A Differential Privacy Approach for Context-Aware Service Provisioning in Mobile Networks

Franc Pouhela*, Sogo Pierre Sanon* and Hans D. Schotten*†

*Intelligent Networks Research Group, German Research Center for Artificial Intelligence (DFKI GmbH), D-Kaiserslautern.
Email: {franc.pouhela | sogo_pierre.sanon | hans_dieter.schotten}@dfki.de
†Institute for Wireless Communication and Navigation, RPTU University of Kaiserslautern-Landau, D-67663 Kaiserslautern.
Email: {schotten}@rptu.de

***Abstract*—This paper proposes a Differential Privacy approach for adaptive service provisioning in mobile networks. With the increasing demand for mobile services and the ever changing network environment, network operators have to be able to dynamically adjust their service provisioning to meet changing user demands. However, this presents a challenge for preserving user privacy while collecting data to inform these decisions. The proposed approach uses Differential Privacy techniques to ensure that user privacy is protected while still allowing for accurate data collection and analysis. The approach also includes an adaptive mechanism for adjusting service provisioning based on the collected data, further improving the efficiency and effectiveness of mobile networks.**

***Index Terms*—Privacy, Differential Privacy, Context-Awareness, Mobile Network, 5G, 6G**

I. Introduction

Context Management (CoMa) has become one of the most desired features for next-generation mobile networks. With the advent of new wireless technologies such as 5G and 6G, the need for efficient context management is increasingly important.

A context-aware mobile network can leverage context information from multiple connected entities to better manage and coordinate the interactions between different devices, networks, and services, enabling efficient and effective utilization of network resources as well as opening a door for new business models and revenue streams for Mobile Network Operators (MNOs) and better user experience for consumers.

However, the most prominent argument against context awareness is the privacy of the users providing their real-time context information. The acquisition of private information, such as location data, browsing history, and personal preferences, can lead to the exposure of sensitive information that could be exploited for malicious purposes. Therefore, the collection, storage, and processing of private data must be done with extreme caution and with adequate safeguards to protect users' privacy and it is also critical to ensure that data acquisition and processing comply with relevant privacy laws and regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States.

Differential Privacy (DP) can help mitigate the limitations of collecting private data. DP is a mathematical technique that allows for the collection and analysis of private data while protecting the privacy of individuals by adding noise to the data.

One significant advantage of this technique is that it can provide a measurable guarantee of privacy protection. By adding noise to the data, it ensures that individual data points cannot be re-identified, even by an attacker with access to all other data in the dataset. This guarantee can increase users' trust in the network and its services, thereby mitigating the risks of reputational damage and loss of user engagement.

Another advantage of DP is that it can enable data sharing and collaboration without compromising privacy. By adding noise to the data, DP allows for the sharing of sensitive data between multiple parties while protecting the privacy of individuals. This can enable new forms of collaboration and research that were so far impossible due to privacy concerns.

DP can also address the ethical concerns regarding users' consent and transparency in data collection practices. By adding noise to the data, DP ensures that individual data points cannot be traced back to specific individuals, thereby ensuring anonymity and protecting users' privacy. Additionally, DP can enable users to control their data and revoke their consent to data collection at any time, thereby increasing transparency and empowering users.

This study explores how DP can be leveraged in mobile networks to provide adaptive service provisioning based on context data. The paper is structured as follows: Section II gives a brief overview of the related work on this topic. Section III provides a detailed description of the DP algorithm. Section IV presents a proposed context management architecture, including the context data acquisition and processing steps. Section V focuses on the implementation and integration aspects, while Section VI illustrates a variety of potential use cases. The paper concludes in Section VII with a summary of the contributions and suggestions for future work.

II. Related Work

As part of the Open6GHub project in Germany, a Context Management Architecture for Decoupled Acquisition and Distribution of Information in Next-Generation Mobile Networks was proposed in [1]. The architecture leverages a publish/subscribe messaging model to ensure decoupling between providers and consumers, addressing the network providers' need for context awareness in their networks.

