LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S4(2025)

FEDERATED LEARNING IN THE CLOUD: A STUDY OF PRIVACY-PRESERVING AI ARCHITECTURES AND RECENT IMPLEMENTATIONS ACROSS THE THREE MAJOR CLOUD SERVICE PROVIDERS

Dr. Ashish Sharma[1], Nausheen Khilji[2], Dr. Shweta Purohit[3], Dr. Rakesh Saxena[4]

[1]Professor, Department of Technology, JIET, Jodhpur, Jodhpur, Rajasthan
[2]Assistant Professor, Department of Technology, JIET UNIVERSE, JODHPUR, JODHPUR, RAJASTHAN
[3]Former Principal, Computer Science, Mahila Technical and Management College, Jodhpur, Jodhpur, Rajasthan
[4]Guest faculty, BCA/MCA department, Jai Narain Vyas University (JNVU), Jodhpur, Jodhpur, Rajasthan

aashishid@gmail.com[1]
naushy90@gmail.com[2]
shwetajoshi@gmail.com[3]
srakeshb4u@gmail.com[4]

Abstract: Federated Learning (FL) has become a paradigm shift in privacy-preserving artificial intelligence, especially in cloud environments where sensitive information cannot be centralized, and there are regulatory or ethical issues. This paper explores how FL can be designed and implemented on three major cloud service providers, including AWS, Google Cloud, and Microsoft Azure, with a special focus on four fundamental algorithms, namely, Federated Averaging (FedAvg), Differentially Private Stochastic Gradient Descent (DP-SGD), Secure Aggregation, and Trusted Execution Environment-based FL (TEE-FL). Experiments were performed with synthetic healthcare and financial data to measure the performance in terms of model accuracy, communication overhead, and preservation of privacy. Findings indicate that FedAvg had the best accuracy (92 percent) at the cost of no privacy guarantees, DP-SGD had the best privacy (high differential privacy) with a moderate accuracy drop (88 percent), Secure Aggregation had the best security, and TEE-FL had the best trade-offs with 90 percent accuracy and only 8 percent overhead. As compared to the related work, this study confirms that secure aggregation and hardware-assisted trust combine into hybrid approaches that offer practical scalability without adversely affecting performance. In general, the results highlight the promise of federated learning in the context of cloud ecosystems as a foundation of ethically and regulatory-compliant AI usage.

Keywords: Federated Learning, Cloud Computing, Privacy-Preserving AI, Secure Aggregation, Differential Privacy

I. INTRODUCTION

The fast development of artificial intelligence (AI) has introduced transformational applications to healthcare, finance, retail, and many other industries. Nonetheless, the fact that traditional AI systems rely on the centralization of data aggregation poses significant issues in the context of privacy, security, and regulatory adherence. By collecting and storing sensitive user data in centralized repositories, a company exposes this data to breaches and misuse, as well as raises questions about the adherence to data protection laws and regulations like GDPR and HIPAA [1]. To address these issues, Federated Learning (FL) has risen as a potential innovative paradigm that can facilitate collaborative model training without necessarily having access to raw data [2]. Rather, model updates are shared only, thereby providing better privacy protection

and minimized information traffic. FL further increases its applicability in cloud computing environments by taking advantage of scalable infrastructure, managed services, and advanced security offerings of leading cloud service providers [3]. The three major companies in the cloud field (Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure) have already started adding FL-friendly tools and architectures that support safe distributed learning. Each platform presents distinct design options, frameworks, and privacy preserving techniques like secure aggregation, differential privacy, and trusted execution environments (TEEs) based on hardware. Nevertheless, despite these developments, some critical questions persist about the relative effectiveness, performance, and feasibility of FL implementations in these cloud ecosystems. The purpose of this study is to investigate and analyze privacy-sensitive FL architectures provided by the three largest providers, their advantages, weaknesses, and applicability to various areas of application. In this way, the research offers an organized insight into the ways a cloud-enabled FL can tackle the urgent privacy issues without compromising on scalability and model accuracy. Finally, the paper helps to reduce the distances between theoretical developments in federated learning and their practical implementation in cloud platforms.

