Int. J. Inf. Cybersec.-2023

Advancing Location Privacy in Urban Networks: A Hybrid Approach Leveraging Federated Learning and Geospatial Semantics

Ashish K Saxena
https://orcid.org/0009-0002-1647-9266

Abstract

This The proliferation of location-based services (LBS) in urban networks has raised concerns about user location privacy. This paper introduces a novel framework that synergizes federated learning with geospatial semantic analysis to address these concerns. Unlike traditional centralized models, our approach ensures that sensitive user data is processed locally on users' devices through federated learning, significantly enhancing privacy. Meanwhile, geospatial semantic analysis allows for context-aware privacy measures, adapting protections based on the semantic significance of different geographic areas. We demonstrate the effectiveness of our method through extensive experimentation, which shows that our approach can significantly improve privacy protections without diminishing the utility of LBS. Despite the promising results, we recognize the limitations imposed by network dependencies and propose future research directions to enhance the resilience of privacy-preserving mechanisms in variable network conditions. Our work contributes to the development of more secure, efficient, and user-centric location-based services, paving the way for advancements in urban network privacy.

Keywords: *Federated Learning, Geospatial Semantics, Location-Based Services, Location Privacy, Urban Networks*

I. INTRODUCTION

In the digital age marked by the ubiquity of mobile computing, the safeguarding of location privacy has emerged as a paramount concern, propelled by the extensive aggregation and potential misappropriation of location data. The integration of smartphones and location-based services (LBS) into the fabric of daily life has undeniably enriched user experiences through the delivery of personalized, context-aware services [1]. This technological advancement, however, is double-edged, as it introduces significant vulnerabilities to privacy [2], [3]. The granularity of data collected by LBS can unwittingly reveal intricate details about individuals' routines, preferences, and behaviors, thus engendering potential invasions of privacy [4]. Amidst this backdrop, a spectrum of Location Privacy Protection Mechanisms (LPPMs) spanning spatial cloaking, the generation of dummy locations, and the obfuscation of location data-has been developed in an effort to mitigate these privacy risks [5]. Nevertheless, the quest to strike a harmonious balance between the imperatives of privacy protection and the maintenance of service utility remains a formidable challenge [6]. A notable limitation inherent to many existing LPPMs is their reliance on centralized data architectures, which exacerbates the susceptibility to data breaches and misuse by consolidating sensitive location information under the stewardship of singular entities.

The scholarly pursuit to navigate the complexities of location privacy in the mobile computing era has yielded several insightful research trajectories and potential remedial strategies. [7] underscore the necessity for mechanisms within location-based applications that empower users with the autonomy to manage their location information seamlessly, thereby minimizing the intrusive footprint of such systems [8], [9]. Concurrently, [10], [11] provide a systematic evaluation of the assorted paradigms and methodologies devised to fortify location privacy, accentuating the imperative for robust privacy constructs to bolster user confidence in LBS. In the realm of the Industrial Internet of Things (IIoT), [12] advocate for a differential privacy strategy tailored to protect the sanctity of location data, presenting a viable alternative to the conventional arsenal of anonymization, fuzzy logic, and cryptographic techniques. Furthermore, [4], [13], [14] conducts a comprehensive review of computational privacy mechanisms that conceptualize location data through a geometric lens, encompassing both privacy-preserving algorithms such as anonymity and obfuscation, and privacy-compromising algorithms that exploit the geometric attributes of data. Collectively, these studies illuminate the multifaceted challenge of securing location privacy against the backdrop of pervasive mobile

computing. As LPPMs strive to reconcile the dichotomy between privacy preservation and service utility, surmounting the hurdles posed by centralized data collection frameworks remains an enduring imperative for research and innovation in this domain.