A CoMa framework leveraging agent technology in 4G mobile networks is introduced in [2]. The focus is on enabling intelligent services that are context-aware, particularly in the context of secure handovers. [3] proposed the adoption of a reconfigurable context management system in wireless mesh networks. [4] addresses the limitations of traditional opportunistic routing by introducing a new protocol called Context-aware Opportunistic Routing and [5], [6] proposed a context-aware resource allocation system in distributed sensor networks and cellular wireless networks respectively. A context-aware security for 6G wireless using physical layer security is developed in [7]. This work focuses on context-aware service provisioning in mobile networks and proposes a private approach using DP techniques.

III. Differential Privacy

DP is a mathematical framework for ensuring the privacy of individuals in datasets. It can provide a strong guarantee of privacy by allowing data to be analyzed without revealing sensitive information about any individual in the dataset. One important application of DP in mobile networks is adaptive service provisioning, which involves dynamically adjusting the services provided to individual users based on their context and behavior. DP algorithms provably resist identification and reidentification attacks.

A. Different Concepts of Differential Privacy

There are four main formulations of the concept of DP, ε-DP [8] [9], (ε, δ)-DP [10], Renyi Differential Privacy (RDP) [11] and Gaussian Differential Privacy [12]. Each formulation provides varying levels of privacy protection and flexibility.

*1) **ε-Differential Privacy**:* A randomized algorithm $\mathcal{A}$ is ε-DP if, for any two neighboring datasets (datasets that differ in only one individual's data), D and D' and a set S the following is satisfied:

$$P[\mathcal{A}(D) \in S] \leq e^{\varepsilon} \times P[\mathcal{A}(D') \in S]. \tag{1}$$

This means that the probability of the algorithm outputting any particular result is at most e^{ε} times greater for one dataset than for the other. ε-DP is the most common variant of DP and ε is a privacy parameter that controls the level of privacy protection, with smaller values of ε providing stronger privacy guarantees. When ε is small, the presence or absence of any individual's data has a limited impact on the final query result. ε-DP can be achieved by any algorithm by applying the Laplace mechanism [8] or the exponential mechanism [13].

*2) **(ε, δ)-Differential Privacy**:* A more general and flexible variant of DP is (ε, δ)-DP. An algorithm $\mathcal{A}$ is (ε, δ)-DP if, for any two neighboring datasets, D and D' and a set S the following is satisfied:

$$P[\mathcal{A}(D) \in S] \leq e^{\varepsilon} \times P[\mathcal{A}(D') \in S] + \delta. \tag{2}$$

This means that the probability of the algorithm outputting any particular result is at most e^{ε} times greater for one dataset than for the other, except with probability δ. (ε, δ)-DP can be achieved through the application of Gaussian mechanism [10].

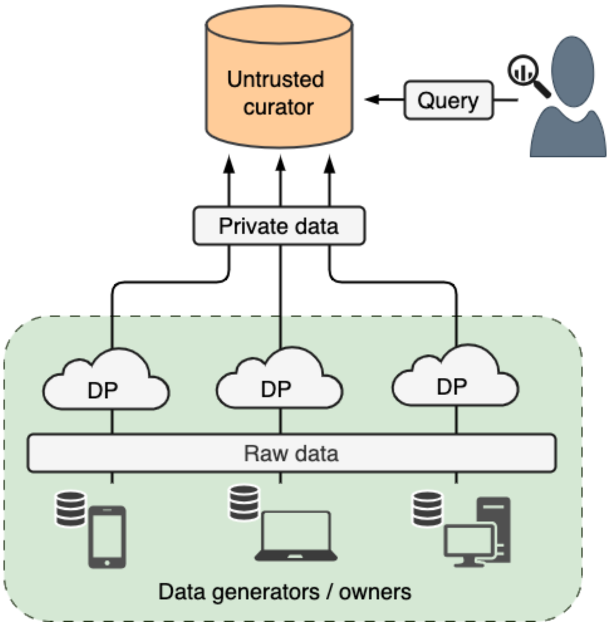

Figure 1. Differentially Private Data Query

*3) **Renyi Differential Privacy**:* RDP represents a versatile privacy paradigm that goes beyond the constraints of both ε-DP and (ε, δ)-DP. By introducing a continuum of privacy guarantees through the parameter α, RDP offers an unparalleled level of generality and flexibility in privacy protection. The parameter α in RDP enables the privacy level to be continuously adjusted, accommodating varying degrees of privacy requirements.