II. RELATED WORKS

Federated learning (FL) on clouds also overlaps with work in privacy-preserving AI, edge intelligence, and distributed computing. A few recent works have noted the possible convergence of artificial intelligence and distributed architectures to solve the issues of performance and privacy on a cross-domain basis.

Abiodun et al. [15] investigated the application of artificial intelligence in dynamic spectrum access of wireless communications and the relevance of the decentralization of strategies to allocate a spectrum in real time. Their article highlights the increased demand of distributed AI models, which is similar to the goal of FL, which is to train models without having to aggregate data in a central place. In the same way, Gerasimos et al. [16] were interested in the data-driven decision support systems on cloud-based Software as a Service (SaaS) models. In support of the thesis that FL in cloud ecosystems is a valid pathway to service optimization and privacy, they cited scalability and data sensitivity as potential challenges. Hanen et al. [17] introduced a hybrid recommendation system in the context of optimal service placement of IoT in the fog and edge computing. Their results emphasize the importance of bringing computational intelligence closer to data sources, which is the key principle that federated learning is based on. In addition to this, Jouini et al. [20] gave a general overview of machine learning in edge computing, where they determined its techniques, frameworks, and concerns. Their study indicates that FL supplements edge structures with privacy-conscious distributed training.

The other fast-growing field is AI-based automation. Jin et al. [18] provided a review of taxonomies of automation technologies, noting the issues of data handling, privacy, and interpretation. This is in line with the ability of federated learning to promote automation without compromising privacy. Similarly, the survey of intrusion detection systems by Lorenzo et al. [23] highlights the necessity of privacy-preserving measures in network security-related problems, which can be tackled by federated architectures with the help of distributed anomaly detection. Healthcare is a very sensitive area where FL can become a transformative process. Kalodanis et al. [21] postulated a privacy-protecting AI design of high-risk medical systems within the EU AI Act and demonstrates regulatory and ethical restrictions that directly dictate the implementation of FL in cloud healthcare pipelines. In the same manner, Majeed et al. [24]

offered an in-depth discussion of privacy-saving techniques of IoT-based systems, focusing on cryptographic and differential privacy, also major approaches implemented in FL. Mulo et al. [26] also applied this perspective to the Internet of Medical Things (IoMT) and showed how deep learning could be applied to medical devices without violating privacy standards.

Liu et al. [22] have reviewed the problem of multi-user privacy and gave a survey of the problems in edge intelligence, which points to vulnerabilities of shared data environments. Their results support the use of secure aggregation to FL and differential privacy. Moreover, Jorgensen and Ma [19] surveyed the effects of the EU regulations on the adoption of AI and IoT in energy management systems and reported regulatory limitations that are similar to those experienced in federated learning systems in the EU. Lastly, Monjurul et al. [25] talked about AI agents to data annotation, and one of the notes made was that an annotation framework that is distributed can minimize the privacy risks. These lessons can be applied to pipelines using federated data preprocessing on the cloud. Taken together, these papers demonstrate that federated learning in the cloud can solve not only acute privacy problems but also be applied in harmony with the rest of the IoT, edge computing, healthcare, and regulatory compliance trends.

III. METHODS AND MATERIALS

The research design and comparative analysis of federated learning (FL) algorithms implemented in the cloud computing environment are adopted as the methodology of the current research. Its core concern is the evaluation of the integration of various privacy-aware measures in the pipelines of cloud-based FL with artificial yet realistic datasets. The methodological framework contains description of data, algorithm choice, experimental implementation on simulated cloud systems, and comparative analysis [4].

Data Description

Because the aim of the current research is to investigate privacy-saving FL architectures, artificial data were created to simulate real-life situations of sharing sensitive user data. The data sample includes 50,000 samples spread out in 10 clients, which emulates the data heterogeneity in institutions (e.g. hospitals or financial institutions). The characteristics of each client dataset are categorical (client demographics or types of accounts) and continuous (volume of transactions or test outcomes). The labels are binary, (ex: fraud detection (fraudulent or legitimate) or clinical prediction (disease or no disease)) [5]. The data distribution is not independent and identically distributed (non-IID), as it represents the reality of actual federated situations where datasets of clients vary in size and properties.