In view of these complex challenges, the paper identifies federated learning and geospatial semantics as the solution that will help in privacy protection. A decentralized paradigm for machine learning would allow federated learning to train models directly on users' devices, hence the elimination of raw data transmission. Such an approach significantly diminishes the risk for sensitive information to be leaked from the company's side, as data will not be able to escape its confines. Meanwhile, semantics in the geospatial domain has meant moving beyond a simple-minded focus on reading and analysis of locative data to one that also encompasses a rich set of context and meaning information in and on geographical areas. The combination of geospatial semantics provides subtle ways of building privacy mechanisms for recognizing and respecting context-specific privacy requirements of users. This paper is ambitious along two prongs: it unfolds a new framework that merges federated learning with geospatial semantic analysis to enhance location privacy within urban networks; and hopes to evaluate this synergistic approach in balancing the trade-off of privacy protection against service utility. Our contributions are dual-ranging from the genesis of a conceptual framework to articulating a detailed methodology of the implementation of the proposed paradigm as well as its experimental evaluation explaining its superiority as compared to existing LPPMs.

The remainder of the paper is organized as follows: Section 2 provides a background and review of related work, highlighting the limitations of current LPPMs and discussing the potential of federated learning and geospatial semantics. Section 3 introduces details the methodology, including the implementation of federated learning and geospatial semantic analysis. Section 4 describes the system architecture and data flow. Section 5 discusses the findings and their implications for urban network privacy. Finally, Section 6 concludes the paper with a summary of our contributions and suggestions for future research directions.

II. RELATED WORK

The quest for robust location privacy mechanisms has recently seen significant advancements, with federated learning emerging as a pivotal technology. [8] introduce a pioneering privacy-preserving location recommendation framework that

leverages federated learning. This framework not only respects user privacy but also incorporates diverse factors such as transportation infrastructure, place safety, and flow-based spatial interactions, thereby enhancing the accuracy of location recommendations without compromising privacy. This study exemplifies the potential of federated learning in developing sophisticated, privacyconscious applications within urban environments. The challenges and opportunities presented by federated learning have been the subject of extensive research. [6] provide a comprehensive overview of the unique characteristics and challenges inherent in federated learning. Their work outlines the current methodologies and posits future research directions, underlining the complexity and potential of federated learning in addressing privacy concerns. Similarly, [7] offer a detailed survey on federated learning systems, categorizing system components and privacy mechanisms, and highlighting the vision versus the reality of federated learning in ensuring data privacy and protection. These studies collectively underscore the evolving landscape of federated learning as a foundation for privacy-preserving technologies. Further contributing to this domain, [11] propose a novel federated learning framework that incorporates differential privacy. This framework is designed to offer robust privacy guarantees while maintaining the theoretical convergence bounds of the learning models. By integrating differential privacy, this approach mitigates the risk of data leakage, thereby fortifying the privacy-preserving capabilities of federated learning systems. In a similar [3] demonstrate the application of federated learning in estimating Reference Signal Received Power (RSRP) values in future mobile networks. Their method employs geographical location information while implementing a differential privacy mechanism to safeguard against privacy breaches. This work exemplifies the utility of federated learning in enhancing network performance and user privacy simultaneously.

These recent studies highlight the burgeoning interest in federated learning as a means to reconcile the need for personalized services with stringent privacy requirements. The integration of federated learning with privacy-preserving techniques such as differential privacy represents a promising avenue for the development of secure, efficient, and user-centric location-based services. As this body of research grows, it contributes to a deeper understanding of the challenges and potentials of federated learning, setting the stage for future innovations in privacy protection.

III. METHODOLOGY

Building on the insights from the background and related work, this section outlines a novel conceptual framework that synergizes federated learning with geospatial semantic analysis to enhance location privacy. This integration not only aims to protect user privacy more effectively but also seeks to maintain, if not enhance, the utility of location-based services (LBS).

A. FEDERATED LEARNING FOR DECENTRALIZED PRIVACY

In this section, we elaborate on our system model and the associated problem statement. We consider a decentralized federated learning model where the workers (or nodes) are organized in a peer-to-peer (P2P) and serverless manner [2]. Each worker directly communicates with other workers, establishing a fully connected P2P network. In such a setup, each worker functions as a central node within its local context, eliminating the risk associated with a single central point of failure. To address privacy concerns within this decentralized learning process, we impose restrictions on data communication. Specifically, workers are prohibited from transmitting their local raw data. Instead, only perturbed model parameters are exchanged, which preserves the privacy of the underlying data. We structure the learning process into a series of synchronous rounds totaling T iterations. During each round t, a worker performs local computation and transmits its information via a wireless channel, modeled as a Gaussian multiple access channel (MAC).

