The Scientific Temper (2024) Vol. 15 (spl): 291-297

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.34

https://scientifictemper.com/

REVIEW ARTICLE

The socio-technical opportunities and threats of crowdsensing

P. Ananthi*, A. Chandrabose

Abstract

The exponential growth of mobile crowd sensing (MCS) has provided unparalleled opportunities to collect large-scale data through a network of mobile devices, empowering diverse applications in smart cities, healthcare, and environmental monitoring. However, the inherently participatory nature of MCS raises critical privacy concerns, as sensitive user information is often at risk of exposure. This literature review examines recent advancements in employing machine learning techniques to enhance privacy preservation in MCS frameworks. It explores methods such as federated learning, differential privacy, and encryption-enhanced neural networks that aim to minimize data leakage while maintaining model accuracy. Additionally, this review analyzes the efficacy and limitations of various privacy-preserving algorithms, particularly regarding their adaptability to different MCS contexts and their impact on computational overhead and communication efficiency. Through a comprehensive synthesis of current studies, this review highlights emerging trends, identifies research gaps, and suggests future directions for developing robust privacy-preserving machine learning models tailored to the unique demands of MCS systems.

Keywords: Mobile crowd sensing, Machine learning, Privacy-preserving techniques, Sensitive information.

Introduction

Mobile crowd sensing (MCS) is a data collection paradigm that leverages the widespread adoption of mobile devices, enabling participants to gather, share, and analyze information across various domains, from public health monitoring to urban planning. MCS capitalizes on the capabilities of mobile devices, including sensors, GPS, and communication modules, to collect real-time data, offering an efficient, scalable, and cost-effective approach to harnessing large-scale environmental and social data. However, while MCS presents an innovative way to address societal needs, it also introduces significant challenges, particularly in terms of privacy preservation, which remains one of the most pressing concerns for participants and researchers alike, Liu, Y., Kong, L., & Chen, G. (2019), Boubiche, D. E., Imran, M., Maqsood, A., & Shoaib, M. (2019).

The key privacy issues in MCS stem from the sensitive nature of the collected data. Participants' location, habits, and even health status are often inferred from MCS datasets, posing potential risks of identity exposure, data misuse, and security breaches. This erosion of privacy can deter user participation, ultimately compromising the reliability and success of MCS applications. Consequently, achieving a balance between effective data utilization and strong privacy protection has become a fundamental objective in MCS research, Wang, Y., Yan, Z., Feng, W., & Liu, S. (2020).

Recent advancements in machine learning (ML) have shown promise in addressing these privacy concerns by offering solutions that protect data confidentiality while enabling robust data analysis. Among the most widely researched methods are federated learning, differential privacy, and encrypted machine learning frameworks, each of which provides distinct privacy advantages tailored to MCS. Federated learning, for example, enables collaborative model training on distributed data without requiring data centralization, thus preserving data privacy by design. Differential privacy introduces controlled data perturbations, making it difficult to infer individual data points, while cryptographic techniques secure data during processing to prevent unauthorized access, Sultana, M. N., & Chang, K. (2020), Peng, F., Tang, S., Zhao, B., & Liu, Y. (2019, May).

This literature review aims to provide a comprehensive analysis of the current state of machine learning techniques

Edayathangudy G.S Pillay Arts and Science College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli), Nagapattinam, Tamil Nadu, India.

***Corresponding Author:** P. Ananthi, Edayathangudy G.S Pillay Arts and Science College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli), Nagapattinam, Tamilnadu, India., E-Mail: ananthi.csc@gmail.com

How to cite this article: Ananthi, P., Chandrabose, A. (2024). The socio-technical opportunities and threats of crowdsensing. The Scientific Temper, **15**(spl):291-297.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.34

Source of support: Nil

Conflict of interest: None.

© The Scientific Temper. 2024

Received: 09/09/2024 **Accepted:** 30/09/2024 **Published** : 16/10/2024

applied in privacy-preserving MCS, identifying the strengths and limitations of each approach. The review begins by discussing the fundamental privacy challenges associated with MCS, followed by a detailed examination of ML-based privacy-preserving methodologies. In addition, it evaluates the effectiveness of these techniques across diverse application scenarios, including healthcare, traffic monitoring, and social sensing, where privacy concerns are particularly acute. Furthermore, this review investigates the computational and communication trade-offs inherent to privacy-preserving ML approaches, which are crucial for the scalability and sustainability of MCS systems.