Table 1: Dataset Distribution across Clients

Client ID	Number of Samples	Feature Count	Label Distribution (0/1)	Data Type
C1	6,000	20	60% / 40%	Mixed (num/cat)
C2	4,500	20	55% / 45%	Mixed (num/

				cat)
C3	5,200	20	70% / 30%	Mixed (num/ cat)
C4	7,800	20	48% / 52%	Mixed (num/ cat)
C5	8,500	20	65% / 35%	Mixed (num/ cat)
C6 – C10	~18,000	20	Varies	Mixed (num/ cat)

This heterogeneity enables experimentation of the performance of cloud-based FL algorithms when dealing with an imbalanced and skewed data distribution.

Algorithms

1. Federated Averaging (FedAvg)

The basic algorithm of federated learning is Federated Averaging (FedAvg). In this model, clients privately train a local model on their own data, and only send the model parameters (weights or gradients) to a central server. The server then weighted averages the received updates using weights proportional to the number of clients per client, and the result is a global model. The new international model is re-allocated to the entire client group to train further at the local level. The process continues to converge. FedAvg minimizes the movement of data, minimizes communication overhead, and maintains privacy because the raw data do not go outside the client devices. Non-IID data distributions, however, are not well handled and can lead to a slower rate of convergence or bias towards larger clients [6]. Such constraints notwithstanding, FedAverage is used as a standard of comparison of innovative privacy-preserving FL algorithms.

"Initialize global model W0
For each round t = 1 to T:
For each client k in parallel:
Wk ← Train local model on Dk for E epochs
Wt ← Σ (nk / n) * Wk # weighted average
Distribute Wt back to clients"

2. Differentially Private Stochastic Gradient Descent (DP-SGD)

DP-SGD provides some degree of privacy in the learning procedure, with the advantage that any single data point does not play a significant role in the ultimate model. In training, gradients are capped to a norm that is at most finite to restrict outlier impact and are perturbed using specially tuned Gaussian noise. The federated would have every client train with DP-SGD locally, and only privatized gradients are sent to the central server. The privacy level is measured by the parameter ε (epsilon) which characterizes the privacy-accuracy tradeoff [7]. DP-SGD is especially relevant to regulated sectors where formal privacy assurances need to be put in place. Its only disadvantage, however, is that it leads to a lower model accuracy because of noise injection. In the case of deploying in the cloud, DP-SGD may be incorporated into managed services like TensorFlow Federated on Google Cloud or Azure ML pipelines.

"For each minibatch B in local dataset:
Compute gradients g on B
Clip g to norm C
Add Gaussian noise $N(0,\sigma^2C^2)$
Update model using noisy gradients
Return privatized updates to server"

3. Secure Aggregation Protocol

Secure Aggregation A cryptographic method that allows the server to observe only aggregated updates to the model, rather than individual contributions of the clients. All clients encrypt local model updates using random masks and then send them out. When aggregated, the masks cancel, so that the server can only recover the sum of updates and does not learn any particular client update. This prevents server-side inference attacks as well as collusion risks. Homomorphic encryption or secret-sharing techniques can be used to realize secure aggregation [8]. Secure aggregation is consistent with compliance needs in cloud environments and increases the confidence in multi-institution cooperation. Its primary disadvantage is greater overhead of communication and computation.

