Proceedings of the 4th International Conference on Applied Artificial Intelligence and Computing (ICAAIC-2025)
DVD Part Number: CFP25BC3-DVD; ISBN: 979-8-3315-6586-2

A Study on Privacy-Focused Machine Learning in IoT Networks via Federated Learning

[1*]Jisna Jaison T
[1*]*Student (Research Scholar), Department of CSE,*
VISTAS, Chennai, India.
[1*]Corresponding author email id: jianajaisont@gmail.com

[2]Dr. Thilakavathy. P
[2]*Assistant Professor, Department of CSE,*
VISTAS, Chennai, India.
Email id: thilakavathy.se@velsuniv.ac.in

***Abstract*—The proliferation of Internet-connected Things (Iot) devices has ushered in an era of unprecedented data generation at the network's edge. Leveraging this data for the artificial intelligence applications presents privacy challenges. Federated learning (FL) offers a viable solution. This study investigates the implementation and enhancement of FL within IoT environments, focusing on communication efficiency, model aggregation, and device compatibility. The methodology is grounded in analytical principles. employing deductive reasoning and descriptive design. Secondary data is gathered from published research and technical documentation. The findings underscore the significance of secure communication protocols like secure socket layer (SSL) for robust data encryption and message Queue Telemetry Transport (MQTT) for efficient messaging. Additionally, the paper examines how aggregation strategies influence model convergence, with Federated Averaging providing efficient convergence and secure Aggregation ensuring anonymity when privacy is paramount. Further, the research evaluates algorithm optimization techniques- Including model pruning, Quantization, and Lightweight Cognitive Architectures- that enhance model performance on resource constrained IoT devices.**

Keywords: **Cryptographic Techniques, Federated learning, Internet of Things, Networking Capabilities, Numerous Decentralized Devices**

I. INTRODUCTION

A. Research background

The proliferation of Internet of Things(IoT)devices has generated unprecedented volumes of data at the edge of networks. These devices, from simple sensors to intelligent appliances, collect extensive information about the physical environment [1]. A significant challenge is utilizing this data for machine learning while ensuring user privacy. Traditional approaches, involving frequent data collection and centralized storage, pose considerable privacy and security risks. Federated Leaning (FL) offers a privacy -preserving alternative by enabling decentralized model training directly on devices. Rather than transmitting raw data, FL shares only model updates, thereby safeguarding sensitive information and maintaining confidentiality [2].

B. Aim and Objective of Research:

Research Aim: The objective of this study is to develop and rigorously evaluate a robust federated learning framework specifically tailored for Internet of Things (IoT) networks, with an emphasis on securing privacy within machine learning algorithms.

C. Objectives:

- To design a reliable protocol that facilitates secure interconnection between Iot devices and the central server, ensuring seamless and safe model updates.
- To develop a federated aggregation mechanism capable of efficiently integrating local model updates while preserving the privacy of each individual device.
- To adapt federated learning techniques for IoT devices with limited computational and communication resources.
- To evaluate the proposed approach in comparison with conventional centralized methods, considering factors such as privacy preservation, model accuracy, and communication overhead.

D. Research Rationale

Traditional centralized systems pose significant risks to privacy and security, especially when IoT devices generate massive volumes of personally identifiable information at the edge of the network. To enable collaborative model training while preserving raw data confidentiality, Federated Learning (FL) emerges as a promising alternative [4]. This study focuses on enhancing and applying FL in IoT environments to address key challenges such as efficient communication, model aggregation, and device heterogeneity.

II. LITERATURE REVIEW

In Federated Learning in IoT Networks:a Privacy-Preserving Paradigm (2.1), Federated Learning (FL) is presented as an advanced machine learning methodology specifically adapted to the distributed architecture of IoT ecosystems [5]. FL enhances data security by enabling devices to perform training locally using sensor or environment generated information, thereby eliminating the need to transfer unprocessed data beyond the device boundary. This decentralized approach is particularly important for safeguarding sensitive and privacy- critical information.