Finally, by synthesizing insights from recent studies, this review identifies existing research gaps and explores potential directions for future work. Emerging fields such as adversarial learning and blockchain-based privacy solutions are examined for their potential to strengthen privacy guarantees in MCS. Through this discussion, the review aims to support researchers and practitioners in navigating the complex landscape of privacy-preserving machine learning in MCS, ultimately contributing to the development of secure, user-trustworthy MCS frameworks that encourage widespread participation and facilitate impactful data-driven insights.

Background Study On Privacy-Preserving Methods

Mobile crowd sensing (MCS) leverages the widespread use of mobile devices equipped with sensors to collect data from the environment, enabling various applications such as environmental monitoring, urban planning, and public health. The integration of crowd-sourced data allows for real-time insights and decision-making, fostering enhanced community engagement and resource management.

To address the privacy challenges in MCS, several methods have been developed, categorized into various approaches:

Data Anonymization

Anonymization techniques aim to remove personally identifiable information (PII) from the data before it is shared or processed. Common techniques include Yi, X., Lam, K. Y., Bertino, E., & Rao, F. Y. (2019):

K-Anonymity

Ensures that any individual is indistinguishable from at least k–1 others in the dataset, thereby protecting their identity.

L-Diversity

Enhances k-anonymity by ensuring that sensitive attributes within each equivalence class have diverse values, reducing the risk of attribute disclosure.

T-Closeness

Focuses on maintaining the distribution of sensitive attributes, ensuring that it is close to the overall distribution in the dataset.

Data Encryption

Encryption techniques secure data both in transit and at rest, ensuring that even if data is intercepted, it remains unreadable without the proper keys. Approaches include Pius Owoh, N., & Mahinderjit Singh, M. (2020):

Homomorphic Encryption

Allows computations to be performed on encrypted data, enabling data analysis without exposing raw data.

Secure Multi-Party Computation (SMPC)

Enables multiple parties to collaboratively compute a function over their inputs while keeping those inputs private.

Differential Privacy

Differential privacy adds a controlled amount of noise to the data or the queries made to the data, ensuring that the inclusion or exclusion of a single user's data does not significantly affect the outcome. This approach provides a mathematical guarantee of privacy, allowing for the analysis of aggregate data without compromising individual privacy, Wang, J., Wang, Y., Zhao, G., & Zhao, Z. (2019).

Access Control Mechanisms

Implementing robust access control mechanisms restricts who can view or interact with the collected data. Techniques include Wang, J., Yin, X., & Ning, J. (2021):

Role-Based Access Control (RBAC)

Assigns permissions based on user roles, ensuring that only authorized users can access sensitive data.

Attribute-Based Access Control (ABAC)

Uses user attributes and environmental conditions to determine access rights dynamically.

Secure Data Aggregation

This technique ensures that data from multiple sources can be aggregated without revealing individual data points. Methods include Yan, X., Ng, W. W., Zeng, B., Lin, C., Liu, Y., Lu, L., & Gao, Y. (2021):

Cryptographic Protocols

Using secure protocols for aggregating data, ensuring that individual contributions remain confidential.

Data Perturbation

Modifying the data before aggregation to obscure individual contributions while still allowing for meaningful analysis.

Background Study on Machine Learning

Machine learning (ML) is a subset of artificial intelligence (AI) that focuses on the development of algorithms that enable computers to learn from and make predictions or decisions based on data. Unlike traditional programming, where explicit instructions are coded, machine learning models are trained on data to identify patterns, enabling them to

generalize their findings to new, unseen data. This capability makes ML a powerful tool across various domains, including healthcare, finance, marketing, and autonomous systems. Machine learning models can be broadly classified into three main categories based on the nature of the learning task, Rahmani, A. M., Yousefpoor, E., Yousefpoor, M. S., Mehmood, Z., Haider, A., Hosseinzadeh, M., & Ali Naqvi, R. (2021):

Supervised Learning

In supervised learning, the model is trained on a labeled dataset, where each training example consists of input-output pairs. The objective is to learn a mapping from inputs to outputs. Common supervised learning algorithms include Verma, R., Nagar, V., & Mahapatra, S. (2021):

Linear Regression

Used for predicting continuous outcomes based on one or more predictor variables.