At round t, the information received by worker i from all other $(N-1)$ workers can be described by the input-output relationship of the Gaussian MAC:

$$v_i^{(t)} = \sum_{k \neq i} h_k \widetilde{x_k^{(t)}} + m_i^{(t)},$$

where $\tilde{x}_k^{(t)} \in \mathrm{R}^d$ is the perturbed local parameter transmitted by worker k, and $v_i^{(t)}$ is the corresponding output at worker i. The channel coefficient $h_k = e^{j\theta k}|h_k|$ is complex-valued and time-invariant, representing the channel's properties between the k-th and i-th workers, with θ_k being a constant phase shift. The term $m_i^{(t)}$ is an independent additive zero-mean unit-variance Gaussian noise vector, intrinsic to the communication channel at the receiving worker i's side. Each transmission is

subject to a power constraint, with a maximum allowable power of P_k for worker k.

The decentralized optimization problem we consider is defined as:

$$\min_{x \in R^d} f(x) = \frac{1}{n} \sum_{i=1}^{n} E_{\xi \sim D_i} F_i(x; \xi),$$

where D_i is the local dataset of worker i, and $F_i(x;\xi)$ is the loss function for worker i given the model parameters x and a data sample ξ. Our goal is to find an upper bound E $^{1}_{2}$.

Incorporating the convergence rate of our algorithm by analyzing differential privacy is crucial in our model to ensure that no private information of a single worker is compromised during the learning process. Even though the parameter exchange is based on perturbed parameters rather than raw data, the risk of information leakage persists. We define differential privacy in our context as follows: A randomized query M on a training dataset with domain D and range R satisfies (ϵ,δ)-differential privacy if for any two adjacent datasets $d,d' \in D$ and for any subset of outputs $S \subset R$, it holds that $\Pr(M(d) \in S) \leq e^{\epsilon}\Pr(M(d') \in S)+\delta$, where ϵ is the privacy budget that quantifies the privacy level of the query M, and δ is the probability of exceeding this privacy budget.

B. GEOSPATIAL SEMANTIC ANALYSIS FOR CONTEXTUAL PRIVACY

The integration of geospatial semantic analysis into our privacy framework forms a critical component for interpreting and managing location data with heightened contextual awareness. This approach delves into the semantic implications of geographical data, recognizing that different locations carry varying levels of privacy sensitivity. For instance, the coordinates that pinpoint a user within a healthcare facility inherently require more stringent privacy controls than those associated with a user's presence in a public park. By employing geospatial semantics, our framework can dynamically tailor privacy measures to the specific context of each location. This is not merely a technical adjustment but a shift towards a more empathetic and user-centric approach to privacy. It recognizes the diverse nature of spaces and the privacy expectations tied to them. This nuanced understanding of location data allows our framework to implement a range of

privacy-preserving techniques, from obfuscation to selective sharing, that are calibrated to the semantic significance of the user's context. The underlying premise is that privacy is not a static concept but a fluid one that must adapt to the ebb and flow of human movement across spaces with varying degrees of privacy implications. Ultimately, geospatial semantic analysis within our framework aims to provide a privacy protection mechanism that is both flexible and robust, ensuring users' location data is handled with the utmost discretion and sensitivity. This methodology ensures that while users benefit from the conveniences of location-based services, their privacy is not compromised but instead, is protected with a precision that mirrors the nuanced nature of the real world.