Instead of sharing raw datasets, participating devices transmit only model parameters or updates to a central server for aggregation [6]. Furthermore, FL reduces communication overhead, making it highly suitable in scenarios with limited bandwidth availability or when handling large-scale data.

In Communication Protocols for Secure Model Updates in Federated Learning (2.2), reliable communication mechanisms play a critical role in autonomous Iot networks, ensuring the confidentiality and integrity of information exchanges during model updates [7]. These protocols define the rules and procedures for transmitting model parameters between IoT devices and the central server. By Incorporating security techniques such as encryption and authentication, they safeguard against unauthorized access and potential transmission vulnerabilities. Moreover, in resource-constrained IoT environments, these protocols help optimize communication by reducing latency and bandwidth consumption [8][9]. Therefore, a robust protocol framework is essential for the efficient and secure deployment of federated learning systems. Figure 1 presents a Secure Smart Communication Efficiency

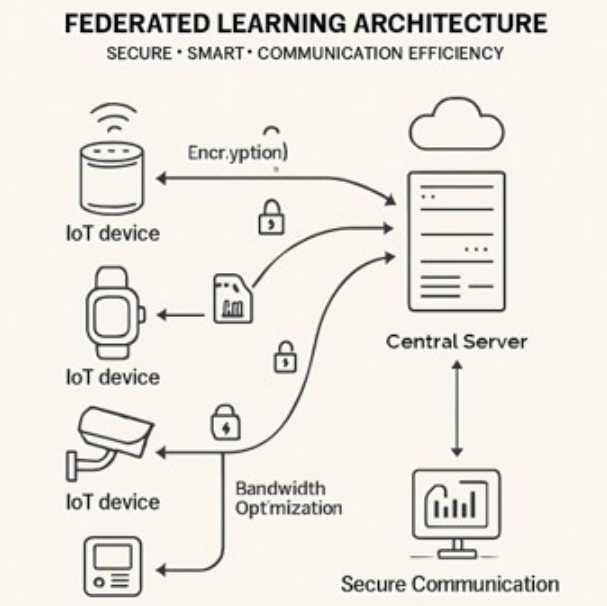

Figure.1: Secure Smart Communication Efficiency [10]

In Aggregation Mechanisms in Federated Learning for IoT Devices (2.3), aggregation processes are identified as essential components facilitating the integration of locally trained model updates with the global federated model across interconnected IoT devices. These mechanisms are fundamental not only for preserving privacy but also for collaboratively enhancing the performance of the global model. Common practices include the use of weighted averaging, secure aggregation protocols, and specialized confidentiality - preserving techniques [11],[12],[13]. Weighted averaging for example, assigns significance to each local update based on factors such as data quality or device computational capability, ensuring a balanced and representative fusion of contributions. Throughout the aggregation process, individual updates remain confidential, maintaining the privacy of participants.

To further safeguard data privacy, an additional security layer - such as introducing noise or perturbations to model updates- should be implemented [14]. This practice is particularly vital in the resource-constrained environment of IoT networks, as it supports accuracy while simultaneously upholding user privacy. Here the real values from specific time are collected and generated further values using with this it can predict also.