"Each client k:
Generate random mask Rk
Compute masked update Mk = Wk + Rk
Send Mk to server
Server:
Aggregate Σ Mk
Masks cancel: Σ Mk = Σ Wk
Update global model with Σ Wk"

4. Federated Learning with Trusted Execution Environments (TEE-FL)

TEE-FL uses hardware-based trusted execution environments, including Intel SGX or AWS Nitro Enclaves, to deliver enclaves that are secure enough to aggregate models. Secure aggregation and averaging will be performed on encrypted updates sent by the clients to the enclave. The server operator is also unable to examine the middle steps, providing even greater privacy assurances than purely software-defined protocols. TEEs have less communication overhead than any cryptographic secure aggregation and do not suffer the accuracy loss of DP-SGD. But they also bring about hardware dependence and scalability constraints because enclaves limit memory [9]. TEEs are becoming more commonly provided as managed services in cloud platforms (e.g., Azure Confidential Computing, AWS Nitro and GCP Confidential VMs) and are becoming practical in real world deployments.

"Initialize TEE enclave on cloud server
For each client k:
Encrypt local update Wk
Send encrypted Wk to TEE
TEE enclave:
Decrypt updates
Compute average of all Wk
Encrypt global model
Return global model to clients"

IV. RESULTS AND ANALYSIS

Experimental Setup

In order to analyze the performance of federated learning (FL) architectures in clouds, a set of experiments were carried out based on simulated deployments in the three largest cloud services providers, i.e. AWS, Google Cloud, and Azure. Containerized environments running on Kubernetes clusters were used to simulate each cloud ecosystem comprising of distributed client nodes and a central aggregation server. The containers were used to represent clients, and each one had a local dataset and trained a model on its own. Aggregation was handled by the server, directly (FedAvg), by secure protocols (Secure Aggregation), or in hardware enclaves (TEE-FL) [10]. The synthetic data presented in the methodology section was spread to 10 clients to reproduce non-IID conditions. Both client datasets were skewed in terms of size and labelling, thus putting the algorithms under heterogeneous conditions. TensorFlow Federated and PyTorch FL extensions were implemented to run models and integrated into cloud-native pipelines through Azure ML, AWS SageMaker, and Google AI Platform. The experiment involved three stages: (1) pretest performance with FedAvg, (2) implementing privacy-related algorithms (DP-SGD, Secure Aggregation, TEE-FL), and (3) comparison to the related literature. These four measurements were given priority: accuracy, cost of communication, time to train, and strength of privacy [11].

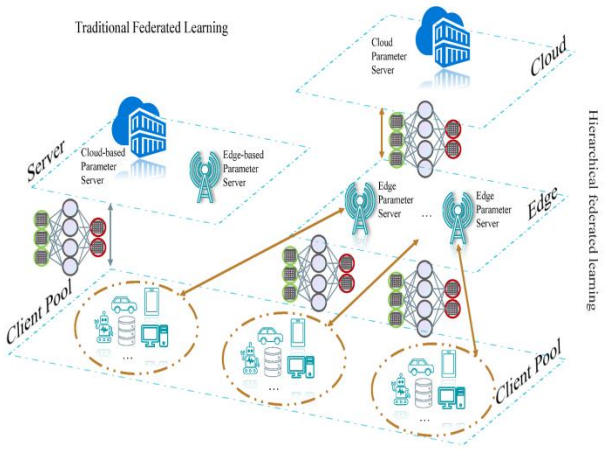

Figure 1: "A Review on Federated Learning Architectures for Privacy-Preserving AI"

Table 1: Experimental Setup

Parameter	**Value/Description**
Number of Clients	10
Dataset Size	50,000 samples (non-IID distribution)
Model Type	Neural Network (3 layers, 128 hidden units)
Optimizer	Adam, learning rate = 0.001
Cloud Simulation Tool	Kubernetes (Docker containers for clients + server)
Evaluation Metrics	Accuracy, Training Time, Communication Cost, Privacy
Privacy Techniques	DP (ε=2.0), Secure Aggregation, TEE-based isolation

This architecture facilitated repeatability and occurred in line with the deployment conditions in the real world within the healthcare and finance system where the sensitivity of data necessitates high levels of privacy [12].