Logistic Regression

Utilized for binary classification tasks, estimating the probability of a categorical outcome.

Decision Trees

A tree-like model that splits the data into subsets based on feature values, leading to a decision about the output.

Support Vector Machines (SVM)

A classification technique that finds the hyperplane that best separates classes in the feature space.

Neural Networks

Computational models inspired by the human brain, consisting of interconnected layers of nodes (neurons) that can learn complex patterns.

Unsupervised Learning

Unsupervised learning involves training models on datasets without labeled outputs. The goal is to discover hidden patterns or structures in the data. Common unsupervised learning techniques include Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019):

Clustering Algorithms

Such as K-means and hierarchical clustering, which group similar data points together based on their features.

Principal Component Analysis (PCA)

A dimensionality reduction technique that transforms data into a lower-dimensional space while retaining the most variance.

Association Rule Learning

Methods like the Apriori algorithm, which identify interesting relationships between variables in large datasets.

Reinforcement Learning

Reinforcement learning focuses on training agents to make decisions by interacting with an environment. The agent learns by receiving rewards or penalties based on its actions. Key concepts include, Dong, H., Dong, H., Ding, Z., Zhang, S., & Chang, T. (2020), Ding, Z., Huang, Y., Yuan, H., & Dong, H. (2020):

Markov Decision Processes (MDPs)

A mathematical framework for modeling decision-making, involving states, actions, rewards, and policies.

Q-Learning

A popular algorithm that seeks to learn the value of actions in a given state to maximize cumulative rewards.

Deep Reinforcement Learning

Combines deep learning with reinforcement learning, using neural networks to approximate value functions or policies.

Literature Review

The authors design a secure aggregation algorithm (SecAgg) through the threshold Paillier cryptosystem to aggregate training models in an encrypted form. Also, to stimulate participation, we present a hybrid incentive mechanism combining the reverse Vickrey auction and posted pricing mechanism, which is proved to be truthful and fails. Results of theoretical analysis and experimental evaluation on a practical MCS scenario (human activity recognition) show that CrowdFL is effective in protecting participants' privacy and is efficient in operations. In contrast to existing solutions, CrowdFL is 3× faster in model decryption and improves an order of magnitude in model aggregation, Zhao, B., Liu, X., Chen, W. N., & Deng, R. H. (2022).

The authors proposed an efficient and strong privacy-preserving truth discovery scheme, named EPTD, to protect users' task privacy and data privacy simultaneously in the truth discovery procedure. In EPTD, we first exploit the randomizable matrix to express users' tasks and sensory data. Then, based on the matrix computation properties, we design key derivation and (re-)encryption mechanisms to enable truth discovery to be performed in an efficient and privacy-preserving manner. Through a detailed security analysis, we demonstrate that data privacy and task privacy are well preserved, Zhang, C., Zhao, M., Zhu, L., Wu, T., & Liu, X. (2022).

The authors exploited K -K-means clustering and matrix multiplication to realize a secure and efficient grouping mechanism, which achieves the selection of high-quality and accurate target users set with privacy preserving. Based on the short group signature algorithm and 0–1 encoding technique, we construct a privacy-preserving matching mechanism to guarantee the anonymous authentication and achieve the matching for task requirements and user reputation levels in a privacy-preserving way. Finally, we give a security analysis, and we evaluate the computational costs and communication overhead, and the experimental result shows the efficiency of the proposed PMTA scheme, Zhang, Y., Ying, Z., & Chen, C. P. (2022).