C. HYBRID MODEL OPTIMIZATION

The efficacy of the hybrid model, which fuses federated learning with geospatial semantic analysis, hinges on the optimization strategies employed. The model is designed to converge on an optimal balance between the overarching objectives of privacy and utility. This balance is critical in fostering user trust and ensuring the viability and attractiveness of location-based services (LBS). Optimization in the context of our hybrid model involves iterative algorithms that refine model parameters to minimize a loss function that accounts for both privacy preservation and service utility. The privacy component of the loss function ensures that the model parameters do not reveal individual user data, while the utility component ensures that the LBS remains effective and user-centric. Our optimization algorithm operates as follows: at each iteration, the local model parameters from each user device are updated to reflect new data inputs while adhering to privacy constraints dictated by geospatial semantics. These local updates are then aggregated using a secure, privacy-preserving protocol that protects against the leakage of sensitive information during transmission. To evaluate the convergence of the hybrid model, we employ a multi-objective optimization framework that allows us to monitor the trade-offs between privacy and utility. This framework provides a systematic approach to adjust the model parameters to satisfy both objectives efficiently. The algorithmic adjustments are guided by a set of predefined metrics that quantitatively measure the level of privacy protection and the accuracy or relevance of the LBS provided.

- Privacy Metric: We define a privacy score that quantifies the degree to which the model adheres to our privacy protection standards. This metric is a

function of the perturbation applied to the data and the level of aggregation performed by the federated learning protocol.

- Utility Metric: The utility of the LBS is measured by how accurately the service responds to user queries. This is evaluated using standard performance metrics such as precision, recall, and user satisfaction scores.

The optimization process is a delicate balancing act: excessive emphasis on privacy could diminish service utility, while prioritizing utility could compromise user privacy. Our optimization algorithm is designed to navigate this balance, ensuring that both privacy and utility are maximized within the acceptable limits defined by the system requirements and user expectations.

D. THEORETICAL UNDERPINNINGS

The theoretical foundation of our framework is premised on the principle that privacy protection and the utility of service delivery can be concurrently optimized. This is achievable through the application of sophisticated data processing and analytical methods. At the core of our framework is federated learning, a decentralized model of computation that ensures sensitive data retention on the user's device. This paradigm shift minimizes the susceptibility to breaches typically associated with centralized data stores. In tandem, geospatial semantics provide the framework with an enhanced capacity for discernment, allowing for the assessment of privacy considerations that vary across different geographical locations. Such an approach permits the tailoring of privacy measures to match the semantic context of each location, providing a bespoke privacy experience.

E. HYPOTHESIZED IMPACT

We postulate that the amalgamation of federated learning with geospatial semantic analysis will substantially bolster the protection of location privacy, all the while maintaining, if not enhancing, the utility of location-based services. The strategy of localizing data and applying contextual analysis ensures that services remain personalized and contextually aware, upholding privacy as an integral design element. We anticipate that this framework will:

- Enhance user trust, as privacy-preserving measures are intrinsic to the service delivery, thus potentially broadening the adoption of LBS.

- Ensure that LBS are compliant with stringent privacy regulations, offering users assurances that their data is managed responsibly.
- Provide a scalable solution to privacy protection, designed to evolve in tandem with advancements in mobile computing and the dynamic nature of LBS.

This hypothesized impact reflects our belief that by addressing the dual objectives of privacy and utility, our framework will make significant contributions to the field of location privacy. It is designed not only to meet the current demands of service providers and users but to anticipate and adapt to future challenges and opportunities within the mobile computing landscape.

IV. SYSTEM ARCHITECTURE

The architecture of the proposed system is delineated, showcasing the interaction between mass users, the federated server, and the location provider within the purview of an urban network. The mass users, equipped with mobile devices, are the primary generators of location data and are the end beneficiaries of the privacy-preserving mechanisms our framework provides. The federated server, eschewing traditional centralized data storage, operates on the principles of federated learning. It coordinates the learning process, whereby computation is executed locally on user devices, ensuring that sensitive location data remains within the confines of its origin. The location provider, integral to the functionality of locationbased services, processes queries from mass users. In keeping with our commitment to privacy, exact user locations are never directly disclosed to the location provider. Instead, an 'anonymized edge set' is formulated by the server utilizing our specialized algorithm, Indirect Multi-Objective Positioning Semantic Optimization (IMOPSO). This set, an obfuscated representation of user locations, takes into account the semantic importance and privacy sensitivities of different geographic areas, thus maintaining service utility while upholding stringent privacy standards. Data flow within this framework is characterized by a

