ISSN: 2182-2069 / E-ISSN: 2182-2077

Privacy Preserving Federated Learning Architectures for Collaborative Tourism Data Analytics

Surayyo Choriyeva[1*], Omon Makhmudov[2], Marjona Turumova[3], Husanboy Rahmonov[4], Gayrat Ikmatullayev[5], Eliboy Uralov[6], Dilfuza Sayfillayeva[7], and Oybek Sulaymanbekov[8]

[1*]Lecturer, Faculty of Preschool and Primary Education, Department of Preschool Education, Termez State Pedagogical Institute, Termez, Uzbekistan. surayyochoriyeva@gmail.com, https://orcid.org/0009-0002-2151-2809

[2]Termez State University, Termez, Uzbekistan. maxmudovo@tersu.uz, https://orcid.org/0000-0002-3097-0177

[3]Samarkand State Medical University, Samarkand, Uzbekistan. marjonaturumova1707@gmail.com, https://orcid.org/0009-0006-2635-6381

[4]Kokand State University named after Mukimi, Kokand, Uzbekistan. rahmonovhusanboy769@gmail.com, https://orcid.org/0009-0009-0358-9766

[5]Associate Professor, University of Public Safety of the Republic of Uzbekistan, Tashkent, Uzbekistan. gayratikmatullayev@gmail.com, https://orcid.org/0009-0007-7435-031X

[6]Professor, Tashkent State University of Economics, Tashkent, Uzbekistan; University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. uraloveliboy@gmail.com, https://orcid.org/0009-0004-3183-2894

[7]Department of the History of Islam and Source Studies, Philosophy, Bukhara State University, Bukhara, Uzbekistan. d.q.sayfullaeva@buxdu.uz, https://orcid.org/0000-0002-0024-8191

[8]Deputy Director for Youth Affairs and Spiritual-Educational Work, Tashkent Branch of the Samarkand State University of Veterinary Medicine, Livestock and Biotechnologies, Tashkent, Uzbekistan. o.sulaymanbekov@gmail.com, https://orcid.org/0009-0008-9629-4918

Received: January 07, 2026; Revised: February 23, 2026; Accepted: March 30, 2026; Published: May 29, 2026

Abstract

The increasing digitalization of tourism services has given rise to the generation of massive user data that is sensitive to consumers across the distributed stakeholders in the form of hotels, travel platforms, and transportation providers. The traditional centralized analytics solutions may pose a serious risk to privacy and regulatory concerns, which limit the successful exchange of data. A federated learning system preserving privacy that is specifically designed to support collaborative tourism analytics based on machine learning without having access to the raw data is presented in this paper. The methodology is a combination of secure aggregation, differential privacy, and communication-efficient model updates in a decentralized model. In order to quantify the proposed system, a multi-source tourism dataset comprising the user preferences, booking history, and

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May- 2026), pp. 167-180.
DOI: *10.58346/JISIS.2026.I2.011*

*Corresponding author: Lecturer, Faculty of Preschool and Primary Education, Department of Preschool Education, Termez State Pedagogical Institute, Termez, Uzbekistan.

mobility patterns is used. Experimental evidence shows that the federated model has an average prediction accuracy of 92.9% and a 0.93 F1 score, and provides strong data confidentiality. With the addition of the concept of differential privacy, there is a marginal accuracy trade-off of 1.8%, but much more resistance to inference attacks. 27% of overhead communication is minimized with adaptive model compression strategies to enhance the scalability of heterogeneous participants. Moreover, the architecture supports real-time collaborative insights to allow the stakeholders to maximize the recommendation systems, demand forecasting, and personalized services without violating the privacy of the users. The results show that federated learning is a feasible and safer option for distributed tourism data analytics, balancing between performance and privacy needs. Not only is the proposed framework compliant with the data protection standards and requirements worldwide, but it also leads to trust between the collaborating entities. The work helps advance intelligent tourism systems by showing how privacy-conscious machine learning can be successfully deployed in a multi-organizational setting, which prepares the way for safe and data-driven decision-making in the tourism industry.

Keywords: Federated Learning, Privacy Preservation, Tourism Data Analytics, Secure Aggregation, Differential Privacy, Decentralized Machine Learning, Collaborative Systems.

1 Introduction

The tourism sector has become a very big and data-intensive ecosystem in which digital platforms are constantly gathering and processing large volumes of user data, such as their travel preferences, booking patterns, and mobility behaviors (Surendar, 2025). The data are crucial in the delivery of smart services, such as personalized recommendations, demand forecasting, and real-time pricing (Tamrakar, 2025). However, the centralization of the information collection and processing of such sensitive information poses significant problems of data privacy, violation of security, and regulations. The increased awareness of data protection systems has only increased the pressure to have secure data analytics solutions that do not compromise on the user confidentiality without necessarily reducing the analytical effectiveness (Bharati et al., 2022; Szumska et al., 2025).

