can be extended to handle larger and more complex multi-cloud environments with a greater number of participating nodes. Advanced privacy methods such as differential privacy, homomorphic encryption, and blockchain-based model verification can be incorporated to provide stronger protection against information leakage and malicious updates. The system can also be enhanced with deep learning models to identify sophisticated zero-day attacks and rapidly changing threat patterns. Further work may focus on reducing communication overhead, improving training speed, and selecting trustworthy cloud nodes during the aggregation process. Support for real-time threat intelligence and automated incident response could make the framework more useful in practical cloud deployments. These

improvements can help the system become more scalable, secure, and suitable for protecting future distributed cloud infrastructures.

REFERENCES

- [1] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A Survey on Security and Privacy of Federated Learning," *Future Generation Computer Systems*, vol. 115, pp. 619–640, 2021. doi: 10.1016/j.future.2020.10.007.
- [2] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and Security in Federated Learning: A Survey," *Applied Sciences*, vol. 12, no. 19, Art. no. 9901, 2022. doi: 10.3390/app12199901.
- [3] N. Truong, K. Sun, S. Wang, F. Guitton, and Y. Guo, "Privacy Preservation in Federated Learning: An Insightful Survey From the GDPR Perspective," *Computers & Security*, vol. 110, Art. no. 102402, 2021. doi: 10.1016/j.cose.2021.102402.
- [4] M. Asad, A. Moustafa, and T. Ito, "FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning," *Applied Sciences*, vol. 10, no. 8, Art. no. 2864, 2020. doi: 10.3390/app10082864.
- [5] G. Liu, C. Wang, X. Ma, and Y. Yang, "Keep Your Data Locally: Federated-Learning-Based Data Privacy Preservation in Edge Computing," *IEEE Network*, vol. 35, no. 2, pp. 60–66, 2021. doi: 10.1109/MNET.011.2000215.
- [6] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7751–7763, 2020. doi: 10.1109/JIOT.2020.2991401.
- [7] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, "Privacy-Preserved Federated Learning for Autonomous Driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8423–8434, 2022. doi:

- 10.1109/TITS.2021.3081560.
- [8] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated Learning for Healthcare Informatics," *Journal of Healthcare Informatics Research*, vol. 5, pp. 1–19, 2021. doi: 10.1007/s41666-020-00082-4.
- [9] R. Lazzarini, H. Tianfield, and V. Charissis, "Federated Learning for IoT Intrusion Detection," *AI*, vol. 4, no. 3, pp. 509–530, 2023. doi: 10.3390/ai4030028.
- [10] X. Jin, Q. Zhou, X. Li, and S. Wu, "Efficient Secure Aggregation for Privacy-Preserving Federated Learning," *Journal of University of Science and Technology of China*, 2024. doi: 10.52396/JUSTC-2022-0116.
- [11] T. Eltaras, F. Sabry, W. Labda, K. Alzoubi, and Q. Ahmedeltaras, "Efficient Verifiable Protocol for Privacy-Preserving Aggregation in Federated Learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2977–2990, 2023. doi: 10.1109/TIFS.2023.3272591.
- [12] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, "Achieving Security and Privacy in Federated Learning Systems: Survey, Research Challenges and Future Directions," *Engineering Applications of Artificial Intelligence*, vol. 106, Art. no. 104468, 2021. doi: 10.1016/j.engappai.2021.104468.
- [13] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Privacy-Preserving Aggregation in Federated Learning: A Survey," *IEEE Transactions on Big Data*, vol. 10, no. 2, pp. 157–177, 2024. doi: 10.1109/TBDATA.2022.3190835.
- [14] A. Khraisat, A. Alazab, and A. Alazab, "Survey on Federated Learning for Intrusion Detection Systems: Concepts, Architectures, Aggregation Strategies, Challenges, and Future Directions," *ACM Computing Surveys*, vol. 57, no. 4, 2025. doi: 10.1145/3687124.
- [15] E. M. Timofte et al., "Federated Learning for Cybersecurity: A Privacy-Preserving Approach for Intrusion Detection and Malware Classification," *Applied Sciences*, vol. 15, no. 12, Art. no. 6878, 2025. doi: 10.3390/app15126878.
- [16] E. Hallaji, R. Razavi-Far, M. Saif, B. Wang, and Q. Yang, "Decentralized Federated Learning: A Survey on Security and Privacy," *IEEE Transactions on Big Data*, vol. 10, no. 2, pp. 194–213, 2024. doi: 10.1109/TBDATA.2024.3362191.
- [17] B. Guembe, S. Misra, and A. Azeta, "Privacy Issues, Attacks, Countermeasures and Open Problems in Federated Learning: A Survey," *Applied Artificial Intelligence*, vol. 38, no. 1, 2024. doi: 10.1080/08839514.2024.2410504.
- [18] Q. Han, S. Lu, W. Wang, H. Qu, J. Li, and Y. Gao, "Privacy Preserving and Secure Robust Federated Learning: A Survey," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 13, Art. no. e8084, 2024. doi: 10.1002/cpe.8084.
- [19] A. Rahdari, E. Keshavarz, E. Nowroozi, R. Taheri, M. Hajizadeh, M. Mohammadi, S. Sinaei, and T. Bauschert, "A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 3710–3744, 2025. doi: 10.1109/OJCOMS.2025.3560034.
- [20] H. Wang, T. Yang, Y. Ding, S. Tang, et al., "VPPFL: Verifiable Privacy-Preserving Federated Learning in Cloud Environment," *IEEE Access*, vol. 12, 2024. doi: 10.1109/ACCESS.2024.3472467.
- [21] P. Kairouz et al., "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, nos. 1–2, pp. 1–210, 2021. doi: 10.1561/22000000083.
- [22] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep

Networks From Decentralized Data,” in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[23] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, “Federated Learning: Strategies for Improving Communication Efficiency,” NIPS Workshop on Private Multi-Party Machine Learning, 2016.

[24] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated Machine Learning: Concept and Applications,” ACM Transactions on Intelligent Systems and Technology, vol. 10, no. 2, Art. no. 12, 2019. doi: 10.1145/3298981.

[25] K. Bonawitz et al., “Practical Secure Aggregation for Privacy-Preserving Machine Learning,” in Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS), 2017, pp. 1175–1191. doi: 10.1145/3133956.3133982