The authors proposed a novel Privacy-preserving and utility-aware participant selection scheme PUPS. Firstly, we claim that the total data utility of a set of participants within a certain area should be calculated according to the data quality of each participant and the location coverage of the sensing data. Secondly, a participant selection scheme has been proposed, which determines a set of participants with maximum total data utility under the budget constraint and shows that it is a Quadratic Integer Programming problem. We show that our optimization problem is a quadratic integer programming problem. Further, to preserve the data qualities and location privacy of participants, homomorphic encryption-based Euclidean distance and one-time padding schemes are integrated. Extensive simulations have been conducted to solve the selection problem. Through performance evaluation, we demonstrate the accuracy, efficacy, and scalability of PUPS by comparing it with three other selection schemes: Data Quality First Selection (DQFS), Lowest Bid Price First Selection (LBFS), and Random Selection (RS), respectively, Azhar, S., Chang, S., Liu, Y., Tao, Y., & Liu, G. (2022).

The authors proposed a novel privacy-preserving and customization-supported data aggregation scheme that can achieve multiple types of aggregation. Specifically, we utilize additive secret sharing (ASS) to protect the privacy of both sensing data and aggregation results and then propose a simplified, secure triplet generation protocol based on ASS to construct secure aggregation operations. Moreover, we design a secure comparison (SC) algorithm and a secure top-K algorithm to realize customized aggregation (i.e., statistical aggregation over top- K largest or smallest values of sensing data). The formal theoretical analysis demonstrates that the proposed scheme is effective, and the extensive experiments conducted on a real-world data set show that the proposed approach is privacy-preserving and efficient, Yan, X., Zeng, B., & Zhang, X. (2022).

In this study, the authors comprehensively survey the state-of-the-art mechanisms for protecting the location privacy of workers in MCS. We divide the location protection mechanisms into three categories depending on the nature of their algorithm and compare them from the viewpoints of architecture, privacy, computational overhead, and utility. Moreover, the authors discuss certain promising future research directions to spur further research in this area, Kim, J. W., Edemacu, K., & Jang, B. (2022).

The authors proposed a spatiotemporal-aware privacy-preserving task matching scheme, achieving efficient and fine-grained matching while protecting privacy between users and task publishers. Specifically, the time matching score (TMS) and location matching score (LMS) between users and tasks are defined for the spatiotemporal requirement of MCS. In addition, a lightweight protocol called SCP (secure computing protocol) is constructed based on Shamir secret sharing and Carmichael theorem for securely calculating TMS and LMS and matching attribute values by size and range, Peng, T., Zhong, W., Wang, G., Zhang, S., Luo, E., & Wang, T. (2023).

The authors proposed a new system architecture that adapts a two-cloud peer model while leveraging garbled circuit (GC). Users only need to transfer data to two clouds once, which realizes low user workloads while supporting dynamic users. The two cloud terminals cooperate to complete the weight update through the GC but execute the truth discovery algorithm, respectively. In this way, the noninteractive comes true and the users' workloads are transferred to the cloud server side. The weight update finish and weight privacy are fulfilled through GC. Meanwhile, the other intermediate values maintain strong privacy. At the same time, because the collaborative cloud architecture of the two clouds ensures the confidentiality of the truth value in the cloud and the homomorphism at the inquiry side, it ensures the strong privacy of the whole process from users to inquiries, Liu, X., Zhou, S., Zhang, W., Dong, T., & Li, K. (2023).

The authors [24] presented a lightweight scheme called LRRV in MCS which relies on a single round of range reliability assessment to guarantee the reliability of data while achieving lightweight and privacy preservation. Moreover, to fairly stimulate participants, constrain participants' malicious behavior, and improve the probability of high-quality data, the authors designed a quality-aware, reputation-based reward and penalty strategy to achieve dual incentives (including money incentives and reputation incentives) for participants. Furthermore, comprehensive theoretical analysis and experimental evaluation demonstrate that the proposed schemes are significantly superior to the existing schemes in several aspects, Wan, L., Liu, Z., Ma, Y., Cheng, Y., Wu, Y., Li, R., & Ma, J. (2024).