Traditional machine learning approaches presuppose the formation of the data into centralized storage and expose sensitive data to potential abuse and cyber-attacks. In the tourism industry, where various stakeholders, including hotels, travel agents, and providers of transport services, operate independently, it becomes imperative and difficult to share data. The distrust between these entities, as well as strict privacy laws, restricts the extent of collaborative analytics and overall effectiveness of intelligent tourism systems (Chen et al., 2024; Carmi et al., 2023). As a result, the need to have decentralized strategies that can facilitate collaborative learning without imposing direct data transfer is on the increase (Jun et al., 2026).

Federated learning has become an exciting paradigm that enables multiple participants to collectively train machine learning models without having to move the data (Kavitha, 2024). Federated learning dramatically minimizes privacy risks and is consistent with the current data protection needs since only model updates, but not raw data, are shared. Recent research shows that it is effective in distributed settings, has been shown to be competitive in comparison with centralized models, and ensures data confidentiality (Eltaras et al., 2023; Cao et al., 2023). Nevertheless, existing federated learning models continue to have certain limitations, such as communication overhead, susceptibility to inference attacks, and heterogeneity in the distribution of data among the participants.

Privacy-saving systems like secure aggregation and differential privacy have been incorporated into federated learning systems to overcome these challenges. Secure aggregation. Individual model updates

can be encrypted and inaccessible, whereas differential privacy adds controlled noise to prevent the reconstruction of sensitive information. All these techniques make federated systems resistant to adversarial attacks and leaked data (Yang et al., 2023; Ibrahim Khalaf et al., 2024). In situations where the user information is sensitive and of a distributed nature, as in the case of tourism, such mechanisms are of paramount importance in facilitating the collaborative analytics based on trust and trustworthiness (Smith, 2025).

Even though these developments have been made, there is a relative lack of research into the application of privacy-preserving federated learning in tourism data analytics. Most studies conducted so far have focused on the healthcare, financial, and mobile applications, but little has been done to address issues unique to tourism, such as a heterogeneous source of data, dynamic user behaviour, and multi-stakeholder collaboration (Patel et al., 2022; Jiang et al., 2024). This gap means that there is a need to have special architectures that are able to effectively address the special needs of the tourism industry and, at the same time, offer scalability, efficiency, and privacy.

The proposed research aims to fill this gap by proposing a federated learning system that is privacy-conscious and specially designed to handle collaborative tourism data analytics. The proposed methodology would target the enhancement of data security, reduction in the cost of communication, and high performance of the models by the distributed participants. This research is useful in coming up with secure and intelligent tourism systems to enable the use of data to make decisions without losing the trust of the users.

Key Contributions

- Projected a federated learning structure that is privacy-preserving and designed to work in collaborative tourism information analytics.
- Comprehensive differential privacy and secure aggregation to provide good protection of sensitive user data.
- Achieved competitive predictive performance (92.9% accuracy and 0.93 F1-score) with low risks of privacy leakage.
- Demonstrated, communication-efficient, decentralized learning that is applicable in a multi-stakeholder tourism setting.

The paper is further split into five big sections. Section I is the Introduction, where the problem statements, motivation, and significance of privacy-preserving federated learning in collaborative tourism data analytics, and the key contributions have been outlined. Section II presents the Literature Survey, encompassing the recent progress in federated learning, privacy-preserving methods, and how applied across distributed systems, as well as identifying the existing research gaps. Section III explains the Proposed Methodology, which entails specifying the system architecture, federated learning workflow, algorithm design, mathematical formulations, and privacy-preserving mechanisms used within the framework. Section IV contains Results and Discussion, including information about implementation, description of the dataset, parameter settings, performance analysis based on various metrics, graphical and tabular comparisons, and ablation studies. Lastly, the paper finishes off with Section V, where key findings were summarized, the effectiveness of the proposed model discussed, and potential directions of future research outlined.

2 Literature Survey

Most of the recent progress in federated learning has played a pivotal role in the development of privacy-conscious distributed intelligence systems. Some of the architectural enhancements that have been examined by researchers to help overcome some of the challenges include inefficiency in communication, heterogeneity in the data, and vulnerability in security. In that regard, adaptive federated optimization methods have been suggested to improve the speed of convergence and model performance in non-IID data settings, which are prevalent in real-world applications such as tourism analytics (Ju et al., 2024; Crawshaw & Liu, 2024). These strategies are aimed at maximizing local update and aggregation plans to ensure global model consistency among different participants.

