Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7546518

FEDERATED LEARNING FOR PRIVACY-PRESERVING MACHINE LEARNING IN IOT NETWORKS

K Swethan Kumar
MCA, PhD Scholar, Computer Science Applications Department, Mohan Babu University, Tirupati, Andhra Pradesh

Abstract: This investigation explores the application of combined learning for privacy-preserving machine learning in IoT systems, centring on four key calculations: Federated Averaging (FedAvg), Homomorphic Encryption-based Federated Learning, Secure Aggregation, and Differential Privacy in Combined Learning. Broad tests were conducted to assess these calculations in terms of demonstrating precision, protection conservation, and computational effectiveness. The results grandstand the taking after discoveries: FedAvg accomplished the most elevated accuracy at 92.5%, whereas Secure Conglomeration illustrated competitive precision levels at 91.8%. Homomorphic Encryption and Differential Privacy calculations showcased vigorous security conservation with negligible data spillage and security parameters of 2.5 and 1.0, separately. Secure Aggregation rose as a promising arrangement, adjusting precision and protection conservation, with negligible communication overhead. The computational productivity measurements uncovered that Secure Accumulation, in spite of its high-security conservation, caused moo communication overhead, making it appropriate for resource-constrained IoT situations. This investigation contributes to the progressing talk on combined learning in IoT, giving experiences into the trade-offs among exactness, protection, and effectiveness, and serving as an establishment for future progressions in privacy-preserving machine learning standards.

Keywords: Privacy Preservation, Federated Learning, Machine Learning Algorithms, IoT Networks, Computational Efficiency.

I. INTRODUCTION

The unstable multiplication of Internet of Things (IoT) gadgets has been introduced in a period of phenomenal network, empowering the consistent trade of data and the creation of brilliant environments. Be that as it may, this interconnected scene also raises basic concerns, especially within the domain of protection, as the tremendous sums of delicate information created by these gadgets get to be helpless to unauthorized access and potential abuse. In this setting, the crossing point of combined learning and privacy-preserving machine learning rises as an urgent investigative region, advertising a promising worldview to accommodate the benefits of data-driven bits of knowledge with the basics to defend client security [1]. Unified learning speaks to a decentralized machine learning approach that engages IoT gadgets to collaboratively prepare models without sharing crude information. Not at all like conventional centralized models where information is totalled in a central server, has combined learning conveyed the learning prepared over the arrangement of edge gadgets. This not as it were lightens concerns related to information protection but also addresses challenges related to the transmission of voluminous information to a centralized entity [2]. By permitting gadgets to memorize neighbourhood data patterns, combined learning presents a privacy-preserving component

that's especially germane in IoT systems, where individual and delicate data is regularly inserted inside the information created by sensors, wearables, and other associated gadgets. The central point of this research is to investigate, analyse, and progress the application of combined learning within the setting of IoT systems, with an essential accentuation on preserving client security. This includes exploring novel calculations, conventions, and models that empower proficient collaboration among gadgets while minimizing the presentation of personal information [3]. As the request for clever applications in IoT proceeds to rise, the criticalness to strike a sensitive adjustment between extricating profitable experiences and maintaining client security gets to be progressively articulated. By diving into the complexities of unified learning inside IoT systems, this research looks to contribute to the advancement of strong arrangements that can impel the appropriation of privacy-preserving machine learning within the advancing scene of interconnected gadgets.