The authors proposed BLIND, an innovative open-source truth discovery system designed to improve the quality of information (QoI) through the use of privacy-preserving computation techniques in mobile crowdsensing scenarios. The uniqueness of BLIND lies in its ability to preserve user privacy by ensuring that none of the parties involved are able to identify the source of the information provided. The system uses homomorphic encryption to implement a novel privacy-preserving version of the well-known K-Means clustering algorithm, which directly groups encrypted user data. Outliers are then removed privately without revealing any useful information to the parties involved. We extensively evaluate the proposed system for both server-side and client-side scalability, as well as truth discovery accuracy, using a real-world dataset and a synthetic one to test the system under challenging conditions. Comparisons with four state-of-the-art approaches show that BLIND optimizes QoI by effectively mitigating the impact of four

different security attacks, with higher accuracy and lower communication overhead than its competitors, Agate, V., Ferraro, P., Re, G. L., & Das, S. K. (2024).

The authors proposed an independent task selection environment that defines actions, states, and rewards of RL to enable FedSense to achieve satisfactory task completion and data quality while preserving location privacy. Besides, FedSense applies an asynchronous FL aggregation algorithm that reduces participants' network stabilization and device computing ability requirements. Analysis proves that participants' location information does not leave the local device during the model training and task selection process, effectively avoiding privacy leakage. Simulation shows that compared with existing location-preservation crowdsensing mechanisms, FedSense achieves the highest task completion and sensing accuracy for dynamic tasks and participants, You, Z., Dong, X., Liu, X., Gao, S., Wang, Y., & Shen, Y. (2024).

The authors explored contemporary state-of-the-art issues related to privacy and security. It reviews 35 recent research published by high-quality sources and provides a topic-oriented survey for these efforts. It shows that only 16% of the papers evaluate their schemes through experiments on real smartphones, and Huawei is the most widely used mobile (45%). It shows an increasing trend in publications from 2017 till now. It highlights recent challenges faced the privacy in MCS and potential research directions for developing more advanced methods to optimise MCS, Alamri, B. H. S., Monowar, M. M., Alshehri, S., Zafar, M. H., & Khan, I. A. (2022).

The authors explored an integrated paradigm called "*hybrid sensing*" that harnesses both IoT-sensing and crowdsensing in a complementary manner. In hybrid sensing, users are incentivized to provide sensing data not covered by IoT sensors and provide crowd-sourced feedback to assist in calibrating IoT sensing. Their contributions will be rewarded with credits that can be redeemed to retrieve synthesized information from the hybrid system. In this article, the authors developed a hybrid sensing system that supports explicit user privacy—IoT sensors are obscured physically to prevent capturing private user data, and users interact with a crowdsensing server via a privacy-preserving protocol to preserve their anonymity. A key application of our system is smart parking, by which users can inquire and find the available parking spaces in outdoor parking lots, Zhu, H., Chau, S. C. K., Guarddin, G., & Liang, W. (2022).

A secure and timely MCS framework (PPFO: privacy preservation-oriented data freshness optimization) is put forward to achieve privacy preservation and data freshness optimization, that is, Aol minimization on the five-layer architecture. Particularly in the link and operation layers privacy preservation is realized by an encryption approach. Game theory methodology provides a solution to Aol optimization in the perception and transmission layers. Finally, the numerical results have shown the feasibility and effectiveness of the proposed framework, Yang, Y., Zhang, B., Guo, D., Wang, W., Li, X., & Hu, C. (2023).

The authors explored the geo-statistics of tourist areas. The proposed 'FedLens' brings tourists closer to their interests using augmented reality through the virtual guide. ArcGIS software maps a tourist area. 5G mobile crowdsensing helps to explore unknown tourist spots in real-time. 'FedLens' provides a privacy-preserving incentive mechanism to encourage reliable contributors to get better Quality of Information. The average global data aggregation time is approximately 12%. The contributor's collection time is 88% of the total processing time. The contributors use multifaceted intelligent federated computing to provide detailed geospatial information and promote sustainable ecotourism. Augmented reality-based virtual tourism ecosystem development is the ultimate goal of this work to attract more virtual tourists for a sustainable environment, De, D. (2024).

The authors proposed a mobile edge crowdsensing scheme based on Federated Learning (FL-MECS). The scheme aims to provide efficient sensing data analysis and effective privacy protection methods for crowdsensing systems. The approach utilizes local training and initial aggregation of the model at the edge node to avoid the risk of privacy leakage caused by the direct transmission of sensing data to the aggregation node. The evaluation shows that FLMECS can withstand collusion attempts and effectively preserves the model's local positive and negative sign parameter information. Experimental results on the MNIST dataset show that FL-MECS outperforms other alternatives in terms of model correctness, Chen, J., Gong, L., & Chen, J. (2024).