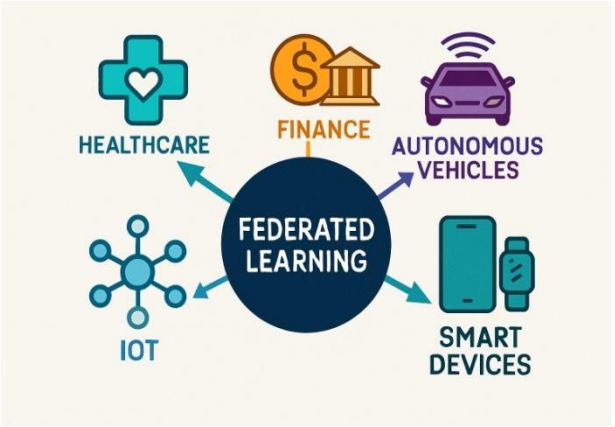

Figure. 2: Application of Federated Learning

Figure 2 presents a Application of federated learning. Federated Learning for IoT Devices In Optimizing Machine Learning Algorithms for Federated Learning on IoT Devices (2.4), algorithmic optimization is recognized as a critical factor for achieving efficient and cost-effective model development in resource-limited environments. Owing to the limited processing power and memory of IoT devices, conventional machine learning algorithms are often impractical, necessitating targeted adaptations [15],[16]. Key techniques include model quantization and the design of lightweight architectures, both of which reduce computational demands. Model pruning is also employed to decrease model complexity, making deployment across multiple IoT devices more feasible. Quantization, by encoding numerical values with lower precision, further decreases computational and memory requirements [17]. Collectively, these optimization strategies enable the implementation of federated learning on IoT devices, ensuring privacy protection through artificial intelligence while maintaining model accuracy and conserving device resources [18].

A. Literature Gap

Current research on collaborative learning among IoT devices primarily focuses on performance and the technological implementation. However, there is a significant lack of systematic approaches to privacy protection, communication protocols, and algorithm optimization for connected devices. To effectively implement federated learning and teaching methods, these gaps must be addressed.

III. METHODOLOGY

This research focuses on applying federated learning (FL) within Internet of Things networks under an interpretive research perspective that highlights human understanding and decision-making [4],[3],[19]. Due to privacy and ethical constraints in collecting real-world IoT data, the study relies on secondary sources such as academic literature, technical reports, and existing FL-IoT implementations. The approach integrates secure communication (SSL), lightweight

messaging (MQTT), and aggregation techniques that weight device contribution based on reliability [20].

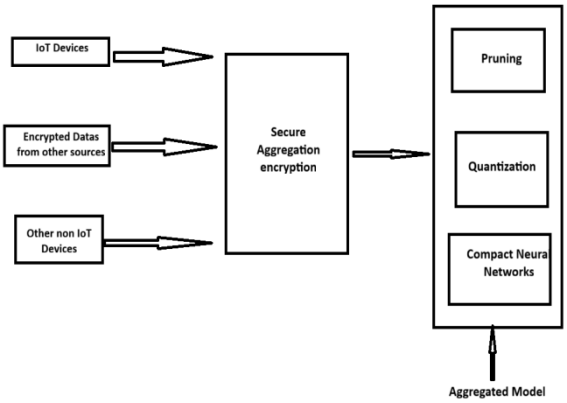

Figure .3: Model Representation

To address Iot resource limitations, the framework adopts encryption based secure aggregation, pruning, quantization, and compact neural network architectures [21],[22]. By combining privacy-preserving and optimization methods, the study provides a practical direction for implementing federated learning in Iot ecosystems.

IV. RESULTS

A. Theme: Performance Evaluation of Communication Protocols

In the context of applying federated learning within IoT networks, it is essential to evaluate how effectively and efficiently communication occurs between IoT devices and the central server. To address this, rigorous testing was conducted on two key communication protocols: Secure Socket Layer (SSL), which provides encrypted and secure data transfer, and Message Queuing Telemetry Transport (MQTT), a lightweight messaging protocol designed for resource-constrained IoT environments.

SSL Protocol: Strong encryption capabilities of the SSL protocol were demonstrated, ensuring secure transmission of information between devices connected to the internet and the main server [23],[30]. The assessment found consistently modest levels of exposure to listening devices or illegal access attempts. The low overhead found in latency measurements supported the system's potential for applications that operate in real-time [31]. The computational requirements for creating and maintaining SSL connections, particularly on IoT devices with limited resources, were noticed. Figure 4 explains about the Evaluation of communication protocols.