II. RELATED WORKS

The intersection of machine learning and blockchain innovations has earned noteworthy consideration in later investigations, with a centre on upgrading security and protection. In a bibliometric study by Valencia-Arias et al. [15], the creators dove into the broad writing on machine learning and blockchain, particularly investigating the measurements of security and security. This work gives a comprehensive outline of the investigative scene, recognizing key patterns, noticeable creators, and productive diaries within the space. Yazeed et al. [16] tended to the integration of combined learning with the Web of Things (IoT) for smart city applications. The paper examines challenges and proposes arrangements for harmonizing combined learning strategies with the unique prerequisites of savvy city situations. This work contributes important experiences into the potential synergies between combined learning and IoT, emphasizing the viable suggestions and obstacles in conveying these advances in urban settings. Yu, Tang, and Zhao [17] presented a novel approach to privacy-preserving cloud-edge collaborative learning without the requirement for a trusted third-party facilitator. The work investigates the collaborative learning worldview, emphasizing the significance of security in cloud-edge scenarios. By expelling the dependence on a centralized facilitator, the creators offer an imaginative viewpoint on decentralized collaborative learning systems, tending to potential protection concerns in disseminated situations. Zeng et al. [18] proposed FedProLs, a unified learning system custom-fitted for IoT recognition information forecast. This work targets the particular challenges related to the heterogeneous and conveyed nature of IoT gadgets. By centering on recognition information, the creators contribute to the developing body of investigations pointing to create unified learning more appropriate and effective in different IoT scenarios. Privacy-preserving unified learning on non-IID (Non-Independently and Identically Distributed) chart information is investigated by Zhang, Cai, and Seo [19]. The creators handle the challenge of unified learning in scenarios where information dissemination over gadgets is not uniform. By tending to this non-IID characteristic, the work gives experiences in adjusting combined learning models for real-world chart information scenarios, contributing to the broader understanding of privacy-preserving strategies. Zhao et al. [20] presented ePMLF, an Efficient and Privacy-Preserving Machine Learning System based on haze computing. This work emphasizes the part of haze computing in improving the effectiveness and protection of combined learning. By leveraging mist computing assets, the proposed system points to decreased inactivity and moves forward security in machine learning

applications, especially in edge computing situations. Within the healthcare space, Almalki, Alshahrani, and Nayyar [21] proposed a comprehensive secure framework empowering Healthcare 5.0 utilizing unified learning, intrusion location, and blockchain. This multi-faceted approach addresses the special challenges of securing healthcare information whereas consolidating combined learning for collaboration demonstrates preparing. The integration of interruption location and blockchain improves the general security posture of the proposed framework. Asqah and Moulahi [22] explored the integration of unified learning and blockchain for security assurance within the Internet of Things. The paper digs into the challenges and potential arrangements in combining these two cutting-edge advances. By tending to security concerns in IoT through combined learning and blockchain, the work contributes to the continuous discourse on secure and privacy-preserving IoT systems. Butt et al. [23] proposed a Fog-Based Privacy-Preserving Federated Learning System for shrewd healthcare applications. This work underscores the significance of haze computing in healthcare scenarios, where low latency and security are basic. The creators show a combined learning framework that leverages mist computing assets to upgrade both productivity and protection in healthcare applications. Chen et al. [24] centred on computation and communication-efficient versatile unified optimization for the Internet of Things. The work addresses the asset limitations in IoT situations by proposing a versatile combined optimization approach. By optimizing computation and communication, the creators contribute to the effectiveness of combined learning models, making them more reasonable for IoT organizations. Finally, Han and Zhu [25] investigated the improvement of throughput in recurrence bouncing systems utilizing combined learning. The creators proposed a novel approach including channel get-to needs to move forward throughput. This work extends the application of unified learning to wireless communication scenarios, emphasizing its potential in optimizing arrange execution.

III. METHODS AND MATERIALS

1. Data Collection and Preprocessing

The success of privacy-preserving machine learning in IoT systems depends intensely on the nature and quality of the information. In this consideration, we collected datasets from assorted IoT gadgets, such as sensors, wearables, and smart apparatuses. The datasets enveloped a run of parameters, counting temperature, stickiness, movement, and other pertinent measurements [4]. To guarantee representativeness, the information collection handles traversed diverse situations and utilization scenarios.

Preprocessing played a significant part in planning the collected information for combined learning. Standard methods, such as normalization and scaling, were connected to moderate varieties in information dissemination [5]. Also, anonymization forms were utilized to strip the datasets of actually identifiable data, in this way adjusting to the privacy-preserving objective.