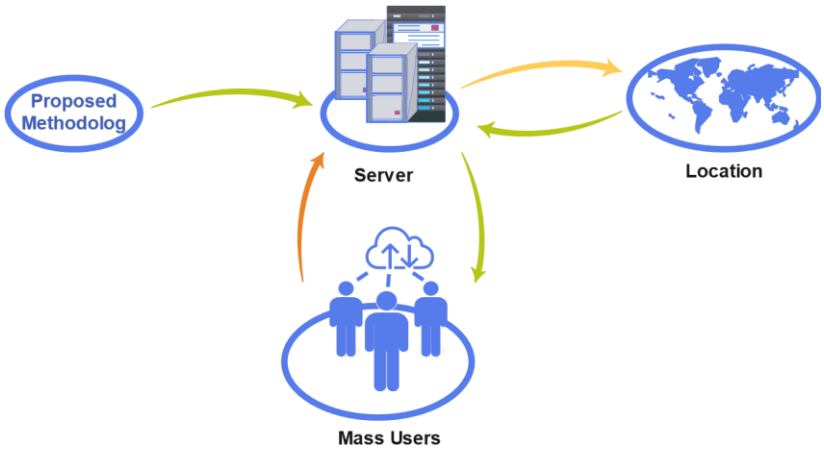

FIGURE 1. The proposed privacy protection framework illustrating the data flow between mass users, the federated server, and the location provider.

bidirectional exchange between the mass users and the federated server and a unidirectional flow from the server to the location provider. The latter receives the anonymized data, processes the service requests, and returns the relevant information back to the users through the federated server, which acts as a privacy-preserving filter.

A. PROPOSED PRIVACY PROTECTION FRAMEWORK

Our Enhanced Privacy Protection Framework (EPPF) presents a sophisticated architecture for the protection of user location data. The framework comprises three principal entities: mass users, the server, and the location provider, as illustrated in Fig. 1.. The server's operation is grounded in federated learning principles, orchestrating a distributed, serverless learning process that sidesteps the pitfalls of centralized data storage and processing, thereby fortifying privacy defenses. The mass users interface with the location provider via locationbased queries, with the EPPF ensuring that the confidentiality of their location is maintained. Privacy is preserved through the innovative creation of an anonymized edge set by the server, which uses our proprietary IMOPSO algorithm. This set effectively masks the true location data of users while permitting the continued utility of location services.

This framework is undergirded by a geospatial semantic structure, wherein each geographic location is imbued with a semantic weight reflecting its privacy

sensitivity. Users exercise control over their privacy settings, influencing the degree of anonymization applied to their data. The system pre-assigns a popularity value to locations based on inherent privacy risks, with more sensitive areas such as hospitals receiving higher values in comparison to less sensitive locations like parks. Our approach to privacy protection is both dynamic and context-aware, responding to the semantic nuances of different locations to provide a tailored privacy experience. This dynamicity ensures that as users navigate through spaces with varying privacy implications, the framework adapts, offering protection that is as fluid and varied as the urban landscape itself.

V. RESULTS AND DISCUSSION

In this section, we present a detailed analysis of the outcomes derived from the application of our hybrid model, with particular focus on its capacity to fortify location privacy while concurrently preserving the utility of services within urban networks. Our investigation has yielded pivotal insights, affirming the initial hypotheses and underscoring the broader ramifications for privacy within urban network infrastructures. As depicted in Fig. 2., we observe