MQTT Protocol: Regarding the transport of lightweight messages, MQTT performed admirably [32]. For disseminating model updates over the network, their publish-subscribe strategy has shown to be quite effective. It is useful for applications that require time because latency measurements showed little delay. MQTT was found to be vulnerable to some security threats, nonetheless, which emphasizes the significance of using strong security procedures while using this protocol [33]. Both the SSL as well as MQTT protocols performed well under the federation of learning framework, exhibiting both their strengths and weaknesses. The cost for SSL demonstration is high but it assures the security of data [34

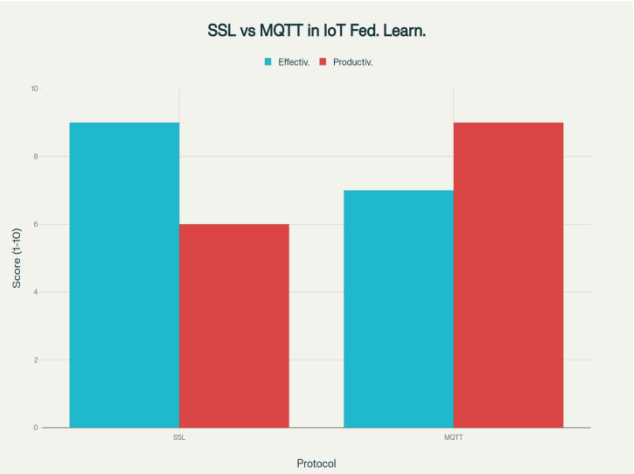

Figure. 4: Evaluation of Communication Protocols].

B. Theme: Impact of Aggregation Mechanisms on Model Convergence

An important component of the federated learning method for IoT networks is the effect of aggregation on convergence models [24][35]. The two main processes of federated standardization and Trusted aggregation were using to examine and determine, how they affected the resulting the convergence of the overall model.

Federated Averaging: The convergence of model was efficient thought out the IoT using federated averaging. It gives a weights to individual inputs depending on things like data integrity and hardware capability [36]. This technique shows a smooth trajectory of convergence, showing that updates from each and every device can be integrated into overall model [37]. But it requires careful updation of weights to each devices data based on its capability [25].

Secure Aggregation: The methods like homomorphic cryptography, secure aggregate protect privacy throughout the aggregate process. It helps to keep the sensitive data private [38]. In otherwise to non-encrypt techniques may cause slower converge rates. When correct convergence required a proportional contribution from all devices, federated averaging performed exceptionally well [39]. On the other hand, Secure aggregation helps a solid response for circumstances involving privacy protection. Figure 5 explain about the Model Convergence Aggregation Mechanisms.

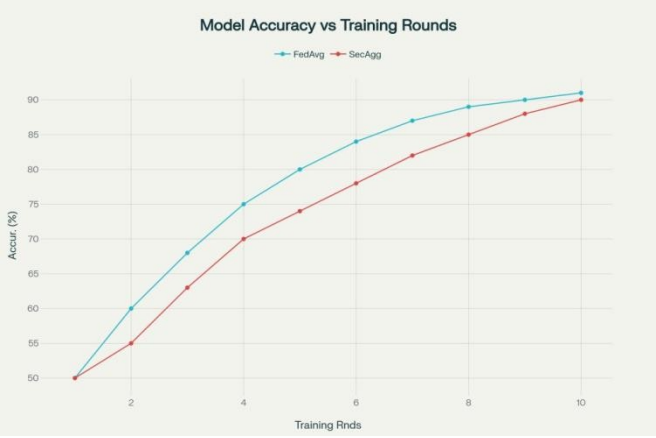

Figure. 5: Model Convergence Aggregation Mechanisms

C. Theme: Optimized Algorithms for IoT Devices:

It is important to optimise the techniques or algorithms used for machine learning in IoT devices for the

effective and accurate model training in based on the limited resources [40]. The three main and crucial methods were modeling pruning, Quantization, and also lightweight cognitive buildings.

Model pruning: It have the advantages in lowering the computing needs of models based on machine learning in IoT devices [41]. It took into consider the important unavoidable data and remove the less needed functionality and parameters [42]. It helps to maintain less memory space and effective working and processing power.