A randomized algorithm $\mathcal{A} : \mathcal{D} \rightarrow \mathcal{R}$ satisfies (α, ε)-RDP if, for any two neighboring data sets D and D' it holds that

$$D_{\alpha}(\mathcal{A}(D) \| \mathcal{A}(D')) \leq \varepsilon. \tag{3}$$

D_{α} is a form of distance function that measures the "distance" between $\mathcal{A}(D)$ and $\mathcal{A}(D')$. If $\mathcal{A}$ is (α, ε)-DP then

$$P[\mathcal{A}(D) \in S] \leq (e^{\varepsilon} \times P[\mathcal{A}(D') \in S])^{1-1/\alpha}. \tag{4}$$

In RDP the privacy loss is measured in terms of Renyi divergence [14] between the distributions of the output of neighboring datasets. RDP converges to ε-DP when α tends to infinity, and when α is set to 1, it corresponds to (ε, δ)-DP for some δ. For more on RDP and DP in general, see [11].

In addition to these privacy definitions, there is a less popular DP definition, Gaussian Differential Privacy [12] which works well in hypothesis testing and makes privacy guarantees easily interpretable.

B. General Approaches to Achieve DP and Applications

DP can be categorized into two types: Local Differential Privacy (LDP) [15] and Global Differential Privacy (Global Differential Privacy (GDP)) [16]. With LDP even if an adversary gains access to an individual's personal responses within the database, they are still unable to obtain information about the user's private data. In contrast, GDP represents a DP model that integrates a central aggregator with direct access to the raw data.

*1) **Local Differential Privacy**:* In LDP the data curator/central aggregator, the person who is aggregating the dataset, does not know the actual value, as users add noise to their own data before sharing and thus privacy is protected, Figure 1. They do not have to trust the data curator or the database owner. With LDP, since each user must add noise to their own data, the total noise is much larger and typically would need many more users to get useful results. Practical applications include:

- **RAPPOR**: Google uses LDP to collect data from users, such as the other running processes and Chrome home pages they visit. This data is used to improve the performance of Google products and services, without compromising the privacy of individual users [17].
- **Private Count Mean Sketch**: Apple uses LDP to collect emoji usage data, word usage, and other information from iPhone users (iOS keyboard). This data is used to improve the accuracy of predictive models, such as the keyboard's auto-correct feature, without compromising the privacy of individual users [18].
- **Privacy-preserving aggregation of personal health data streams**: [19] develops a novel mechanism for privacy-preserving collection of personal health data streams. The data is collected at fixed intervals, and LDP is used to protect the privacy of individual users. This allows researchers to study large datasets of personal health data without compromising the privacy of the individuals involved.

*2) **Global Differential Privacy**:* In GDP the noise is added to the query outputs of a database, specifically at the end of the process before sharing the results with a third party. A trustworthy data curator carries out noise addition and has access to the original raw data in the database. The primary advantage of this approach is that it maintains accuracy while requiring minimal noise addition, even with a low privacy parameter ε. However, a significant challenge lies in establishing trust between users and the data curator and this is especially difficult. Additionally, the global model centralizes all data, raising the risk of breaches if the aggregator is hacked and data is leaked. It's important to note that if the database owner, who also functions as the data curator, can be trusted, the primary distinction between local and global DP is that the latter yields more accurate results with equivalent privacy protection. GDP was adopted in the Census Bureau Adopts Cutting Edge Privacy Protections for 2020 Census [20].

DP is applicable in many domains including data anonymization, and secure queries but also Machine Learning (ML). In ML, especially Deep Learning, there are two main techniques to achieve DP, Differential Privacy Stochastic Gradient Descent (DP-Stochastic Gradient Descent (SGD)) and Private Aggregation of Teacher Ensembles (PATE).

C. *Differential Privacy Stochastic Gradient Descent*

DP-SGD combines the principles of DP with the popular optimization algorithm, SGD [21]. It enables privacy-preserving learning by adding noise into the gradient updates during the training process. With the noise addition, DP-SGD ensures that the updates to the model's parameters are sufficiently random. This protects the privacy of individual data points while still allowing effective model training. DP-SGD satisfies (ε, δ)-DP; it ensures that an individual data point's presence in the training dataset will not significantly impact the model's output or final decision.