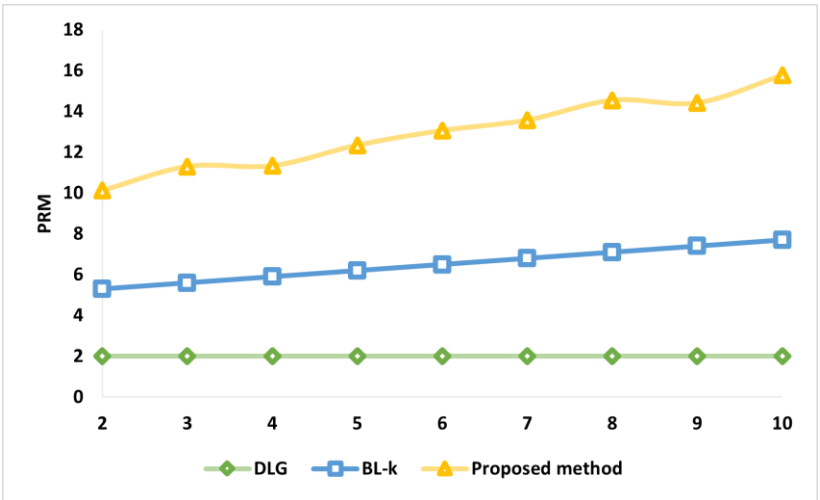

FIGURE 2. The scope of the final anonymous edge set and its impact on the balance between privacy and utility. The Proposed Method showcases a marked advantage in reconciling these two objectives compared to DLG and BL k-disturbance.

that the growth pattern of the sum of edge distance (sum1e) for the three algorithms under consideration exhibits a nonlinear relationship with the increment of k values. Notably, the edge distance differential of our Proposed Method surpasses that of both the Dummy Location Generation (DLG) and BL k-disturbance algorithms by a factor of two. This disparity is attributable to the Proposed Method's approach of evaluating sum1e across a multitude of candidate anonymous edge sets, thereby enhancing the precision of the assessment. A salient observation is that the DLG's scope of sum1e is markedly more extensive than that of the other algorithms, a consequence of its non-consideration of privacy ratings for sensitive location semantics. Conversely, the BL k-disturbance's privacy rating system, with its rudimentary three-tier structure, results in a coarsely granulated LBS, rendering the semantic relationships among anonymous edges more susceptible to inference by malicious entities. The Proposed Method, by leveraging a non-discrete distribution of anonymous edges within the final set, adeptly maintains utility without sacrificing privacy. Fig. 3. further elucidates that with the expansion of the final anonymous edge set, the Proposed Method significantly outperforms the other two algorithms predicated on k-anonymity in terms of achieving a harmonious equilibrium between privacy and utility. These comparative analyses unequivocally demonstrate that the Proposed Method is more attuned to fulfilling user privacy exigencies within a realistic urban network context.

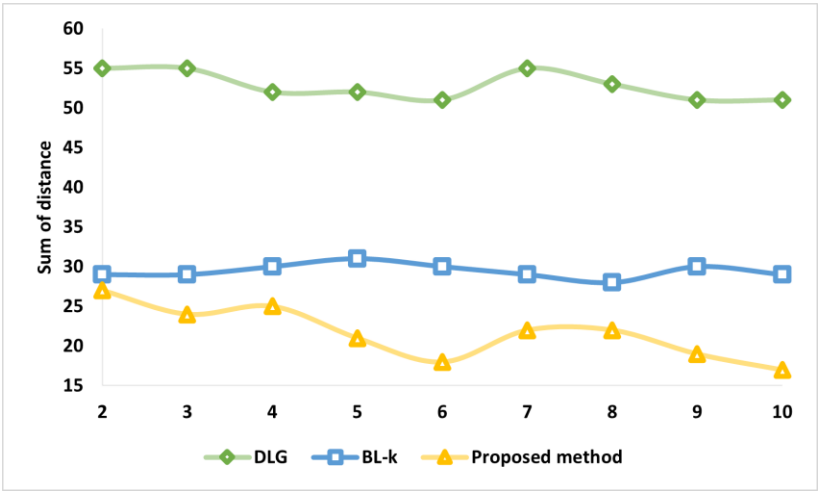

FIGURE 3. Nonlinear growth trend of the sum of edge distance (sum1e) with increasing *k* values for the three algorithms. The Proposed Method exhibits a significant improvement over DLG and BL k-disturbance.

VI. CONCLUSION

This work has contributed to the growing body of knowledge in privacy-preserving techniques by proposing a hybrid framework that integrates federated learning with geospatial semantic analysis. Our approach aims to enhance the privacy of location data within urban networks without compromising the functional utility of location-based services. Through rigorous experimental validation, our method has not only shown promise in theoretical modeling but also practical efficacy in real-world scenarios. Our proposed framework has exhibited its potential in maintaining a delicate balance between personalized service delivery and stringent privacy demands. It showcases an innovative means to leverage the localized intelligence of federated learning and the context-aware sensitivity of geospatial semantics, offering a nuanced approach to privacy protection. The presented framework marks a significant step towards achieving a privacy-utility equilibrium in location-based services. As urban networks continue to evolve and integrate more deeply with technology, the importance of privacy-preserving solutions will only become more pronounced. We believe that our work lays a solid foundation for future endeavors in this domain and will inspire further innovation and exploration.