The authors proposed a privacy-preserving and reputation-based truth discovery framework named PRTD, which can generate the ground truths of sensing tasks with high accuracy while preserving privacy. Specifically, we first preserve sensing data privacy, weight privacy, and reputation value privacy by utilizing the Paillier algorithm and Pedersen commitment. Then, to verify whether the reputation values of mobile users are tampered with and select mobile users that satisfy the corresponding reputation requirements, we design a privacy-preserving reputation verification algorithm based on reputation commitment and zero-knowledge proof and propose a concept of reliability level to select mobile users. Finally, a general TD algorithm with a reliability level is presented to improve the accuracy of the ground truths of sensing tasks. Moreover, theoretical analysis and performance evaluation are conducted, and the evaluation results demonstrate that the PRTD framework outperforms the existing TD frameworks in several evaluation metrics in the synthetic

dataset and real-world dataset, Cheng, Y., Ma, J., Liu, Z., Li, Z., Wu, Y., Dong, C., & Li, R. (2023).

The authors proposed a privacy-preserving publish–subscribe-based decentralized framework for MCS systems named "Pub-SubMCS". The framework allows data sharing, where requesters can subscribe to an existing data request (task) if their requirements match. Otherwise, they can create a new task with specific requirements on considered parameters. Incorporating the publish-subscribe (pub–sub) service model in a decentralized MCS system saves system entities' sensing and computing resources and the cost of acquiring the data by the requesters. However, the pub–sub service model makes the curse of sensing issues more severe. Pub-SubMCS handles the curse of sensing issues by performing access control using smart contracts, which impose restrictions on data collectors (workers) to publish the data and identify and penalize the malicious workers early. To ensure data privacy and validation simultaneously over blockchain, we perform data transformation enabling the validation algorithm to run over transformed data and thus enhancing trust among the system entities. In particular, the authors use the normalization technique to transform data and the Pearson correlation coefficient measure to compare the similarity in the collected sensor data, Agrawal, A., Choudhary, S., Bhatia, A., & Tiwari, K. (2023).

The authors Aim at the trajectory privacy protection problem. This article proposes a differential location privacy-preserving mechanism based on trajectory obfuscation (LPMT). LPMT first extracts the stay points as the features of a trajectory based on the sliding window algorithm and then obfuscates each stay point to a target obfuscation subregion through the exponential mechanism, and finally performs the Laplace sampling in the target obfuscation subregion to obtain the obfuscated GPS points. Compared with the baseline mechanisms, LPMT can reduce data quality loss by more than 20% while providing the same level of obfuscation quality, which indicates that LPMT has the advantages of strong security and high quality of service, Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., & Zhang, J. (2022).

The authors proposed a secure user quality calculation (SQC) protocol to assess user quality instead of requiring user interaction in the case of unknown ground truth. Combinatorial multi-armed bandit (CMAB) based secure user recruitment (SUR) protocol effectively tackles the challenge of recruiting multiple users without prior knowledge and user interactivity while adhering to budget and time limitations. Theoretical analysis confirms lightweight overhead of the PPUR scheme and its multi-class data security. Experimental results show that SQC has superior performance in both computational cost and communication overhead. The regret indicator's findings demonstrate that SUR can effectively utilize budget and time to achieve optimal user recruitment decisions, Lin, R., Huang, Y., Zhang, Y., Bi, R., & Xiong, J. (2024).

Problem Statement

While MCS presents numerous advantages, it raises significant privacy concerns due to the nature of the data being collected, which often includes sensitive personal information. Key privacy challenges include:

User Identity Disclosure

Participants' identities can be inferred from the data they contribute, risking personal privacy.

Location Tracking

Continuous location data collection can lead to unwanted tracking and profiling of users.

Data Leakage

The aggregation of data can inadvertently expose sensitive information if not properly managed.

Unintended Data Sharing

Users may unknowingly share more information than intended, especially in applications that require data aggregation.