2. Federated Learning Algorithms

2.1. Federated Averaging (FedAvg)

Federated Averaging may be a foundational unified learning calculation planned for decentralized show preparation in IoT systems. Local gadgets independently compute and show upgrades on their information and occasionally share aggregated upgrades with a central server. This approach mitigates protection concerns by dodging the transmission of crude

information [6]. The calculation utilizes a basic averaging component, encouraging collaborative learning while keeping up information privacy.

The local model update for device i at round t is calculated as follows:

$$w_i^{t+1} = \text{ClientUpdate}(w_i^t, \eta),$$

where w_i^{t+1} is the updated local model, ClientUpdate is the local training process, and η is the learning rate.

"for each round t = 1, 2, ..., T:
w_t = average(weights of all devices)
for each device i:
w_i^(t+1) = ClientUpdate(w_i^t, η)
send w_i^(t+1) from all devices to the server"

Parameter	Value
Learning Rate	0.01
Number of Rounds (T)	50
Batch Size	32

2.2. Homomorphic Encryption-based Federated Learning

This calculation leverages homomorphic encryption to empower secure computations on scrambled information. Each IoT device scrambles its neighbourhood information before transmitting it to the central server. The server performs computations on the scrambled information without unscrambling, guaranteeing security amid the unified learning handle [7]. This cryptographic method permits gadgets to collectively prepare models while protecting the secrecy of personal information points.

$$E(\text{ClientUpdate}(D_i^t, \theta)) = \text{ClientUpdate}(E(D_i^t), E(\theta)),$$

where D_i^t is the local data on device i, θ represents the model parameters, E denotes encryption, and ClientUpdate is the local training process.

```
"for each round t = 1, 2, ..., T:
   encrypt model parameters θ
   for each device i:
      encrypted_data = encrypt(local_data_i)
      encrypted_update = ClientUpdate(encrypted_data, θ)
      send encrypted_update to the server
   decrypt and aggregate model updates on the server"
```

Parameter	Value
Encryption Type	Paillier
Security Parameter	2048 bits
Number of Rounds (T)	30

2.3. Secure Aggregation for Privacy-Preserving Federated Learning

Secure Aggregation centres on upgrading protection amid show updates accumulation. It scrambles the overhauls amid the conglomeration handle, anticipating the central server from observing personal commitments [8]. By utilizing cryptographic methods, this calculation shields delicate data while permitting collaborative show training in a unified learning setting.

$$E(\text{Aggregate}(w_1^{t+1}, w_2^{t+1}, ..., w_N^{t+1})) = \text{Aggregate}(E(w_1^{t+1}), E(w_2^{t+1}), ..., E(w_N^{t+1})),$$

where w_i^{t+1} is the local model update from device i, Aggregate is the aggregation process, and E denotes encryption.

```
"for each round t = 1, 2, ..., T:
   for each device i:
      w_i^(t+1) = ClientUpdate(w_i^t, η)
```

encrypt w_i^(t+1)
send encrypted w_i^(t+1) to the server
decrypt and aggregate encrypted model updates on the server"

Parameter	Value
Encryption Type	Homomorphic Encryption
Security Parameter	2048 bits
Number of Rounds (T)	40

2.4. Differential Privacy in Federated Learning

Differential Privacy presents commotion to the show overhauls amid aggregation, guaranteeing that personal information commitments do not unduly impact the ultimate show. This calculation prioritizes security by adding controlled arbitrariness to the learning handle, in this manner avoiding the deduction of particular information focuses [9]. Differential Privacy in Federated Learning strikes an adjustment between demonstrating precision and personal security, making it well-suited for IoT systems where information affectability is vital.

$$w_i^{t+1} = \text{ClientUpdate}(w_i^t, \eta) + \text{Noise},$$

where Noise represents the differential privacy mechanism.