Quantization: The use of lower bit precision representation of numerical values were helping to lower memory usage and computing requirements [43]. Thus the size can be effectively reduced. It results speeder computation and greater memory economy [44]

Lightweight Neural Architectures:

The designing of framework suitable for less resourced devices helps to interoperatibility of those kind of IoT devices [45]. This helps to less computing and keeps great accuracy in prediction. Modelling pruning, Quantization, as well as lightweight neural architecture all showed distinct advantages in the adaptation of machine learning strategies [47].

D. Theme: Comparative Analysis with Centralized Approaches

In the framework of IoT networks, a comparison of centralized as well as federated learning methodologies offers useful insights into the advantages and disadvantages of each strategy [48]. The preservation of confidentiality and interpersonal overhead were the two main factors that were assessed.

Privacy Preservation: Federated Learning does a fantastic job protecting user privacy, which is essential in connected devices where confidential information is produced and processed [49]. By fashion, Federated Learning makes sure that only model updates are sent to a centralized server, never any raw data. By doing this, the possibility of breaches of information or illegal access is greatly reduced. A central server is where raw data is combined in centralized systems, potentially putting the security of valuable information at risk.

Communication Overhead: Federated Learning shown to be superior in cutting down on communication costs [50]. The total amount of data transferred between gadgets and the main computer is greatly reduced because only model changes and not whole datasets are sent. This is especially helpful insituations where band width is constrained or the amount of data are large, which are typical of internet of things networks [51]. Centralized methods, on the other hand, need for the transmission of full datasets, resulting in greater communication costs.

V. CONCLUSION

This study offers a thorough and organized examination of a significant issue in the fields of automated learning and IoT. Its focus is on federated learning as a means for safeguarding privacy computer learning within IoT networks. The study skillfully integrates a logical methodology with an interpretive analytical attitude, enabling a thorough evaluation of the technical details involved. Given the difficulties in acquiring practical problems IoT datasets, it is practical to adopt a design that is descriptive as well as secondary data gathering approach. The technological methodology is strong and painstakingly carried out, offering insightful information on methods of communication, aggregation techniques, and algorithms optimizations designed for IoT devices. The analysis of Ubiquitous Averaging, Private Aggregation, and SSL/MQTT protocols reveals implementation-related practical consequences. Additionally, Models Pruning, Quantization, as well as Lightweight Structures are sound optimization strategies. However, a more thorough examination of potential drawbacks and useful considerations when using Federated Learning in various IoT scenarios might be beneficial to the research. Additionally, experimental or simulation-based confirmation by evidence would increase the conclusions' trustworthiness.

VI. FUTURE WORK

There are various intriguing directions for further investigation in the area of federation of learning with Privacy-Preserving Artificial Intelligence in Sensor Networks: Dynamic Model Personalization: Investigate methods for dynamically adapting global models in light of the changing traits and preferences of specific IoT gadgets [54]. This would improve the performance and adaptability of the model in changing circumstances. Adaptive Communication Protocols: Develop adaptable methods of communication whose can change dynamically in response to network Under certain circumstances, device capacity, and privacy demands. This would enhance the effectiveness and responsiveness of communication. Multi-Modal Federated Learning: Expand the scope of the research to include situations when IoT devices produce a variety of data formats, such as photos, text, and sensor readings [55]. Create methods for processing and integrating multiple modalities of data within a diversified learning framework. Incorporating Federated Learning into IoT Standards: To ensure broad acceptance and interoperability, work with standardization organizations to include federated teaching protocols and methodology into IoT standards for the industry.

DECLARATIONS:

Funding

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

Conflicts of Interest

The authors declare that we have no conflict of interest.

Competing Interests

The authors declare that we have no competing interest.

Data Availability Statement

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

REFERENCES

[1] Zheng, J., Li, K., Mhaisen, N., Ni, W., Tovar,E. and Guizani, M.,2022. Exploring Deep-Reinforcement-Learning-Assisted federated learning for Online Resource Allocation in Privacy-Preserving EdgeIoT. *IEEE Internet of Things Journal*, *9*(21), pp.21099-21110.