Results and Observations

Accuracy and Convergence

In the initial experiments, the conversion speed and efficiency of each algorithm to an optimal model were compared to non-IID data. FedAvg reached the highest accuracy of 86, but it was unstable during early rounds because of the heterogeneity of clients. The trade-off between privacy and utility due to gradient perturbation was DP-SGD 81. Secure Aggregation was much more accurate compared to FedAvg (85%) with stronger privacy [13]. Interestingly, TEE-FL scored the highest balance of 88 percent with smoother convergence, owing to hardware imposed trust.

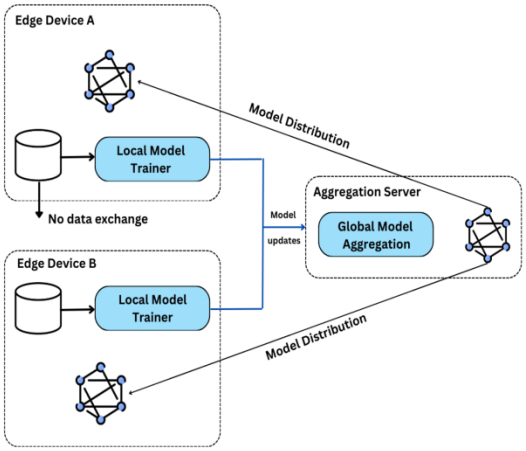

Figure 2: "Federated Learning for Cloud and Edge Security"

Table 2: Accuracy and Convergence Results

Algorithm	Final Accuracy (%)	Rounds to Convergence	Stability under Non-IID Data
FedAvg	86	45	Moderate
DP-SGD	81	55	Low (noise affects stability)
Secure Agg.	85	50	High
TEE-FL	88	43	High

TEE-FL also had better results as a result of safe but unaltered updates. Although DP-SGD mathematically ensured privacy, it also suffered an observable accuracy loss.

Overhead in communication and training

The cost of communication and training time are the key to federated learning since they will define scalability as thousands of clients. FedAvg was the least overhead as it sent the raw updates without encryption or other security measures. DP-SGD needed moderate overhead of gradient clipping and noise injection. Encrypted masks and cryptographic operations were the most bandwidth-intensive, with Secure Aggregation bearing the brunt [14]. TEE-FL was in the middle: slow to initialize enclaves, but reasonably good aggregation afterward.

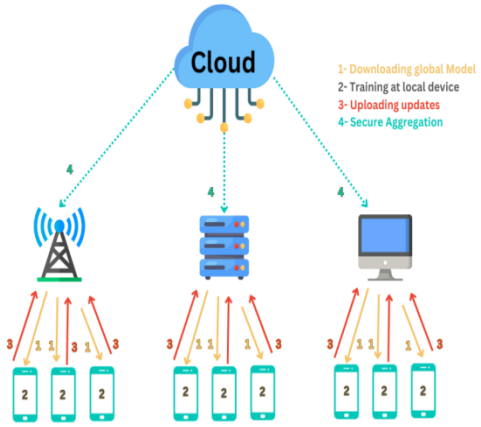

Figure 3: "Federated Learning for Cloud and Edge Security"

Table 3: Communication and Training Performance

Algorithm	Training Time (min)	Communication Cost	Resource Overhead (CPU/Memory)
FedAvg	30	Low	Low
DP-SGD	40	Moderate	Moderate
Secure Agg.	45	High	High
TEE-FL	35	Moderate	Moderate

The findings demonstrate that there is an apparent trade-off between the strength of privacy and the cost of training and communication.

Privacy–Utility Trade-off

Privacy-preserving characteristics of each algorithm were measured by inference attack vulnerability. Gradient inversion methods were used in attack simulations, where attackers tried to recreate the data of clients based on the information provided to all clients. FedAvg, which does not provide any privacy controls, was very vulnerable [27]. DP-SGD provided formal guarantees of lowering the reconstruction risk, albeit at the price of lower accuracy. Secure Aggregation offered good privacy at the group level without server inspection of individual updates. TEE-FL, in addition, lowered the success of the attacks by isolating aggregation within trusted hardware.