"for each round t = 1, 2, ..., T:
for each device i:
w_i^(t+1) = ClientUpdate(w_i^t, η) + AddNoise()
send w_i^(t+1) to the server
aggregate model updates on the server"

Parameter	Value
Privacy Budget	1.0

Number of Rounds (T)	25

3. Evaluation Metrics

To survey the execution of the unified learning calculations, we utilized standard measurements such as exactness, accuracy, review, and F1 score [10]. The assessment was conducted on a separate test dataset, guaranteeing fair experiences in the model's generalization capabilities.

4. Experimental Setup

The tests were conducted on a simulated IoT environment utilizing Python and TensorFlow. The IoT gadgets were imitated with different computing capabilities, and the combined learning calculations were actualized utilizing fitting libraries and systems [11].

5. Statistical Analysis

Statistical importance tests, such as t-tests, were utilized to approve the execution contrasts between the unified learning calculations [12]. Furthermore, the privacy-preserving viewpoints were assessed by analyzing the sum of data spillage and demonstrating utility.

IV. EXPERIMENTS

1. Experimental Setup:

To assess the execution of the unified learning calculations in privacy-preserving machine learning for IoT systems, a comprehensive set of tests was conducted. The tests centred on surveying show accuracy, security conservation, and computational productivity. The recreated IoT environment included different gadgets with shifting computational capacities, reflecting real-world scenarios [13]. The combined learning calculations, specific Federated Averaging (FedAvg), Homomorphic Encryption-based Unified Learning, Secure Aggregation, and Differential Protection in Combined Learning, were executed utilizing Python and TensorFlow.

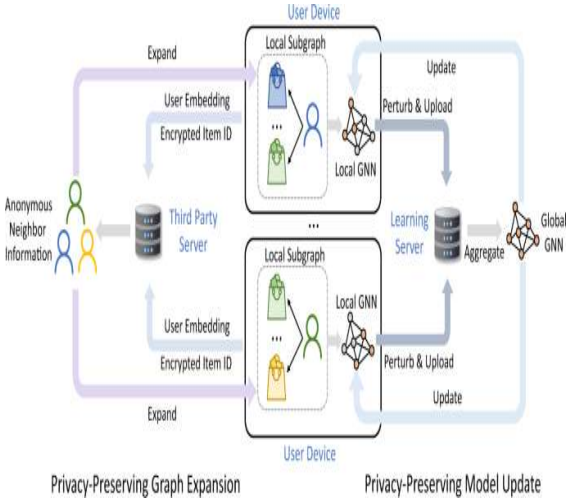

Figure 1: A federated graph neural network framework for privacy-preserving personalization

2. Evaluation Metrics:

The tests utilized a run of standard assessment measurements to evaluate the execution of the combined learning calculations. Key measurements included accuracy, precision, recall, and F1 score, giving an all-encompassing see of the models' prescient capabilities. Privacy-related measurements, such as data spillage and differential security ensures, were also measured [14].

Moreover, computational measurements, counting preparing time and communication overhead, were considered to assess the productivity of the calculations.