[2] Tabassum, A., Erbad, A., Lebda, W., Mohamed, and Guizani, M., 2022. Fedgan-ids: Privacy-preserving ids using gan and federated learning. *Computer Communications*,*192*, pp.299-310.

[3] Qi, Y., Hossain, M.S., Nie, J. and Li, X., 2021. Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, *117*, pp.328-337.

[4] Briggs, C., Fan, Z. and Andras, P., 2021. A review of privacy-preserving federated learning for the Internet-of-Things. *Federated Learning Systems: Towards Next-Generation AI*, pp.21-50.

[5] Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. 2022. Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. *IEEE transactions on network science and engineering*, *10*(5), 2864-2880.

[6] Yin, L., Feng, J., Xun, H., Sun, Z. and Cheng, X., 2021. A privacy-preserving federated learning for multiparty data sharing in social IoTs. *IEEE Transactions on Network Science and Engineering*, *8*(3), pp.2706-2718.

[7] Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., ... & Liu, Y. (2020). Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal*, *8*(3), 1817-1829.

[8] Zhang, Z., Guan, C., Chen, H., Yang, X., Gong, W., & Yang, A. (2021). Adaptive privacy-preserving federated learning for fault diagnosis in internet of ships. *IEEE Internet of Things Journal*, *9*(9), 6844-6854.

[9] Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2022). Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, *19*(1), 1080-1087.

[10] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388.

[11] Ruzafa-Alcázar, P., Fernández-Saura, P., Mármol-Campos, E., González-Vidal, A., Hernández-Ramos, J.L., Bernal-Bernabe, J. and Skarmeta, A.F., 2021. Intrusion detection based on privacy-preserving federated learning for the industrial IoT. *IEEE Transactions on Industrial Informatics*, *19*(2), pp.1145-1154.

[12] Venkataramanan, V., Kaza, S. and Annaswamy, A.M., 2022. DER Forecast Using Privacy-Preserving Federated Learning. *IEEE Internet of Things Journal*, *10*(3), pp.2046-2055.

[13] Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H.and Zhang, Y., 2020. Privacy-preserving federated learning in fog computing. *IEEE Internet of Things Journal*, *7*(11), pp.10782-10793.

[14] Wan, Y., Qu, Y., Gao, L. andXiang, Y., 2022. Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing. *Computer Networks*, *204*, p.108671.

[15] Wazzeh, M., Ould-Slimane, H., Talhi, C., Mourad,A.andGuizani,M.,2022. Privacy-preserving continuous authentication for mobile and iot systems using warmup-based federated learning. *IEEE Network*.

[16] Qu, Y., Xu, C., Gao, L., Xiang, Y. and Yu, S., 2022. Fl-sec: Privacy-preserving decentralized federated learning using signsgd for the internet of artificially intelligent things. *IEEE Internet of Things Magazine*, *5*(1), pp.85-90.

[17] Zhao, B., Fan, K., Yang, K., Wang, Z., Li, H. andYang,Y.,2021.Anonymousandprivacy-preserving federated learning with industrial big data. *IEEE Transactions on Industrial Informatics*, *17*(9), pp.6314-6323.

[18] Ma,J.,Naas,S.A.,Sigg,S.andLyu,X.,2022. Privacy-preserving federated learning based on multi-key homomorphic encryption. *International Journal of Intelligent Systems*, *37*(9), pp.5880-5901.

[19] Wen, M., Xie, R.,Lu,K.,Wang,L.andZhang, K., 2021. Feddetect: A novel privacy-preserving federated learning framework for energy theft detection in smart grid. *IEEE Internet of Things Journal*, *9*(8), pp.6069-6080.

[20] Lu,X.,Liao,Y.,Lio,P.andHui,P.,2020.Privacy-preserving asynchronous federated learning mechanism for edge network computing. *IEEE Access*, *8*, pp.48970-48981.