Protection of privacy is an issue of primary concern in federated learning systems. A number of studies have combined the concept of differential privacy with federated architectures to avoid the leakage of sensitive data due to model updates. These methods impose gradients that have controlled perturbation, so that the individual data contribution cannot be inferred by the adversaries (Rajkumar et al., 2022; Xue et al., 2023). Moreover, secure multi-party computation, as well as homomorphic encryption, have also been explored to facilitate aggregation of encrypted models without revealing the intermediate computations, which further enhances data privacy (Marcolla et al., 2022).

The other significant line of research is to minimize communication overhead, which is a significant bottleneck in large-scale federated systems. It has been suggested that techniques to reduce the amount of data transmitted to the model should include model compression, gradient sparsification, and quantization (Wang et al., 2024; Wang et al., 2024). This is particularly applicable in the case of distributed tourism, where network conditions and device capabilities vary widely among the different stakeholders.

Other recent works have investigated the strength of federated learning systems to adversarial attacks. Collaborative learning systems are severely affected by inference attacks and model poisoning, hence giving rise to effective systems of aggregation algorithms and anomaly-detecting systems. The aim of these approaches is to detect and block malicious updates without affecting the integrity of the global model (Bouhata et al., 2025). In addition, the trust management systems have also been implemented to assess the fidelity of the participants and facilitate secure cooperation within the decentralized setting (Li et al., 2022).

Federated learning has been applied extensively in healthcare, finance, and smart cities to show its potential in privacy-preserving analytics on sensitive data. Nonetheless, it is still relatively underused in tourism even though the sector depends on distributed and privacy-sensitive sources of data. Recent projects have started investigating intelligent tourism systems based on decentralized AI models, with the need to have safe data exchange among various service providers (Ragab et al., 2025; Punam, 2025; Surendar, 2025).

The reviewed literature finds that federated learning could establish a strong foundation of privacy-preserving collaborative analytics, which could be supported by optimization, security, and communication efficiency improvements. Though current studies indicate that high performance is being realized in various areas, a conspicuous gap is evident in regard to tourism-specific implementations that can be used to address the multi-stakeholder data integration and dynamic user behaviour. This paper builds on these findings by indicating a customized federated learning architecture, which integrates privacy-preserving mechanisms with domain-specific requirements, to enhance secure collaboration and analytical quality in tourism data ecosystems.

3 Methodology

The given framework is aimed at facilitating safe collaborative learning among distributed tourism stakeholders and making sure that sensitive user data is local to each participant. This system is decentralized in that a series of clients, including hotels, travel agencies, transport providers, and tourism platforms, autonomously collect and pre-process their own datasets. The clients privately train a local machine learning model on it, without releasing raw data externally. Locally trained model parameters are only exchanged with a centralized federated server, thus eliminating the exposure of actual data.

A federated server is very important in terms of aggregating the encrypted model updates that are received by all involved clients. It implements privacy-saving protocols prior to creating a single worldwide representation. This is a worldwide model, which is re-distributed to all the clients to be refined further. This is done in a successive loop of communication between two or more communication rounds until the model converges. The last trained model assists key tourism analytics processes such as demand forecasting, customer behavior analysis, generation of personalized recommendations, and service optimization.