D. *Private Aggregation of Teacher Ensembles*

PATE is another differentially private ML framework [22]. It works by first training an ensemble of teacher models on disjoint subsets of the sensitive data. Each teacher model is trained independently, so no individual's data is shared with any other individual. The knowledge of teacher ensembles is transferred to a student model by letting the teachers vote for the label of each record from an unlabeled public dataset. The voting process is done in a way that adds noise to the teacher's predictions, making it difficult to learn anything about the individual data points that were used to train the teacher models. The amount of noise that is added to the teacher predictions is controlled by the privacy budget ε, it is ε-DP. The larger the privacy budget, the less noise is added, and the more accurate the student model will be. However, a larger privacy budget also means that it is less likely that the student model will be differentially private.

DP emerges as a promising technique in many domains. It can be useful in addressing privacy concerns and establishing a balance between context management and privacy preservation in mobile wireless communication.

IV. Context Management Framework

Many consider context-awareness in mobile networks to be a cornerstone feature that can provide centralized user and device data handling, ensuring optimized resource allocation, and delivering personalized experiences through insights into user behavior, network conditions, and application needs. This feature enables seamless mobility between network technologies, enhances security, and enables dynamic adaptation based on real-time context. Such an intelligent framework empowers efficient service provisioning, network automation, and scalability, making it a key element in shaping the future of mobile connectivity and services.

A. *Context Management Process*

Following are the different phases involved in a Context Management System (CoMaS):

1) **Context Acquisition**: It involves gathering context data from diverse sources, such as devices, apps, and users, using sensors, probes, or any existing techniques.
2) **Context Storage**: Involves centralizing and structuring context info in a repository using database systems and indexing technologies, while defining data models and relationships.
3) **Context Processing**: Compasses analyzing context information for valuable insights using ML, data mining, and analytical methods, facilitating meaningful results generation.

4) **Context Dissemination**: It involves the exchange of context data with relevant systems using protocols, Application Programming Interfaces (APIs), and communication methods to accurately deliver data to intended recipients.
5) **Context Utilization**: This phase involves the use of context information to support various applications and services within or outside the network.
6) **Context Evaluation**: Compasses appraising the quality of the CoMaS process and context data. This phase utilizes metrics, benchmarks, and issue resolution to gauge CoMa system performance and effectiveness.
7) **Context Maintenance**: Continuous maintenance and updates to the CoMaS system. This includes capturing, storing, processing, and sharing new context data, while also retiring outdated or irrelevant context information.

B. Context Data Model

Context data can be classified into four major categories:

- **Device Context**: refers to information about the characteristics and capabilities of a particular device, such as its hardware and software specifications, connectivity status, and location.
- **Network Context**: refers to information about the characteristics and state of the network, including its topology, bandwidth, and performance.
- **User Context**: refers to information about the preferences, habits, and characteristics of the user, such as their location, language, and personal preferences.
- **Application Context**: refers to information about the specific application or service being used, such as the type of data being transmitted and the requirements of the application.

C. Context Management Architecture

The diagram in Figure 2 represents a high-level architecture of a CoMaS. The architecture facilitates context information acquisition and delivery between entities via a publish/subscribe communication model. This communication model is highly scalable and provides a decoupled mechanism for data distribution [23]. The broker enables context providers to publish information, while consumers subscribe to relevant topics. Additionally, consumers can issue queries to the broker to retrieve specific context information.

The Context Providers represent diverse sources of data such as sensors, mobile devices, applications, or even networks. Context Consumers on the other hand represent applications or systems reliant on context, subscribing to the relevant information they require. This architecture enables third-party consumers to query context data for specific use cases.

By utilizing state-of-the-art reasoning and machine learning techniques, the system can extract additional knowledge from the raw data collected from different entities to provide valuable input to the control system that makes all major decisions, such as resource allocation and system shutdown.

V. Implementation and Integration

While a CoMaS can offer numerous benefits for network optimization and service personalization, it raises as mentioned in Section I legitimate concerns about user data privacy and security. As users contribute their context data ranging from location and behavior patterns to personal preferences, there's a potential for misuse, unauthorized access, or breaches. This accumulation of sensitive information in a centralized system can lead to concerns about surveillance, data leakage, and unauthorized profiling. Establishing a balance between reaping the advantages of context-driven networks and safeguarding user privacy becomes paramount, necessitating robust measures like data anonymization, user consent frameworks, stringent security protocols, and compliance with privacy regulations to ensure that the benefits of CoMa do not come at the expense of individual privacy and trust.