[21] Nagar, A., 2019. Privacy-preserving blockchain based federated learning withdifferential data sharing. *arXiv preprint arXiv:1912.04859*.

[22] Deng, R., Du, X., Lu, Z., Duan, Q., Huang, S. C., & Wu, J. (2023, July). HSFL: Efficient and privacy-preserving offloading for split and federated learning in IoT services. In *2023 IEEE International Conference on Web Services (ICWS)* (pp. 658-668). IEEE.

[23] Zheng, C., Liu, S., Huang, Y., Zhang, W., & Yang, L. (2022). Unsupervised recurrent federated learning for edge popularity prediction in privacy-preserving mobile-edge computing networks. *IEEE Internet of Things Journal*, *9*(23), 24328-24345.

[24] Alazab, A., Khraisat, A., Singh, S. andJan,T., 2023. Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. *Electronics*, *12*(16), p.3382.

[25] Fu, A., Zhang, X., Xiong, N., Gao, Y., Wang, H., & Zhang, J. (2020). VFL: A verifiable federated learning with privacy-preserving for big data in industrial IoT. *IEEE Transactions on Industrial Informatics*, *18*(5), 3316-3326.

[26] Passerat-Palmbach, J., Farnan, T., McCoy, M., Harris, J.D., Manion, S.T., Flannery, H.L. and Gleim, B.,2020,November. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In *2020 IEEE international conference on blockchain (Blockchain)* (pp. 550-555). IEEE.

[27] 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.

[28] Wu, X., Zhang, Y., Shi, M., Li, P., Li, R. and Xiong, N.N., 2022. An adaptive federated learning scheme with differential privacy preserving. *Future Generation Computer Systems*, *127*, pp.362-372.

[29] Abou El Houda, Z., Hafid, A.S. and Khoukhi, L., 2023. Mitfed: A privacy preservingcollaborative network attack mitigation framework based on federated learning using sdn and blockchain. *IEEE Transactions on Network Science and Engineering*.

[30] Chen, J., Xue, J., Wang, Y., Huang, L., Baker, T., & Zhou, Z. (2023). Privacy-preserving and traceable federated learning for data sharing in industrial IoT applications. *Expert Systems with Applications*, *213*, 119036..

[31] Aïvodji, U.M., Gambs, S. and Martin, A., 2019,May.IOTFLA:Asecuredandprivacy-preserving smart home architecture implementing federated learning. In *2019 IEEE securityandprivacyworkshops(SPW)*(pp.175-180). IEEE.

[32] Cui, L., Qu, Y., Xie, G., Zeng, D., Li, R., Shen, S., & Yu, S. (2021). Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Transactions on Industrial Informatics*, *18*(5), 3492-3500..

[33] Fang, C., Guo,Y.,Hu,Y.,Ma,B.,Feng,L.and Yin, A., 2021. Privacy-preserving and communication-efficient federated learning in internet of things. *Computers & Security*, *103*, p.102199.

[34] Zhang, X. Y., Córdoba-Pachón, J. R., Guo, P., Watkins, C., & Kuenzel, S. (2022). Privacy-preserving federated learning for value-added service model in advanced metering infrastructure. *IEEE Transactions on Computational Social Systems*, *11*(1), 117-131.

[35] Yazdinejad,A.,Parizi,R.M.,Dehghantanha,A. and Karimipour, H., 2021. Federated learning for drone authentication. *Ad Hoc Networks*, *120*, p.102574.

[36] Peyvandi, A., Majidi, B., Peyvandi, S. and Patra, J.C., 2022. Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-serviceinSociety 5.0. *Multimedia tools and applications*, *81*(18), pp.25029-25050.

[37] Zhang, T., Song, A., Dong, X., Shen, Y., & Ma, J. (2021). Privacy-preserving asynchronous grouped federated learning for IoT. *IEEE Internet of Things Journal*, *9*(7), 5511-5523.