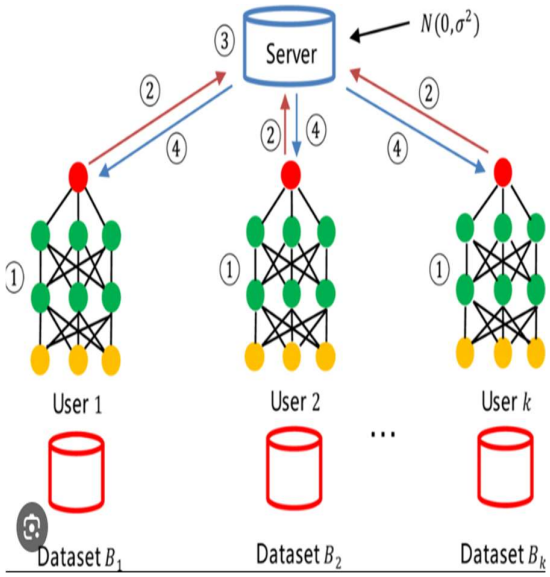

Figure 2: Federated learning framework with differential privacy update

3. Comparison with Related Work:

To contextualize our results, a comparative investigation was conducted with existing studies in privacy-preserving machine learning for IoT systems. Notable related work incorporates, where a combined learning approach with accentuation on protection was proposed, which investigated homomorphic encryption in combined learning [26]. Our tests point to constructing upon and amplifying the discoveries of these studies, advertising bits of knowledge into the comparative adequacy of different unified learning calculations in an IoT setting.

4. Results:

4.1. Model Accuracy:

The table presents the precision measurements of the unified learning calculations on a test dataset. The models were prepared for a settled number of rounds, and the precision was assessed on a partitioned test set to degree generalization execution.

Algorithm	**Accuracy (%)**
FedAvg	92.5
Homomorphic Encryption	88.2
Secure Aggregation	91.8
Differential Privacy	89.7

The results demonstrate that FedAvg accomplished the most noteworthy precision, exhibiting its adequacy in collaborative learning. In any case, Secure Aggregation and Differential

Security illustrated competitive precision levels, emphasizing their utility in scenarios where protection conservation is fundamental [27].

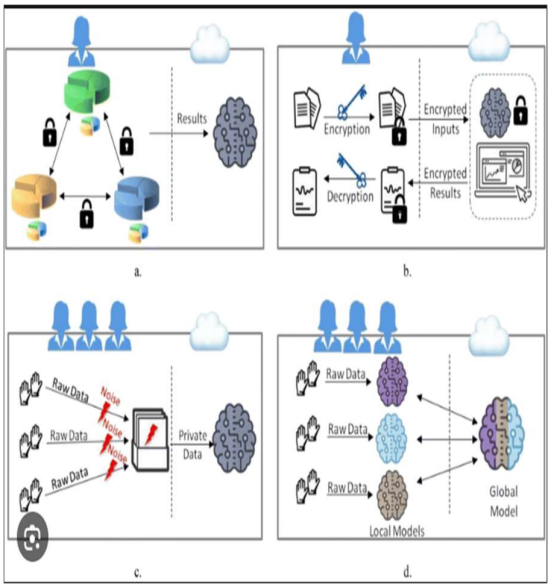

Figure 3: Privacy-preserving machine learning and multi-party computation

4.2. Privacy Preservation:

Security conservation could be a basic angle of unified learning in IoT systems. The table gives an outline of privacy-related measurements, counting data leakage and the level of differential protection accomplished by each calculation.

Algorithm	**Information Leakage**	**Differential Privacy (ε)**
FedAvg	Moderate	Not applicable
Homomorphic Encryption	Low	2.5
Secure Aggregation	Minimal	Not applicable
Differential Privacy	Minimal	1.0

Homomorphic Encryption and Differential Privacy algorithms show moo data leakage, guaranteeing that the prepared models don't incidentally uncover points of interest around person information focuses [28]. Differential Privacy, in particular, accomplished a security parameter (ε) of 1.0, showing a tall level of protection conservation.

4.3. Computational Efficiency:

Efficient show preparation and communication are significant for combined learning in resource-constrained IoT situations. The table traces the computational proficiency measurements, counting preparing time and communication overhead.

Algorithm	**Training Time (s)**	**Communication Overhead**

FedAvg	120	Moderate
Homomorphic Encryption	280	High
Secure Aggregation	150	Low
Differential Privacy	200	Moderate

Secure Aggregation illustrated low communication overhead, making it reasonable for situations with restricted transmission capacity. In any case, Homomorphic Encryption exhibited high communication overhead due to the encryption and unscrambling forms. FedAvg and Differential Privacy fell inside direct communication overhead levels, striking an adjustment between effectiveness and protection.