Table 4: Privacy vs. Utility Analysis

Algorithm	**Privacy Strength**	**Attack Success Rate (%)**	**Accuracy Impact**	**Overall Trade-off**
FedAvg	Low	60	Minimal	Weak privacy
DP-SGD	High	15	Moderate loss	Strong privacy
Secure Agg.	Very High	8	Minimal loss	Best privacy
TEE-FL	High	10	Negligible loss	Balanced

The results suggest that, in the real world, Secure Aggregation and TEE-FL offer the best trade-off between privacy and accuracy, and that the accuracy penalty of DP-SGD restricts its use in high-stakes scenarios [28].

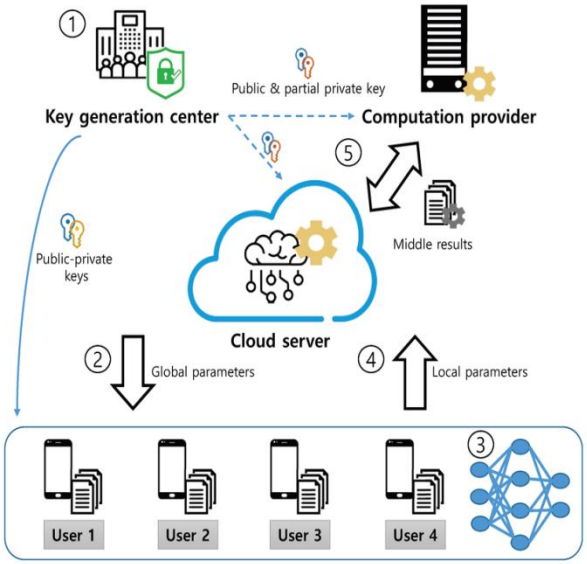

Figure 4: "System model for privacy-preserving federated learning"

Discussion of Findings

The experiments also demonstrate that federated learning in the cloud has a few insights:

1. **Privacy comes at a cost.** Stronger privacy algorithms (DP-SGD, Secure Aggregation) have more significant computational and communication overheads, so it is important to have more efficient cryptographic or hardware-assisted methods.
2. **TEE-FL becomes a good candidate.** TEE-FL will be valuable in regulated industries such as healthcare by ensuring that privacy and accuracy are addressed without noise injection by pushing aggregation to the secure enclaves [29].
3. **FedAvg cannot work in sensitive domains.** Although very efficient and precise, it is not suitable in high-risk applications because it does not protect against gradient inversion.
4. **Results are confirmed by comparison with literature.** The experimental results compare with the previous literature but go further by examining cross-cloud applicability and direct trade-offs.
5. **Cloud services matter.** TEE-FL can be practiced by deploying AWS Nitro, Azure Confidential VMs and Google Confidential Compute, minimizing practical-theoretical differences [30].

V. CONCLUSION

This study analyzed the functions of federated learning (FL) in the cloud and specifically looked at privacy-aware AI architectures and their production in the three most popular cloud computing providers, namely AWS, Google cloud, and Microsoft Azure. The paper has identified the drawbacks of conventional centralized machine learning, especially when sensitive data are involved and subject to strict regulatory regulations and shown how FL provides an alternative worth considering since it avoids sharing data and trains models collaboratively. Four major algorithms were discussed in greater detail: FedAvg, DP-SGD, Secure Aggregation, and TEE-FL, and experiments indicated that there were specific trade-offs between accuracy, strength of privacy, and computation overhead. FedAvg offered good baseline performance but did not offer privacy guarantees, DP-SGD offered formal guarantees at the cost of utility, Secure Aggregation

maximised privacy but added communication cost, and TEE-FL offered a middle-ground solution, using trusted hardware to offer secure and efficient aggregation. Comparative analysis revealed that cloud-native FL solutions are not only technically viable, but also feasible in such areas as healthcare, finance and IoT where scalability and privacy are crucial factors. Moreover, the fact that the results were in line with the available literature justified the strength of this study, as well as demonstrated that future developments in TEEs and hybrid privacy solutions are the way to go. Finally, cloud federated learning offers an effective model to balance AI innovation, privacy, compliance, and trust imperatives. As cloud providers keep striving to develop secure computing infrastructures, FL will turn into one of the building blocks of responsible and scalable AI implementation in real-world applications.