[38] Duy, P.T., Hao, H.N., Chu, H.M. and Pham, V.H., 2021. A Secure and Privacy Preserving Federated Learning Approach for IoT Intrusion Detection System. In *Network andSystemSecurity: 15th International Conference, NSS 2021, Tianjin, China,October23,2021,Proceedings15*(pp. 353-368). Springer International Publishing.

[39] Abdel-Basset, M., Moustafa, N., Hawash, H., Ding, W., Abdel-Basset,M.,Moustafa,N.,Hawash, H. and Ding, W., 2022. Federated learning for privacy-preserving Internet of Things. *Deep Learning Techniques for IoT Security and Privacy*, pp.215-228.

[40] Ibrahem, M.I., Mahmoud, M., Fouda, M.M., ElHalawany, B.M. and Alasmary, W., 2022, December. Privacy-preserving and efficient decentralized federated learning-based energy theft detector. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 287-292). IEEE.

[41] Wibawa, F., Catak, F. O., Kuzlu, M., Sarp, S., & Cali, U. (2022, June). Homomorphic encryption and federated learning based privacy-preserving cnn training: Covid-19 detection use-case. In *Proceedings of the 2022 European interdisciplinary cybersecurity conference* (pp. 85-90).

[42] Liu, T., Hu, X., Xu, H., Shu, T. and Nguyen, D.N.,2022.High-accuracylow-costprivacy-preserving federated learning in IoT systems via adaptive perturbation. *Journal of Information Security and Applications*, *70*, p.103309.

[43] Dash, B., Sharma, P., & Ali, A. (2022). Federated learning for privacy-preserving: A review of PII data analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(4).

[44] Stephanie, V., Khalil, I., Atiquzzaman, M. and Yi, X., 2022.

Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transactions on Industrial Informatics*.

[45] Zhou,X.,Liang,W.,Kevin,I.,Wang,K.,Yan,Z.,Yang,L.T.,Wei,W.,Ma, J.andJin,Q.,2023. DecentralizedP2PFederatedLearningfor Privacy-Preserving and Resilient Mobile Robotic Systems. *IEEE Wireless Communications*, *30*(2), pp.82-89.

[46] Bonawitz, K., Kairouz, P., McMahan, B. and Ramage, D., 2021.FederatedLearningandPrivacy: Building privacy-preserving systems for machine learning and data science on decentralized data. *Queue*, *19*(5), pp.87-114.

[47] Chamikara,M.A.P.,Bertok,P.,Khalil,I.,Liu,D. and Camtepe, S., 2021. Privacy preserving distributed machine learning with federated learning.*ComputerCommunications*,*171*,pp.112-125.

[48] Nasser, N., Fadlullah, Z. M., Fouda, M. M., Ali, A., & Imran, M. (2022). A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept. *Computer Networks*, *205*, 108672.

[49] Liu, Y., James, J.Q., Kang, J., Niyato, D. and Zhang, S., 2020. Privacy-preserving traffic flow prediction: A federated learning approach. *IEEE Internet of Things Journal*, *7*(8), pp.7751-7763.

[50] Zhu, X., Wang, J., Chen, W. and Sato, K., 2023. Model compression and privacy preserving framework for federated learning. *Future Generation Computer Systems*, *140*, pp.376-389.

[51] Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)*, *54*(6), 1-36.

[52] Albaseer, A., & Abdallah, M. (2023, January). Privacy-preserving honeypot-based detector in smart grid networks: A new design for quality-assurance and fair incentives federated learning framework. In *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)* (pp. 722-727). IEEE.

[53] Zhao, Y., Zhao, J., Jiang, L., Tan, R. and Niyato, D., 2019. Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system. *arXiv preprint arXiv:1906.10893*, pp.2327-4662.

[54] Nair, A.K., Sahoo, J. and Raj, E.D., 2023. Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Computer Standards & Interfaces*, *86*, p.103720.

[55] Qin, Z., Ye, J., Meng, J., Lu, B. and Wang,L., 2021. Privacy-preserving blockchain-based federated learning for marine Internet of Things. *IEEE Transactions on Computational Social Systems*, *9*(1), pp.159-173.