Future Research Direction

As ML models become more complex, the need for interpretability and explainability in privacy-preserving approaches is paramount. Future directions can include:

Interpretable ML for Privacy

Investigating methods to enhance the interpretability of privacy-preserving ML models allowing users to understand how their data is protected and how decisions are made.

User-Centric Explanations

Developing frameworks that provide personalized explanations of privacy-preserving mechanisms to users, enhancing trust and acceptance.

Healthcare Monitoring

Investigating the application of privacy-preserving ML in health-related MCS applications, such as monitoring chronic diseases, while ensuring patient confidentiality.

Environmental Sensing

Exploring the use of privacy-preserving techniques in environmental monitoring systems that collect sensitive data from individuals or communities.

References

Agate, V., Ferraro, P., Re, G. L., & Das, S. K. (2024). BLIND: A privacy preserving truth discovery system for mobile crowdsensing. *Journal of Network and Computer Applications*, 223, 103811.

Agrawal, A., Choudhary, S., Bhatia, A., & Tiwari, K. (2023). Pub-SubMCS: A privacy-preserving publish–subscribe and blockchain-based mobile crowdsensing framework. *Future Generation Computer Systems*, 146, 234-249.

Alamri, B. H. S., Monowar, M. M., Alshehri, S., Zafar, M. H., & Khan, I. A. (2022). Preserving privacy in mobile crowdsensing. *International Journal of Sensor Networks*, 40(4), 217-237.

Azhar, S., Chang, S., Liu, Y., Tao, Y., & Liu, G. (2022). Privacy-preserving and utility-aware participant selection for mobile crowd sensing. *Mobile Networks and Applications*, 1-13.

Boubiche, D. E., Imran, M., Maqsood, A., & Shoaib, M. (2019). Mobile crowd sensing–taxonomy, applications, challenges, and solutions. *Computers in Human Behavior*, 101, 352-370.

Chen, J., Gong, L., & Chen, J. (2024). Privacy Preserving Scheme in Mobile Edge Crowdsensing Based on Federated Learning. *International Journal of Network Security*, 26(1), 74-83.

Cheng, Y., Ma, J., Liu, Z., Li, Z., Wu, Y., Dong, C., & Li, R. (2023). A privacy-preserving and reputation-based truth discovery framework in mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, 20(6), 5293-5311.

De, D. (2024). FedLens: federated learning-based privacy-preserving mobile crowdsensing for virtual tourism. *Innovations in Systems and Software Engineering*, 20(2), 137-150.

Ding, Z., Huang, Y., Yuan, H., & Dong, H. (2020). Introduction to reinforcement learning. *Deep reinforcement learning: fundamentals, research and applications*, 47-123.

Dong, H., Dong, H., Ding, Z., Zhang, S., & Chang, T. (2020). Deep Reinforcement Learning. *Singapore*: Springer Singapore.

Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., & Zhang, J. (2022). Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing. *IEEE Transactions on Industrial Informatics*, 18(9), 6290-6299.

Kim, J. W., Edemacu, K., & Jang, B. (2022). Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. *Journal of Network and Computer Applications*, 200, 103315.

Lin, R., Huang, Y., Zhang, Y., Bi, R., & Xiong, J. (2024). Achieving lightweight, efficient, privacy-preserving user recruitment in mobile crowdsensing. *Journal of Information Security and Applications*, 85, 103854.

Liu, X., Zhou, S., Zhang, W., Dong, T., & Li, K. (2023). Privacy-preserving truth discovery for collaborative-cloud encryption in mobile crowdsensing. *IEEE Systems Journal*, 17(3), 4990-5001.

Liu, Y., Kong, L., & Chen, G. (2019). Data-oriented mobile crowdsensing: A comprehensive survey. *IEEE communications surveys & tutorials*, 21(3), 2849-2885.

Peng, F., Tang, S., Zhao, B., & Liu, Y. (2019, May). A privacy-preserving data aggregation of mobile crowdsensing based on local differential privacy. *In Proceedings of the ACM Turing Celebration Conference-China* (pp. 1-5).

Peng, T., Zhong, W., Wang, G., Zhang, S., Luo, E., & Wang, T. (2023). Spatiotemporal-aware privacy-preserving task matching in mobile crowdsensing. *IEEE Internet of Things Journal*.