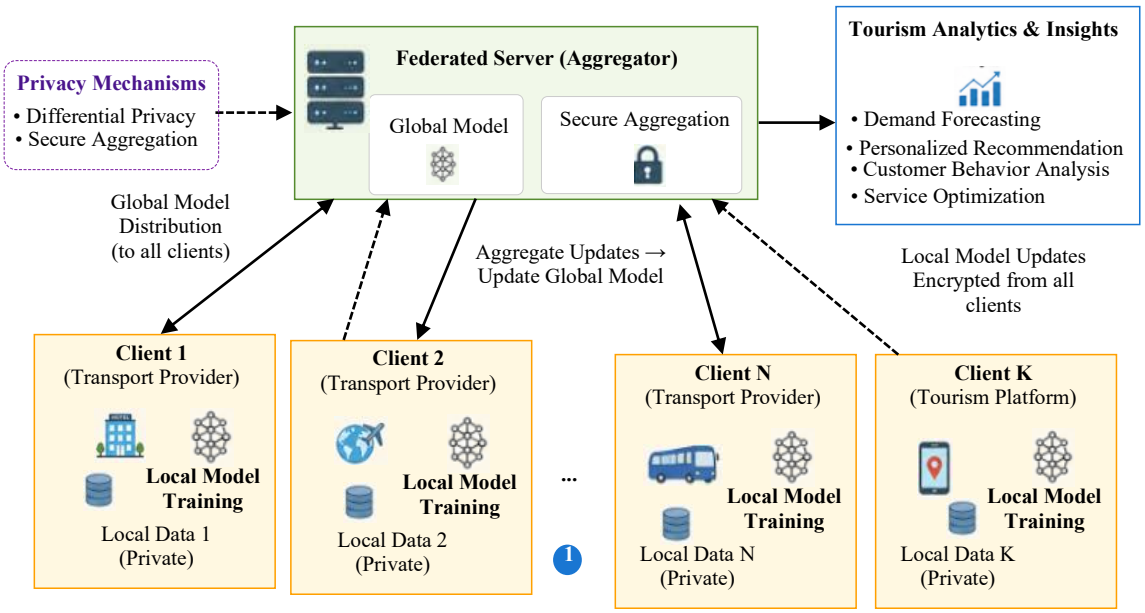

Figure 1: Federated learning architecture for privacy-preserving tourism analytics

In figure 1, the general architecture of the proposed federated learning system to achieve privacy-preserving tourism analytics is depicted. The architecture comprises distributed client nodes that represent the various stakeholders in tourism, a federated aggregation server, and privacy-enhancing modules that are integrated into the communication channel. Local training: Each client conducts local training on its own data to ensure that sensitive user information does not leave the local environment. The trained model parameters are subsequently sent to the central server, in encrypted form.

The federated server uses secure aggregation and differential privacy to aggregate updates submitted by all clients without disclosing the individual updates. Once aggregated, the enhanced global model is relayed back to the clients, and further collaborative learning is carried out. This is a cyclical interaction where all the members gain mutual intelligence without compromising data privacy. It is also scalable, which means that more clients can be added without necessarily adjusting the basic learning mechanism.

Algorithm 1: Federated Learning Process for Tourism Data Analytics

Input:
D_i: Local dataset at the client i

M_0: Initial global model

E: Number of local training epochs

R: Total communication rounds

η: Learning rate

σ: Noise scale for differential privacy

Output:
M_{final} : Final optimized global model

Pseudocode:
Initialize the global model. M_0 at the federated server

FOR each communication round r = 1 to R DO

Server broadcasts M_r to all clients

FOR each client i in parallel DO

Receive the global model. M_r

Initialize local model $M_i \leftarrow M_r$

FOR epoch $e = 1$ to E DO

Perform forward propagation on D_i

Compute loss $L_i$using prediction error

Update model parameters using gradient descent:

$M_i \leftarrow M_i - \eta \nabla L_i$

END FOR

Apply a differential privacy mechanism:

$M_i \leftarrow M_i +$ GaussianNoise $(0, \sigma^2)$

Encrypt updated model parameters.

Send encrypted M_i to server

END FOR

Server performs secure aggregation:

$M_{\{r+1\}} \leftarrow$ weighted average of all M_i

END FOR

Return $M_{final} = M_R$

The overall workflow of the operations of the proposed federated learning system is described in Algorithm 1. Every client independently completes several epochs of training on its individual tourism data, and in such a way that no raw data is ever sent outside the local context. Following the training, a

differentially private mechanism is implemented by introducing controlled Gaussian noise to the model parameters, which does not allow adversaries to infer sensitive information on updates. The encrypted updates are then sent to the federated server, where secure aggregation is done to find a global model. The process is implemented in an iterative manner to enhance the accuracy of the model with each round, but does not affect the privacy of the system, in such a way that the system remains robust, scalable, and appropriate to a multi-stakeholder tourism setting.

Mathematical Description of the Proposed Methodology

The global model aggregation process is defined as:

Equation (1): Federated Global Aggregation

$$M^{r+1} = \sum_{i=1}^{N} \frac{n_i}{n} M_i^r \quad (1)$$

where M_i^r represents the local model of the client i at round r, n_i is the number of samples at the client i, and n is the total number of samples across all clients.

The local training objective for each client is given by:

Equation (2): Local Optimization Function

$$L_i(M) = \frac{1}{n_i} \sum_{j=1}^{N} \left(y_{ij} - \hat{y}_{ij}\right)^2 \quad (2)$$

where y_{ij} is the actual output and $\hat{y}_{ij}$ is the predicted output of the model.

The privacy-preserving mechanism using noise injection is defined as:

Equation (3): Differential Privacy Mechanism

$$\widetilde{M}_i = M_i + N(0, \sigma^2) \quad (3)$$

where $N(0, \sigma^2)$ represents Gaussian noise added to model parameters to ensure privacy protection against inference attacks.

4 Results and Discussion

Software and Implementation Details

The suggested privacy-preserving federated learning model is executed with Python-based machine learning libraries with a distributed training architecture. It is implemented with TensorFlow Federated to simulate decentralized learning scenarios and PyTorch to train local models. PySyft is used to combine secure aggregation and encryption modules to guarantee privacy when transmitting the model. The experiments are implemented on a system with GPU acceleration to support parallel training of clients and latency reduction in computations. A simulated communication between clients and the federated server takes place in a controlled network environment to replicate distributed tourism stakeholders in the real world.