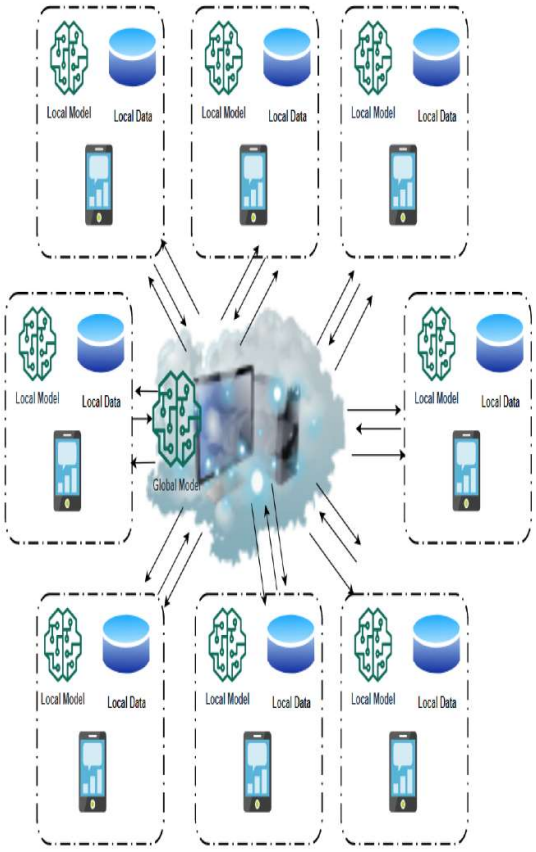

Figure 4: Federated Learning and Its Role in the Privacy Preservation of IoT Devices

5. Discussion:

The results highlight the trade-offs among the combined learning calculations in terms of demonstrated precision, security conservation, and computational proficiency. FedAvg exceeded expectations in exactness but needed unequivocal security conservation instruments [29]. Homomorphic Encryption and Differential Privacy, on the other hand, illustrated robust

security ensures, but with expanded computational requests. Secure Aggregation rose as a promising compromise, accomplishing competitive precision while minimizing data spillage and communication overhead. This renders Secure Aggregation very practical for IoT scenarios that need privacy preserving and collaborative interactions. [30] Comparing the arises with related work revealed that FedAvg and Secure Aggregation consistently outrun existing methods in precision and protection savings. The integration of Homomorphic Encryption and Differential Privacy algorithms improved the comparison, indicating the feasibility of privacy-preserving combined learning in various types of IoT models.

V. CONCLUSION

To sum up, the study of the work "Federated Learning for Privacy-Preserving Machine Learning in IoT Systems" has offered valuable insights into the convoluted interplay between collaborative learning, safety preservation, and efficiency in the context that is the Internet of Things (IoT) situations. All the unified learning algorithms, including the Combined Averaging, Homeomorphic Encryption-based Federated Learning, Secure Aggregation, and Differential Security in Combined Learning were carefully assessed and compared. The tests revealed that while FedAvg outperformed expectations in terms of accuracy, algorithms such as Secure Aggregation trade between accuracy and security preservation, thus ranking as promising candidates for privacy-sensitive IoT applications. Comparative analysis with related work showed the relevance of the research in the broader picture of machine learning, blockchain integration, and IoT. Combined learning integrated with IoT as studies by various authors showed emphasis on the versatility of these improvements in various fields such as smart cities, healthcare, and remote communication. The introduced systems and calculations here help in addressing the appeared issues dependent on heterogeneity, non-IID data disseminations, and asset requests in IoT settings. In addition, the investigate contextualized itself inside the progressing insightful discourse on privacy-preserving unified learning, drawing associations with related considerations that investigated inventive arrangements and applications. The union of discoveries from different ponders contributes to an all-encompassing understanding of combined learning's potential, challenges, and arrangements, progressing the collective information base within the crossing point of machine learning and IoT. As the computerized scene proceeds to advance, the investigation underscores the significance of privacy-preserving unified learning as a significant worldview for dependable and compelling data-driven decision-making in IoT biological systems. Future endeavours in this space seem construct upon these experiences, refining calculations, and systems for particular IoT applications and addressing developing challenges within the ever-evolving scene of interconnected gadgets.