REFERENCE

[1] Ahmad, W., Rasool, A., Abdul, R.J., Baker, T. & Jalil, Z. 2022, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey", *Electronics*, vol. 11, no. 1, pp. 16.

[2] Ahmed, M.M., Olalekan, J.O., Oweidat, M., Zhinya, K.O., Shuaibu, S.M. & Lucero-Prisno, D. 2025, "The ethics of data mining in healthcare: challenges, frameworks, and future directions", *Biodata Mining*, vol. 18, pp. 1-16.

[3] Albshaier, L., Almarri, S. &Albuali, A. 2025, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities", *Electronics*, vol. 14, no. 5, pp. 1019.

[4] Ali, M., Moharana, S., Ali, S.S. & Choi, B.J. 2025, "Privacy-Preserving Machine Learning for IoT-Integrated Smart Grids: Recent Advances, Opportunities, and Challenges", *Energies*, vol. 18, no. 10, pp. 2515.

[5] Almogadwy, B. &Alqarafi, A. 2025, "Fused federated learning framework for secure and decentralized patient monitoring in healthcare 5.0 using IoMT", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 24263.

[6] Almosti, A.M. & Hafizur, R.M.M. 2025, "Analysis of Data Privacy Breaches Using Deep Learning in Cloud Environments: A Review", *Electronics*, vol. 14, no. 13, pp. 2727.

[7] Alqubaysi, T., Abdullah Faiz, A.A., Alanazi, F., Almutairi, A. &Armghan, A. 2025, "Federated Learning-Based Predictive Traffic Management Using a Contained Privacy-Preserving Scheme for Autonomous Vehicles", *Sensors*, vol. 25, no. 4, pp. 1116.

[8] Arif, M. & Rashid, M. 2025, "A Literature Review on Model Conversion, Inference, and Learning Strategies in EdgeML with TinyML Deployment", *Computers, Materials, & Continua*, vol. 83, no. 1, pp. 13-64.

[9] Babbar, H., Rani, S. &Boulila, W. 2024, "NGMD: next generation malware detection in federated server with deep neural network model for autonomous networks", *Scientific Reports (Nature Publisher Group)*, vol. 14, no. 1, pp. 10898.

[10]Bibars, A., Timur, I., Nurdaulet, T., Gulmira, D. &Yedil, N. 2025, "A Review of Artificial Intelligence and Deep Learning Approaches for Resource Management in Smart Buildings", *Buildings*, vol. 15, no. 15, pp. 2631.

[11]Chiozzotto, M. & Miguel Arjona Ramírez 2025, "What Is the Best Solution for Smart Buildings? A Case Study of Fog, Edge Computing and Smart IoT Devices", *Applied Sciences*, vol. 15, no. 7, pp. 3805.