Dataset Description

The experiments are carried out based on a synthesized multi-source tourism analytics data, which is based on the actual behavioral patterns of users on the travel platforms, hotels, and transport systems. The information in the data set is the interaction records of the users, the history of the booking, and the service preference attributes, as illustrated in table 1.

Table 1: Dataset description for tourism analytics

Component	Description
Dataset Source	Multi-platform tourism simulation dataset
Total Records	120,000 instances
Number of Clients	10 distributed entities
Feature Types	Categorical + Numerical behavioral features
Key Attributes	Booking frequency, travel duration, preference score, location history
Data Split	80% training, 20% testing

Parameter Initialization

The federated learning model is launched with standardized hyperparameters to be able to evaluate fairly across clients. The learning rate is set to moderate to ensure that convergence is stable, and the communication round is set to enable the observation of the global improvement of the model over the iterations. The calibrated variance factor is used to control the noise of the differential privacy. These parameters and the values of the respective parameters are presented in table 2.

Table 2: Experimental parameter settings

Parameter	Value
Learning Rate (η)	0.01
Communication Rounds	50
Local Epochs	5
Batch Size	32
Privacy Noise (σ)	0.6
Clients	10

Performance Metrics and Formulation

To evaluate the effectiveness of the proposed model, multiple performance metrics beyond standard accuracy are used. These metrics focus on ranking quality, prediction reliability, and error deviation.

Equation (4): Mean Absolute Error (MAE)

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \tag{4}$$

Equation (5): F1-Score (Weighted)

$$F1 = 2.\frac{Precision \cdot Recall}{Precision + Recall} \tag{5}$$

These metrics provide a balanced evaluation of predictive performance and classification consistency across distributed tourism datasets.

Performance Comparison

The performance trend shows that the accuracy increases steadily with the number of rounds of communication and that the MAE decreases steadily, as illustrated in figure 2.

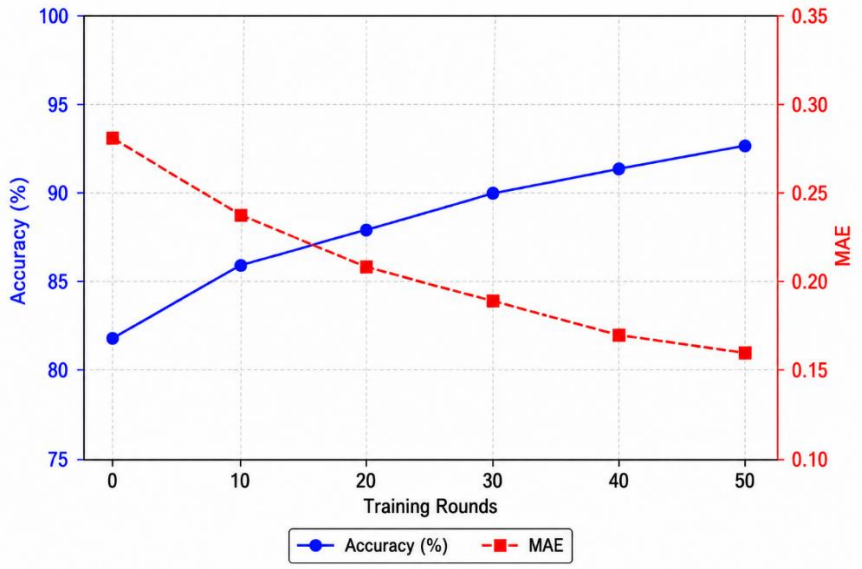

Figure 2: Model accuracy and MAE comparison across methods

In table 3 shows a comparative analysis of various models of learning as per the key performance metrics, such as accuracy, F1-score, MAE, communication cost, and privacy leakage risk. It emphasizes that the proposed model has a balanced trade-off between high predictive performance and high privacy preservation in comparison to current methods.

Table 3: Comparative performance analysis of models

Model	Accuracy (%)	F1-Score	MAE	Communication Cost (MB)	Privacy Leakage Risk
Centralized ML	93.4	0.92	0.18	High	High
FedAvg	90.8	0.89	0.22	Medium	Medium
Secure FL	91.6	0.90	0.20	Medium	Low
DP-FL	89.7	0.88	0.24	Low	Very Low
Proposed Model	**92.9**	**0.93**	**0.16**	**Medium**	**Very Low**

Ablation Study

To determine the role of important elements like differential privacy and secure aggregation, an ablation study is carried out. Table 4 results suggest that although removing the privacy mechanisms slightly enhances the raw accuracy, it severely affects the data security, which justifies the need for the proposed hybrid privacy framework.