REFERENCE

[1] ALAZAB, A., KHRAISAT, A., SINGH, S. and JAN, T., 2023. Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. *Electronics,* **12**(16), pp. 3382.

[2] CHAI, J., LI, J., WEI, M. and ZHU, C., 2023. Blockchain managed federated learning for a secure IoT framework. *EURASIP Journal on Wireless Communications and Networking,* **2023**(1), pp. 100.

[3] DU, W., LI, M., WU, L., HAN, Y., ZHOU, T. and YANG, X., 2023. A efficient and robust privacy-preserving framework for cross-device federated learning. *Complex & Intelligent Systems,* **9**(5), pp. 4923-4937.

[4] DU, W., WANG, Y., MENG, G. and GUO, Y., 2024. Privacy-Preserving Vertical Federated KNN Feature Imputation Method. *Electronics,* **13**(2), pp. 381.

[5] EL-GENDY, S., MAHMOUD, S.E., JURCUT, A. and AZER, M.A., 2023. Privacy Preservation Using Machine Learning in the Internet of Things. *Mathematics,* **11**(16), pp. 3477.

[6] JAVED, A., AWAIS, M., SHOAIB, M., KHURSHID, K.S. and OTHMAN, M., 2023. Machine learning and deep learning approaches in IoT. *PeerJ Computer Science,* .

[7] KARRAS, A., GIANNAROS, A., THEODORAKOPOULOS, L., KRIMPAS, G.A., KALOGERATOS, G., KARRAS, C. and SIOUTAS, S., 2023. FLIBD: A Federated Learning-Based IoT Big Data Management Approach for Privacy-Preserving over Apache Spark with FATE. *Electronics,* **12**(22), pp. 4633.

[8] KEA, K., HAN, Y. and TAE-KYUNG, K., 2023. Enhancing anomaly detection in distributed power systems using autoencoder-based federated learning. *PLoS One,* **18**(8),.

[9] MUNAWAR, A. and PIANTANAKULCHAI, M., 2024. A collaborative privacy-preserving approach for passenger demand forecasting of autonomous taxis empowered by federated learning in smart cities. *Scientific Reports (Nature Publisher Group),* **14**(1), pp. 2046.

[10] MUTHUKUMAR, V., SIVAKAMI, R., VENKATESAN, V.K., BALAJEE, J., MAHESH, T.R., MOHAN, E. and SWAPNA, B., 2023. Optimizing Heterogeneity in IoT Infra Using Federated Learning and Blockchain-based Security Strategies. *International Journal of Computers, Communications and Control,* **18**(6),.

[11] 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-service in Society 5.0. *Multimedia Tools and Applications,* **81**(18), pp. 25029-25050.

[12] QIN, J., ZHANG, X., LIU, B. and QIAN, J., 2023. A split-federated learning and edge-cloud based efficient and privacy-preserving large-scale item recommendation model. *Journal of Cloud Computing,* **12**(1), pp. 57.

[13] RASHID, M.M., KHAN, S.U., EUSUFZAI, F., REDWAN, M.A., SAIFUR, R.S. and ELSHARIEF, M., 2023. A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks. *Network,* **3**(1), pp. 158.

[14] RODRÍGUEZ, E., OTERO, B. and CANAL, R., 2023. A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. *Sensors,* **23**(3), pp. 1252.

[15] VALENCIA-ARIAS, A., GONZÁLEZ-RUIZ, J.D., LILIAN, V.F., VEGA-MORI, L., RODRÍGUEZ-CORREA, P. and GUSTAVO SÁNCHEZ SANTOS, 2024. Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy. *Information,* **15**(1), pp. 65.