Pius Owoh, N., & Mahinderjit Singh, M. (2020). SenseCrypt: a security framework for mobile crowd sensing applications. *Sensors*, 20(11), 3280.

Rahmani, A. M., Yousefpoor, E., Yousefpoor, M. S., Mehmood, Z., Haider, A., Hosseinzadeh, M., & Ali Naqvi, R. (2021). Machine learning (ML) in medicine: Review, applications, and challenges. *Mathematics*, 9(22), 2970.

Sultana, M. N., & Chang, K. (2020). ML Algorithm Performance to Classify MCS Schemes During UACN Link Adaptation. *IEEE Access*, 8, 226461-226483.

Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access*, 7, 65579-65615.

Verma, R., Nagar, V., & Mahapatra, S. (2021). Introduction to supervised learning. *Data Analytics in Bioinformatics: A Machine Learning Perspective*, 1-34.

Wan, L., Liu, Z., Ma, Y., Cheng, Y., Wu, Y., Li, R., & Ma, J. (2024). Lightweight and Privacy-Preserving Dual Incentives for Mobile Crowdsensing. *IEEE Transactions on Cloud Computing*.

Wang, J., Wang, Y., Zhao, G., & Zhao, Z. (2019). Location protection method for mobile crowd sensing based on local differential privacy preference. *Peer-to-Peer Networking and Applications*, 12, 1097-1109.

Wang, J., Yin, X., & Ning, J. (2021). Fine-Grained Task Access Control System for Mobile Crowdsensing. Security and Communication Networks, 2021(1), 6682456.

Wang, Y., Yan, Z., Feng, W., & Liu, S. (2020). Privacy protection in mobile crowd sensing: a survey. *World Wide Web*, 23(1), 421-452.

Yan, X., Ng, W. W., Zeng, B., Lin, C., Liu, Y., Lu, L., & Gao, Y. (2021). Verifiable, reliable, and privacy-preserving data aggregation in fog-assisted mobile crowdsensing. *IEEE Internet of Things Journal*, 8(18), 14127-14140.

Yan, X., Zeng, B., & Zhang, X. (2022). Privacy-preserving and customization-supported data aggregation in mobile crowdsensing. *IEEE Internet of Things Journal*, 9(20), 19868-19880.

Yang, Y., Zhang, B., Guo, D., Wang, W., Li, X., & Hu, C. (2023). PPFO: A Privacy Preservation-oriented Data Freshness Optimization Framework For Mobile Crowdsensing. *IEEE Communications Standards Magazine*, 7(4), 34-40.

Yi, X., Lam, K. Y., Bertino, E., & Rao, F. Y. (2019). Location privacy-preserving mobile crowd sensing with anonymous reputation. *In Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security,* Luxembourg, September 23–27, 2019, Proceedings, Part II 24 (pp. 387-411). Springer International Publishing.

You, Z., Dong, X., Liu, X., Gao, S., Wang, Y., & Shen, Y. (2024). Location Privacy Preservation Crowdsensing with Federated Reinforcement Learning. *IEEE Transactions on Dependable and Secure Computing*.

Zhang, C., Zhao, M., Zhu, L., Wu, T., & Liu, X. (2022). Enabling efficient and strong privacy-preserving truth discovery in mobile crowdsensing. *IEEE Transactions on Information Forensics and Security*, 17, 3569-3581.

Zhang, Y., Ying, Z., & Chen, C. P. (2022). Achieving privacy-preserving multitask allocation for mobile crowdsensing. *IEEE Internet of Things Journal*, 9(18), 16795-16806.

Zhao, B., Liu, X., Chen, W. N., & Deng, R. H. (2022). CrowdFL: Privacy-preserving mobile crowdsensing system via federated learning. *IEEE Transactions on Mobile Computing*, 22(8), 4607-4619.

Zhu, H., Chau, S. C. K., Guarddin, G., & Liang, W. (2022). Integrating IoT-sensing and crowdsensing with privacy: Privacy-preserving hybrid sensing for smart cities. *ACM Transactions on Internet of Things*, 3(4), 1-30.