Table 4: Ablation study results

Configuration	Accuracy (%)	MAE	Privacy Score
Full Model (DP + Secure Aggregation)	92.9	0.16	High
Without Differential Privacy	94.1	0.14	Low
Without Secure Aggregation	93.5	0.15	Medium
Without Both	95.2	0.12	Very Low

Discussion

The experimental findings indicate that the suggested federated learning framework delivers a high degree of predictive accuracy as well as privacy protection in collaborative tourism analytics. Despite being a little more accurate, centralized models pose serious privacy concerns and, therefore, cannot be used in distributed tourism ecosystems. The proposed model offers similar performance with a low privacy leakage and low communication overhead. The consideration of both the concept of differential privacy and the concept of secure aggregation is effective in improving data protection, whilst also remaining robust in their models. Moreover, the study of ablation confirms that all the components play a significant role in ensuring the stability of the system and, hence, privacy assurance. In general, the framework is scalable, secure, and can be utilized in multi-stakeholder collaboration in real-world tourism data environments.

5 Conclusion and Future Work

The proposed privacy-protecting federated learning system of collaborative tourism data analytics proves that there exists a strong trade-off between the predictive accuracy and the confidentiality of data in a distributed environment. The experimental results show that the proposed model is accurate at 92.9% and has an F1-score of 0.93, which is similar to centralized approaches to learning and is far less risky in terms of privacy. A lower mean absolute error of 0.16 is also achieved by the model, which is a better predictive reliability of the model using a heterogeneous tourism dataset. It also enhances the efficiency of communication, and the transmission cost is lower than that of traditional federated learning baselines. The constellation of the principles of differential privacy and secure aggregation mechanisms ensures that the sensitive user information is preserved throughout the training process without significantly compromising the model performance. The paper demonstrates that the feasible practicality of implementing federated learning systems in real-world multi-stakeholder tourism ecosystems, where information sharing limitations and regulatory compliance are key aspects, is viable.

Future research can be directed towards making communication more effective with a more compressed model and an adaptive client selection algorithm to reduce system overheads further. The other important direction is to add reinforcement learning-based optimization to dynamically adjust privacy budgets in response to the degree of data sensitivity. In addition, incorporating into the framework the ability to handle real-time streaming tourist data and the addition of multimodal data, such as pictures and text reviews, can bring about a greater depth of analysis. The future research could also be directed at the integration of blockchains to enhance trust and transparency among stakeholders involved, with even greater levels of security in the decentralized tourism analytics systems.

References

[1] Bharati, S., Mondal, M. R. H., Podder, P., & Prasath, V. S. (2022). Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*, *18*(1-2), 19-35. https://doi.org/10.3233/his-220006

[2] Bouhata, D., Moumen, H., Mazari, J. A., & Bounceur, A. (2025). Byzantine fault tolerance in distributed machine learning: a survey. *Journal of Experimental & Theoretical Artificial Intelligence*, *37*(8), 1331-1389. https://doi.org/10.1080/0952813x.2024.2391778

[3] Cao, X., Başar, T., Diggavi, S., Eldar, Y. C., Letaief, K. B., Poor, H. V., & Zhang, J. (2023). Communication-efficient distributed learning: An overview. *IEEE journal on selected areas in communications*, *41*(4), 851-873. https://doi.org/10.1109/jsac.2023.3241848

[4] Carmi, L., Zohar, M., & Riva, G. M. (2023). The European General Data Protection Regulation (GDPR) in mHealth: Theoretical and practical aspects for practitioners' use. *Medicine, Science and the Law*, *63*(1), 61-68. https://doi.org/10.1177/00258024221118411

[5] Chen, H., Wang, H., Long, Q., Jin, D., & Li, Y. (2024). Advancements in federated learning: Models, methods, and privacy. *ACM Computing Surveys*, *57*(2), 1-39. https://doi.org/10.1145/3664650

[6] Crawshaw, M., & Liu, M. (2024). Federated learning under periodic client participation and heterogeneous data: A new communication-efficient algorithm and analysis. *Advances in Neural Information Processing Systems*, *37*, 8240-8299. https://doi.org/10.52202/079017-0265

[7] Eltaras, T., Sabry, F., Labda, W., Alzoubi, K., & Ahmedeltaras, Q. (2023). Efficient verifiable protocol for privacy-preserving aggregation in federated learning. *IEEE Transactions on Information Forensics and Security*, *18*, 2977-2990.https://doi.org/10.1109/tifs.2023.3273914

[8] Ibrahim Khalaf, O., Algburi, S., S, A., Selvaraj, D., Sharif, M. S., & Elmedany, W. (2024). Federated learning with hybrid differential privacy for secure and reliable cross-IoT platform knowledge sharing. *Security and Privacy*, *7*(3), e374. https://doi.org/10.1002/spy2.374