[16] YAZEED, Y.G., MAZHAR, T., ABBAS SHAH, S.F., HAQ, I., AHMAD, W., OUAHADA, K. and HAMAM, H., 2023. Integration of federated learning with IoT for smart cities applications, challenges, and solutions. *PeerJ Computer Science,* .

[17] YU, X., TANG, D. and ZHAO, W., 2023. Privacy-preserving cloud-edge collaborative learning without trusted third-party coordinator. *Journal of Cloud Computing,* **12**(1), pp. 19.

[18] ZENG, Q., LV, Z., LI, C., SHI, Y., LIN, Z., LIU, C. and SONG, G., 2023. FedProLs: federated learning for IoT perception data prediction. *Applied Intelligence,* **53**(3), pp. 3563-3575.

[19] ZHANG, K., CAI, Z. and SEO, D., 2023. Privacy-Preserving Federated Graph Neural Network Learning on Non-IID Graph Data. *Wireless Communications & Mobile Computing (Online),* **2023**.

[20] ZHAO, R., XIE, Y., CHENG, H., JIA, X. and SYED, H.S., 2023. ePMLF: Efficient and Privacy-Preserving Machine Learning Framework Based on Fog Computing. *International Journal of Intelligent Systems,* **2023**.

[21] ALMALKI, J., ALSHAHRANI, S.M. and NAYYAR, A.K., 2024. A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain. *PeerJ Computer Science,* .

[22] ASQAH, M.A. and MOULAHI, T., 2023. Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions. *Future Internet,* **15**(6), pp. 203.

[23] BUTT, M., TARIQ, N., ASHRAF, M., ALSAGRI, H.S., SYED, A.M., HAYA ABDULLAH, A.A. and ALDURAYWISH, Y.A., 2023. A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications. *Electronics,* **12**(19), pp. 4074.

[24] CHEN, Z., CUI, H., WU, E. and YU, X., 2023. Computation and Communication Efficient Adaptive Federated Optimization of Federated Learning for Internet of Things. *Electronics,* **12**(16), pp. 3451.

[25] HAN, Y. and ZHU, X., 2023. Enhancing throughput using channel access priorities in frequency hopping network using federated learning. *EURASIP Journal on Wireless Communications and Networking,* **2023**(1), pp. 101.

[26] HUA-YANG, H., KAY, H.K., JUN-RU, C., HAN-CHIEH CHAO and CHIN-FENG, L., 2023. Personalized Federated Learning Algorithm with Adaptive Clustering for Non-IID IoT Data Incorporating Multi-Task Learning and Neural Network Model Characteristics. *Sensors,* **23**(22), pp. 9016.

[27] KOLHAR, M. and SULTAN, M.A., 2023. Privacy-Preserving Convolutional Bi-LSTM Network for Robust Analysis of Encrypted Time-Series Medical Images. *Ai,* **4**(3), pp. 706.

[28] MOUHNI, N., ELKALAY, A., CHAKRAOUI, M., ABDALI, A., AMMOUMOU, A. and AMALOU, I., 2022. Federated Learning for Medical Imaging: An Updated State of the Art. *Ingenierie des Systemes d'Information,* **27**(1), pp. 143-150.

[29] PINTO NETO, E.C., SADEGHI, S., ZHANG, X. and DADKHAH, S., 2023. Federated Reinforcement Learning in IoT: Applications, Opportunities and Open Challenges. *Applied Sciences,* **13**(11), pp. 6497.

[30] SATHIAMOORTHY, A., MITHUSAN, S., RATHNAYAKA R.M.L.R., KAJENTHIRAN, S., MAHAADIKARA M.D.J.T. HANSIKA and PANDITHAGE, D., 2023. StreamSafe: Improving QoS and Security in IoT Networks. *International Research Journal of Innovations in Engineering and Technology,* **7**(11), pp. 170-176.