We see DP as a viable solution to alleviate the privacy restrictions associated with a CoMaS. DP can be applied to various stages of CoMaS to protect user privacy while maintaining the utility of the collected data. Here are specific areas within CoMa where DP can be applied:

- **Context Acquisition:** Local DP (Figure 3) can be applied at the point of data collection on mobile devices. It can be used to protect sensitive information such as location updates, user movement patterns, network status, and user preferences before sending data to the network.
- **Context Processing:** Global DP (Figure 4) can be used when processing queries related. Practical DP for SQL Queries like FLEX developed at Uber [24], [25] can be used by the Broker to maintain the privacy of the response even when providing context-related answers to Context Consumers.
- **Context Utilization:** DP can be integrated when managing and analyzing user profiles and preferences. Techniques like DP-SGD and PATE [21], [22] can be used to protect individual preferences and behavior patterns while still allowing for personalized services. In addition, DP can be used to ensure fair resource allocation based on aggregated network conditions and user requirements.

In essence, DP can be applied at multiple stages of CoMa where sensitive user data is collected, processed, aggregated, or queried. The aim is to ensure that even in the presence of powerful adversaries, individual user information remains statistically indistinguishable and the privacy of users is preserved. This can help communications service providers comply with privacy laws and regulations such as GDPR.

VI. Use Cases and Applications

Context-aware service provisioning in mobile networks offers a wide array of practical use cases that enhance the user experience, optimize resource allocation, and improve the efficiency of network operations. Here are some notable use cases:

- **Location-Based Services**: Context-aware provisioning enables precise location tracking of mobile users. This information is invaluable for delivering location-based services such as personalized advertising, local business recommendations, and geofencing for security or marketing purposes.