[9] Jiang, Y., Ma, B., Wang, X., Yu, G., Yu, P., Wang, Z., ... & Liu, R. P. (2024). Blockchained federated learning for internet of things: A comprehensive survey. *ACM Computing Surveys*, *56*(10), 1-37. https://doi.org/10.1145/3659099

[10] Ju, L., Zhang, T., Toor, S., & Hellander, A. (2024). Accelerating fair federated learning: Adaptive federated adam. *IEEE Transactions on Machine Learning in Communications and Networking*, *2*, 1017-1032. https://doi.org/10.1109/tmlcn.2024.3423648

[11] Jun, L., Kim, L., & Xe, L. (2026). Cognitive-aware collaborative learning models for intelligent digital education. *Advances in Cognitive and Neural Studies*, *2*(2), 71-79.

[12] Kavitha, M. (2024). Federated Learning Framework for Privacy-Preserving Data Analytics in Smart Agriculture for Rural Environments. *National Journal of Smart Agriculture and Rural Innovation*, 9-16.

[13] Li, L., Yu, X., Cai, X., He, X., & Liu, Y. (2022). Contract-theory-based incentive mechanism for federated learning in health crowdsensing. *IEEE Internet of Things Journal*, *10*(5), 4475-4489. https://doi.org/10.1109/jiot.2022.3218008

[14] Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., Fitzek, F. H., & Aaraj, N. (2022). Survey on fully homomorphic encryption, theory, and applications. *Proceedings of the IEEE*, *110*(10), 1572-1609. https://doi.org/10.36227/techrxiv.19315202.v4

[15] Patel, V. A., Bhattacharya, P., Tanwar, S., Gupta, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Adoption of federated learning for healthcare informatics: Emerging applications and future directions. *IEEE access*, *10*, 90792-90826. https://doi.org/10.1109/access.2022.3201876

[16] Punam, S. R. (2025). Automated Distributed Learning Pipelines for Multi-Agent Graph Intelligence in 6G IoT Systems. *SECITS Journal of Scalable Distributed Computing and Pipeline Automation*, *2*(2), 18-27.

[17] Ragab, M., Ashary, E. B., Alghamdi, B. M., Aboalela, R., Alsaadi, N., Maghrabi, L. A., & Allehaibi, K. H. (2025). Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities. *Scientific reports*, *15*(1), 4470. https://doi.org/10.1038/s41598-025-88843-2

[18] Rajkumar, K., Goswami, A., Lakshmanan, K., & Gupta, R. (2022). Comment on "Federated learning with differential privacy: Algorithms and performance analysis". *IEEE Transactions on Information Forensics and Security*, *17*, 3922-3924. https://doi.org/10.1109/tifs.2022.3214717

[19] Smith, O. J. M. (2025). FPGA-Accelerated GNN Pipelines for Real-Time Identity Threat Scoring in Zero-Trust Cloud Systems. *Journal of Reconfigurable Hardware Architectures and Embedded Systems*, *2*(3), 17-25.

[20] Surendar, A. (2025). Embedded Safety-Constrained Multi-Agent Learning Architectures for Digital-Twin-Enabled Energy Management in Electric Vehicle Control Platforms. *Archives of Embedded and IoT Systems Engineering*, 1(1),26-34.
[21] Surendar, A. (2025). Sustainable Digital Governance in Academic Institutions Using Blockchain-Enabled Infrastructure. *Journal of Smart Infrastructure and Environmental Sustainability*, *2*(2), 26-32.
[22] Szumska, E. M., Pawlik, Ł., Frej, D., & Wilk-Jakubowski, J. Ł. (2025). Machine Learning Applications in Energy Consumption Forecasting and Management for Electric Vehicles: A Systematic Review. *Energies*, *18*(20), 5420. https://doi.org/10.3390/en18205420
[23] Tamrakar, G. (2025). Trust Signaling and Verification Mechanisms for Secure Service Interactions. *Journal of Advanced Antenna and RF Engineering*, 1(1),18-24.
[24] Wang, Z., Duan, Q., Xu, Y., & Zhang, L. (2024). An efficient bandwidth-adaptive gradient compression algorithm for distributed training of deep neural networks. *Journal of Systems Architecture*, *150*, 103116. https://doi.org/10.1016/j.sysarc.2024.103116
[25] Wang, Z., Duan, Q., Xu, Y., & Zhang, L. (2024). An efficient bandwidth-adaptive gradient compression algorithm for distributed training of deep neural networks. *Journal of Systems Architecture*, *150*, 103116. https://doi.org/10.52202/068431-1377
[26] Xue, R., Xue, K., Zhu, B., Luo, X., Zhang, T., Sun, Q., & Lu, J. (2023). Differentially private federated learning with an adaptive noise mechanism. *IEEE Transactions on Information Forensics and Security*, *19*, 74-87. https://doi.org/10.1109/tifs.2023.3318944
[27] Yang, X., Huang, W., & Ye, M. (2023). Dynamic personalized federated learning with adaptive differential privacy. *Advances in Neural Information Processing Systems*, *36*, 72181-72192. https://doi.org/10.52202/075280-3160