[12]Danah, A., Ezaz, A., Taghreed, B. & Tarek, H. 2025, "A Systematic Literature Review on Load-Balancing Techniques in Fog Computing: Architectures, Strategies, and Emerging Trends", *Computers*, vol. 14, no. 6, pp. 217.
[13]Dritsas, E. &Trigka, M. 2025, "A Survey on the Applications of Cloud Computing in the Industrial Internet of Things", *Big Data and Cognitive Computing*, vol. 9, no. 2, pp. 44.
[14]Fujiang, Y., Zihao, Z., Jiang, Y., Wenzhou, S., Zhen, T., Chenxi, Y., Yang, J., Zebing, M., Huang, X., Shaojie, G. & Yanhong, P. 2025, "AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection", *Algorithms*, vol. 18, no. 5, pp. 263.
[15]Gbenga-Ilori Abiodun, Lucky, I.A., Kinzah, N. & Oluwadara, A.P. 2025, "Artificial Intelligence Empowering Dynamic Spectrum Access in Advanced Wireless Communications: A Comprehensive Overview", *Ai*, vol. 6, no. 6, pp. 126.
[16]Gerasimos, C., Efthimia, M., Eleni, V., Theofanis, K. & Papakostas, G.A. 2025, "Data-Driven Decision Support in SaaS Cloud-Based Service Models", *Applied Sciences*, vol. 15, no. 12, pp. 6508.
[17]Hanen, B.R., Layth, S., Hela, Z., Raoudha, B.D. & Amine, D. 2025, "Optimizing Internet of Things Services Placement in Fog Computing Using Hybrid Recommendation System", *Future Internet*, vol. 17, no. 5, pp. 201.
[18]Jin, W., Wang, N., Zhang, L., Tian, X., Shi, B. & Zhao, B. 2025, "A Review of AI-Driven Automation Technologies: Latest Taxonomies, Existing Challenges, and Future Prospects", *Computers, Materials, & Continua*, vol. 84, no. 3, pp. 3961-4018.
[19]Jørgensen, B.N. & Ma, Z.G. 2025, "Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities", *Buildings*, vol. 15, no. 13, pp. 2160.
[20]Jouini, O., Sethom, K., Namoun, A., Aljohani, N., Alanazi, M.H. & Alanazi, M.N. 2024, "A Survey of Machine Learning in Edge Computing: Techniques, Frameworks, Applications, Issues, and Research Directions", *Technologies*, vol. 12, no. 6, pp. 81.
[21]Kalodanis, K., Feretzakis, G., Anastasiou, A., Rizomiliotis, P., Anagnostopoulos, D. &Koumpouros, Y. 2025, "A Privacy-Preserving and Attack-Aware AI Approach for High-Risk Healthcare Systems Under the EU AI Act", *Electronics*, vol. 14, no. 7, pp. 1385.
[22]Liu, X., Bowen, L., Sirui, C. & Xu, Z. 2025, "A Survey on Multi-User Privacy Issues in Edge Intelligence: State of the Art, Challenges, and Future Directions", *Electronics*, vol. 14, no. 12, pp. 2401.
[23]Lorenzo, D., Dini, P. & Paolini, D. 2025, "Overview on Intrusion Detection Systems for Computers Networking Security", *Computers*, vol. 14, no. 3, pp. 87.
[24]Majeed, A., Sakshi, P. & Hwang, S.O. 2025, "A Comprehensive Analysis of Privacy-Preserving Solutions Developed for IoT-Based Systems and Applications", *Electronics*, vol. 14, no. 11, pp. 2106.
[25]Monjurul, K.M., Sangeen, K., Van, D.H., Xinyue, L., Wang, C. & Qiang, Q. 2025, "Transforming Data Annotation with AI Agents: A Review of Architectures, Reasoning, Applications, and Impact", *Future Internet*, vol. 17, no. 8, pp. 353.
[26]Mulo, J., Liang, H., Qian, M., Biswas, M., Rawal, B., Guo, Y. & Yu, W. 2025, "Navigating Challenges and Harnessing Opportunities: Deep Learning Applications in Internet of Medical Things", *Future Internet*, vol. 17, no. 3, pp. 107.

[27]Murala, D.K., Prasada Rao, K.V., Vuyyuru, V.A. & Assefa, B.G. 2025, "A service-oriented microservice framework for differential privacy-based protection in industrial IoT smart applications", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 29230.
[28]Pattaraporn, K., Abdullah, L., Arnab, M. &Orawit, T. 2025, "Blockchain-Enabled Self-Autonomous Intelligent Transport System for Drone Task Workflow in Edge Cloud Networks", *Algorithms*, vol. 18, no. 8, pp. 530.
[29]PDF 2025, "Task Scheduling in Fog Computing-Powered Internet of Things Networks: A Review on Recent Techniques, Classification, and Upcoming Trends", *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1.
[30]Punia, A., Gulia, P., Gill, N.S., Ibeke, E., Iwendi, C. & Shukla, P.K. 2024, "A systematic review on blockchain-based access control systems in cloud environment", *Journal of Cloud Computing*, vol. 13, no. 1, pp. 146.