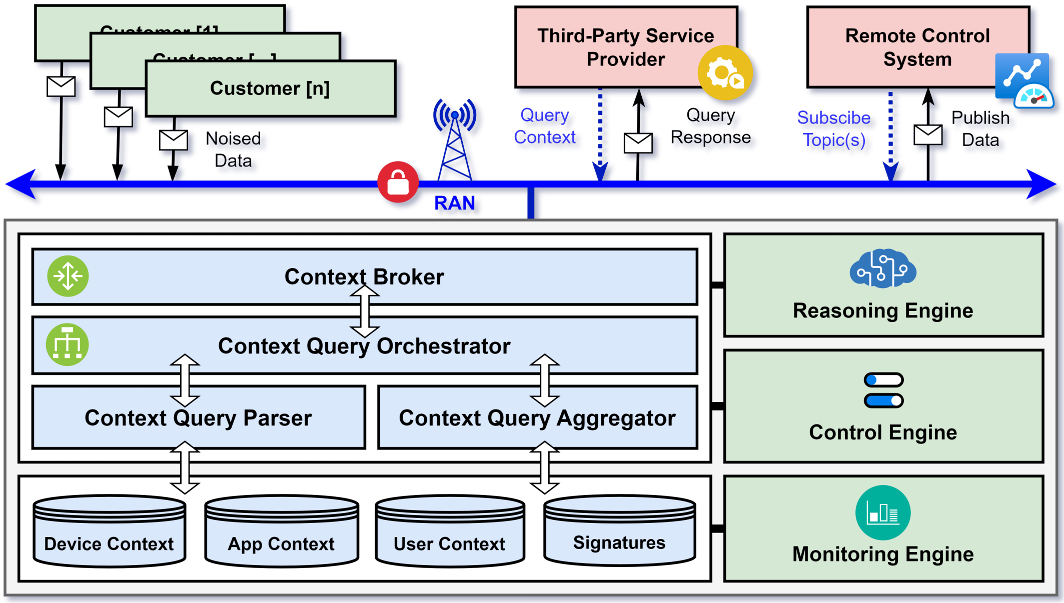

Figure 2. Context Management Architecture

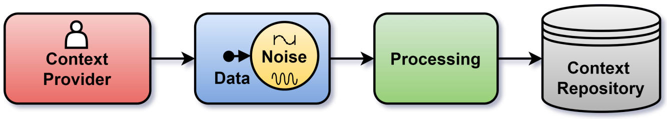

Figure 3. Local Deferential Privacy

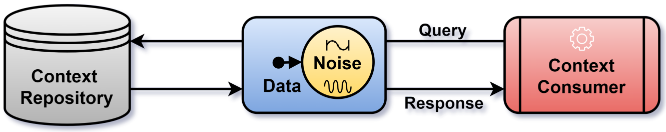

Figure 4. Global Deferential Privacy

Differential privacy enables the generation of context-based heatmaps by adding carefully calibrated noise to the aggregated location and sensor data, ensuring that individual users' precise information remains private. This noise obscures any sensitive details, making it statistically challenging to pinpoint an individual's exact data. As a result, the heatmaps reveal valuable patterns and trends in user behavior or environmental conditions while guaranteeing strong privacy protection, aligning with privacy regulations and user trust.

- **Quality of Service Optimization**: Context-awareness allows mobile networks to adapt their service quality based on factors like network congestion, device capabilities, and user preferences. This ensures that critical applications like video streaming or online gaming receive the necessary bandwidth and low latency while conserving resources for less demanding tasks.
- **Context-Aware Security**: Mobile networks can leverage contextual information like device behavior, location anomalies, and user activity patterns to detect and respond to security threats more effectively. For example, unusual login attempts from an unfamiliar location may trigger additional authentication steps.
- **Energy-Efficient Communication**: Context-aware service provisioning can optimize energy consumption in mobile devices. By considering factors like battery status and device usage patterns, the network can schedule data transfers during periods of lower power consumption, extending device battery life.
- **Seamless Handovers**: Mobile users often move between different access points (e.g., WiFi, cellular) while in motion. Context-aware provisioning ensures smooth handovers by considering factors like signal strength, network availability, and user preferences to minimize service disruption during transitions.
- **Emergency Services**: During emergency situations, context-aware provisioning can prioritize emergency calls and data traffic, ensuring that critical communication services are available and responsive when needed most.
- **Predictive Maintenance**: In the Internet of Things (IoT) domain, context-aware service provisioning can be used to monitor and maintain connected devices more effectively. By analyzing contextual data from sensors, network operators can predict equipment failures and schedule maintenance proactively.
- **Traffic Management and Congestion Control**: Context-aware provisioning assists in traffic management by dynamically rerouting traffic during network congestion or accidents. It considers real-time traffic conditions, user preferences, and alternative routes to optimize traffic flow.
- **Personalized Recommendations**: Utilizing user behavior, location, and preferences, context-aware services can deliver

personalized content recommendations. This can apply to content streaming, news, shopping, or even suggesting nearby points of interest.

- **Smart Transportation**: Context-aware provisioning plays a crucial role in intelligent transportation systems. It enables real-time traffic updates, route optimization, and public transportation information dissemination, enhancing the overall commuting experience.
- **Healthcare and Remote Monitoring**: In healthcare, context-aware service provisioning supports remote patient monitoring. Wearable devices and sensors collect patient data, which is analyzed in real-time to provide medical professionals with relevant information and early warning signs.
- **Smart Cities**: Context-aware services contribute to the development of smart cities by optimizing resource utilization, traffic flow, energy consumption, and public safety. Examples include smart street lighting, waste management, and environmental monitoring.

In all these use cases and applications, techniques like DP are essential in preserving privacy.

VII. Conclusion and future work

In conclusion, this paper introduces a novel approach centered on DP for the dynamic adaptation of service provisioning in mobile networks. As the demand for mobile services continues to surge, and network conditions evolve constantly, network operators face the critical task of flexibly aligning their service offerings with changing user needs. However, this imperative to adjust services presents a challenge in terms of safeguarding user privacy while collecting essential data for informed decision-making. The proposed approach addresses this challenge by leveraging DP techniques, ensuring the preservation of user privacy without compromising the accuracy of data collection and analysis. This dual-pronged strategy not only enhances the efficiency and effectiveness of mobile networks but also reinforces the commitment to protecting user privacy in an era of rapidly evolving mobile services and it represents a logical progression toward creating a user-friendly and participatory environment.