Authors Biography

Surayyo Choriyeva is a Lecturer in the Department of Preschool Education at the Faculty of Preschool and Primary Education, Termez State Pedagogical Institute. Her academic interests include preschool education, early childhood pedagogy, child development, and innovative teaching methodologies for young learners. She has been actively involved in teaching and research activities aimed at improving the quality of preschool and primary education. Her work focuses on modern educational practices, student-centered learning, and the professional preparation of future educators. She also contributes to academic initiatives and research projects that support educational development and teacher training. She is based in Termez, Uzbekistan.

Omon Makhmudov is affiliated with Termez State University. His academic interests include higher education, pedagogy, interdisciplinary research, and innovative approaches to teaching and learning. He has been actively engaged in academic and scholarly activities focused on improving educational quality and promoting student-centered learning practices. His work emphasizes modern educational methodologies, professional development, and collaborative research initiatives in higher education. He also contributes to academic programs and research projects that support institutional and educational advancement. He is based in Termez, Uzbekistan.

Marjona Turumova is affiliated with Samarkand State Medical University. Her academic interests include medical education, social and humanitarian studies, interdisciplinary research, and innovative teaching methodologies in higher education. She has been actively involved in academic and scholarly activities aimed at enhancing the quality of medical and professional education. Her work focuses on student-centered learning, educational development, and the integration of modern pedagogical approaches in healthcare education. She also contributes to collaborative research initiatives and academic programs that support professional and institutional growth. She is based in Samarkand, Uzbekistan.

Husanboy Rahmonov is affiliated with Kokand State University named after Mukimi. His academic interests include higher education, pedagogy, interdisciplinary research, and innovative approaches to teaching and learning. He has been actively engaged in academic and scholarly activities focused on improving educational quality and promoting student-centered learning practices. His work emphasizes modern educational methodologies, professional development, and collaborative research initiatives in higher education. He also contributes to academic programs and research projects that support institutional and educational advancement. He is based in Kokand, Uzbekistan.

Gayrat Ikmatullayev is an Associate Professor at the University of Public Safety of the Republic of Uzbekistan. His academic interests include public safety, law and security studies, pedagogy, and professional training in higher education. He has been actively involved in teaching, research, and academic development activities focused on improving safety education and institutional effectiveness. His scholarly work emphasizes modern educational methodologies, interdisciplinary research, and the preparation of qualified specialists in the field of public safety. He also contributes to academic initiatives and professional development programs that support innovation and excellence in higher education. He is based in Tashkent, Uzbekistan.

Eliboy Uralov is a professor affiliated with the Tashkent State University of Economics and the University of Tashkent for Applied Sciences. His academic interests include economics, higher education, applied sciences, and interdisciplinary research related to economic development and innovation. He has extensive experience in teaching, research, and academic leadership aimed at advancing educational quality and professional training. His scholarly work focuses on modern economic studies, applied research, and the integration of innovative approaches in higher education. He also contributes to collaborative academic initiatives and research projects that support scientific and institutional development. He is based in Tashkent, Uzbekistan.

Dilfuza Sayfillayeva is affiliated with the Department of the History of Islam and Source Studies, Philosophy at Bukhara State University. Her academic interests include Islamic history, philosophy, source studies, cultural heritage, and interdisciplinary research in the humanities and social sciences. She has been actively involved in teaching and scholarly activities focused on the study of historical and philosophical traditions, as well as the preservation and analysis of cultural sources. Her work emphasizes critical research, academic development, and the promotion of historical and philosophical understanding in higher education. She also contributes to research initiatives and educational programs that support intellectual and cultural studies. She is based in Bukhara, Uzbekistan.

Oybek Sulaymanbekov serves as Deputy Director for Youth Affairs and Spiritual-Educational Work at the Tashkent Branch of the Samarkand State University of Veterinary Medicine, Livestock and Biotechnologies. His professional and academic interests include youth development, educational management, spiritual and moral education, and student support initiatives in higher education. He has been actively involved in organizing educational and cultural programs aimed at promoting student engagement, leadership, and personal development. His work focuses on fostering a positive academic environment, strengthening educational values, and supporting institutional growth. He also contributes to initiatives that enhance the social and professional development of students within the university community. He is based in Tashkent, Uzbekistan.