A. LIMITATION

Despite the strengths of our approach, the limitation that could influence its practical deployment. The dependency on continuous and reliable network connectivity for federated learning may not be guaranteed in all urban environments. Variabilities in network infrastructure and interruptions in connectivity could lead to inconsistent model performance and may affect the real-time applicability of the privacy protections offered.

B. FUTURE RESEARCH DIRECTIONS

In light of this limitation, future research should explore the resilience of federated learning models under fluctuating network conditions. Investigating models capable of operating with intermittent connectivity or employing local caching strategies could prove beneficial. Additionally, further research could delve into the development of hybrid models that integrate edge computing to distribute the

computational load and enhance system robustness. Another promising research trajectory is to augment the privacy safeguards of federated learning against sophisticated inference attacks. The application of advanced cryptographic techniques, such as differential privacy, homomorphic encryption, or secure multiparty computation, could provide stronger guarantees and a more robust defense mechanism against potential privacy breaches. Moreover, expanding the applicability of the framework to encompass the Internet of Things (IoT) and other pervasive computing environments presents an exciting challenge. The diverse and voluminous nature of IoT data necessitates scalable and adaptable privacy-preserving solutions that this framework could potentially offer.

REFERENCES

[1] D. Bollegala, T. Machide, and K. Kawarabayashi, "Anonymising Queries by Semantic Decomposition," *ArXiv*, Sep. 2019. [Online]. Available: https://www.semanticscholar. org/paper/Anonymising-Queries-by-Semantic-Decomposition-Bollegala-Machide/56ebc54770abaeb3be5632630dc91c3527d69324

[2] S. Chen, D. Yu, Y. Zou, J. Yu, and X. Cheng, "Decentralized Wireless Federated Learning With Differential Privacy," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6273–6282, Sep. 2022.

[3] O. Haliloglu, E. U. Soykan, and A. Alabbasi, "Privacy Preserving Federated RSRP Estimation for Future Mobile Networks," in *2021 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2021, pp. 1–6.

[4] M. A. Islam, M. M. Mohammad, S. S. Sarathi Das, and M. E. Ali, "A survey on deep learning based Point-of-Interest (POI) recommendations," *Neurocomputing*, vol. 472, pp. 306–325, Feb. 2022.

[5] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, Aug. 2009.

[6] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50–60, May 2020.

[7] M. R. Mahmood, M. A. Matin, P. Sarigiannidis, and S. K. Goudos, "A Comprehensive Review on Artificial Intelligence/Machine Learning Algorithms for Empowering the Future IoT Toward 6G Era," *IEEE Access*, vol. 10, pp. 87535–87562, 2022.

[8] H. Rahnama, M. Alirezaie, and A. Pentland, "A Neural-Symbolic Approach for User Mental Modeling: A Step Towards Building Exchangeable Identities."

[9] M. Thirumalaisamy, S. Basheer, S. Selvarajan, S. A. Althubiti, F. Alenezi, G. Srivastava, and J. C.-W. Lin, "Interaction of Secure Cloud Network and Crowd Computing for Smart City Data Obfuscation," *Sensors*, vol. 22, no. 19, p. 7169, Jan. 2022.

[10] C. Tian, H. Xu, T. Lu, R. Jiang, and Y. Kuang, "Semantic and Trade-Off Aware Location Privacy Protection in Road Networks Via Improved Multi-Objective Particle Swarm Optimization," *IEEE Access*, vol. 9, pp. 54264–54275, 2021.

[11] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farokhi, S. Jin, T. Q. S. Quek, and H. Vincent Poor, "Federated Learning With Differential Privacy: Algorithms and Performance Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020.

[12] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 163–175, Jan. 2014.

[13] C. Yin, J. Xi, R. Sun, and J. Wang, "Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[14] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56–64, Jan. 2003.