Acknowledgment

The authors acknowledge the financial support by the German *Federal Ministry for Education and Research (BMBF)* within the project »Open6GHub« {16KISK003K}, »AI-NET PROTECT« {16KIS1283} and »ALPAKA« {16KIS1841K}.

References

[1] F. Pouhela, D. Krummacker, and H. D. Schotten, "Towards 6G Networks," in *A Context Management Architecture for Decoupled Acquisition and Distribution of Information in Next-Generation Mobile Networks*, ser. ITG, vol. 157, VDE. IEEE, 5 2023.

[2] M. Lee and S. Park, "A secure context management for qos-aware vertical handovers in 4g networks," in *IFIP International Conference on Communications and Multimedia Security*. Springer, 2005, pp. 220–229.

[3] P. Hu, M. Portmann, R. Robinson, and J. Indulska, "Context-aware routing in wireless mesh networks," in *Proceedings of the 2nd ACM international conference on Context-awareness for self-managing systems*, 2008, pp. 16–23.

[4] Z. Zhao, D. Rosário, T. Braun, and E. Cerqueira, "Context-aware opportunistic routing in mobile ad-hoc networks incorporating node mobility," in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, 2014, pp. 2138–2143.

[5] L. B. Bhajantri, N. Nalini, and S. Gangadharaiah, "Context aware resource allocation in distributed sensor networks," *International Journal of Wireless & Mobile Networks*, vol. 4, no. 2, p. 35, 2012.

[6] M. Proebster, M. Kaschub, T. Werthmann, and S. Valentin, "Context-aware resource allocation for cellular wireless networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, pp. 1–19, 2012.

[7] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6g wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, 2022.

[8] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*. Springer, 2006, pp. 265–284.

[9] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*. Springer, 2006, pp. 1–12.

[10] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Advances in Cryptology-EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28-June 1, 2006. Proceedings 25*. Springer, 2006, pp. 486–503.

[11] I. Mironov, "Rényi differential privacy," in *2017 IEEE 30th computer security foundations symposium (CSF)*. IEEE, 2017, pp. 263–275.

[12] J. Dong, A. Roth, and W. J. Su, "Gaussian differential privacy," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 84, no. 1, pp. 3–37, 2022.

[13] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE, 2007, pp. 94–103.

[14] T. Van Erven and P. Harremos, "Rényi divergence and kullback-leibler divergence," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3797–3820, 2014.

[15] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" *SIAM Journal on Computing*, vol. 40, no. 3, pp. 793–826, 2011.

[16] H. Wang, Q. Zhao, Q. Wu, S. Chopra, A. Khaitan, and H. Wang, "Global and local differential privacy for collaborative bandits," in *Proceedings of the 14th ACM Conference on Recommender Systems*, 2020, pp. 150–159.

[17] Úlfar Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 21st ACM Conference on Computer and Communications Security*, Scottsdale, Arizona, 2014. [Online]. Available: https://arxiv.org/abs/1407.6981

[18] "Learning with privacy at scale differential," 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:43986173

[19] J. W. Kim, B. Jang, and H. Yoo, "Privacy-preserving aggregation of personal health data streams," *PLOS ONE*, vol. 13, no. 11, pp. 1–15, 11 2018. [Online]. Available: https://doi.org/10.1371/journal.pone.0207639

[20] R. Jarmin, "Census bureau adopts cutting edge privacy protections for 2020 census," *Director's Blog*, vol. 15, 2019.

[21] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[22] N. Papernot, M. Abadi, U. Erlingsson, I. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," *arXiv preprint arXiv:1610.05755*, 2016.

[23] F. Pouhela, D. Krummacker, and H. D. Schotten, "Wireless Communications for Industry 4.0," in *A Context Management Architecture for Decoupled Acquisition and Distribution of Information in Next-Generation Mobile Networks*. IEEE, 7 2023.

[24] J. Near, "Differential privacy at scale: Uber and berkeley collaboration," in *Enigma 2018 (Enigma 2018)*, 2018.

[25] N. Johnson, J. P. Near, and D. Song, "Towards practical differential privacy for sql queries," *Proceedings of the VLDB Endowment*, vol. 11, no. 5, pp. 526–539, 2018.