Implementation of Extended Differential Privacy for Electric Vehicles Using the Novel Filtering Approach

Mohsin Ali and Farhan Ali
Swinburne University of Technology, Melbourne, Australia

mohsinali45853@gmail.com
farhanali980315@gmail.com

Abstract: As electric vehicles (EVs) become more integrated into intelligent transportation systems, vast amounts of personal and operational data, such as location, driving patterns, and energy consumption, are continuously collected. Ensuring privacy for this sensitive data is critical to prevent tracking, profiling, and unauthorised access. This paper presents the implementation of event-wise differential privacy (DP) to safeguard individual data points in EV ecosystems, focusing on protecting event-level information like GPS updates and charging events. By utilizing the Laplace mechanism, noise is added to each event to guarantee privacy without compromising overall data utility. Additionally, we introduce a Kalman filter to mitigate the impact of noise, improving the accuracy of post-processed data while preserving privacy. The proposed framework demonstrates how event-wise DP can protect user information while still enabling accurate vehicle operations and analytics. Our approach highlights the balance between privacy and functionality, offering a scalable solution to enhance data protection in future smart mobility infrastructures. This research lays the groundwork for further advancements in privacy-preserving technologies within the EV sector, contributing to safer and more secure data-driven systems. To further alleviate the error in the utility of dataset by mitigating the noisy data generated through event-wise differential privacy, we integrate a Kalman filter into our framework. The Kalman filter is a unique and efficient tool for truncating the noise by correct prediction of the mechanism over time. In this research, it helps mitigate the impact of Laplace noise introduced for privacy preservation, ensuring smooth and comparatively accurate data while maintaining user privacy. In the last section of this paper the comparison of results would be provided before and after the implementation of Event-Wise Differential Privacy and the results obtained by the Kalman Filter for improving the utility keeping a trade-off between error and the usefulness of the dataset.

Keywords: Differential privacy, Event wise privacy, Kalman filter, Laplace mechanism, Electric vehicle, GPS, Dataset, Noise

1. Introduction

Differential privacy (DP) functions by the introduction of intelligently controlled noise injected into the dataset, typically Laplace noise to provide the masking to individual's data. This addition of noise is done in such a way that the results obtained from statistics remain useful and accurate by the aggregator. However, it becomes difficult for the adversary to predict the sensitive information (Bunsen 2018). The big challenge here was how to actually apply the extended-DP in order to provide protection to the dataset with optimum noise so that too much noise would not mask the insights in the dataset. Thus, drastically decreasing the risk of data misuse (Shabtai et al. 2014).

It is a case of electrical vehicles in which we are dealing with the critical dataset containing user information on a real-time location of the user, driving behaviour and nature, battery status, payment details, and charging patterns (Chen et al. 2024) (Morrissey, Weldon, and O'Mahony 2016). For example, it can continuously monitor the location of the user when the adversary can gain access to it, or predict the trajectory by the existing information for a profiling attack (Morrissey, Weldon, and O'Mahony 2016). It can also deploy energy consumption data to reveal the daily routine or lifestyle of the user. Protection of such information that could reveal through EVs is crucial, therefore, in tackling to avoid any potential misuse of these data (Langer et al. 2013).

Concurrency can, therefore, be a likely solution for event-based differential privacy, showcasing that it provides a finer granularity towards answering the question of privacy in such setups. Adding noise to every respective individual events instead of on a whole dataset, event-wise concurrent DP provides the privacy more rigorously. This fine-toned application of DP is particularly well-suited for EVs, where every single event is generated continuously and should be protected in real-time scenarios (Chen et al. 2017).

Added noise in the form of place can bring a lot of challenges related to data utility and usefulness of data. Further, this added noise may degrade the accuracy of some important EV functions such as navigation, energy optimization, and diagnostics since it is hard to balance privacy and utility of the shared dataset. That is where the Kalman filter plays an important role.

The Kalman filter, developed initially to use in engineering and control systems for reducing the errors, is a mechanism to predict the state of a dynamic system from noisy observations. It predicts the next state based

on its previous states while correcting measurement noise in real time. This predict-update-dual process of prediction allows the Kalman filter to smooth out noise and arrive at better estimations even when there is some uncertainty. The Kalman filter can be applied to a privacy-preserving system for reversing negative distortion caused by adding noise for differential privacy, hence improving utility while allowing effective privacy guarantees (Wang et al. 2019).

In an electric vehicle, where data accuracy is key to many different operations, the integration of Kalman filter with event-wise differential privacy therefore confers a few remarkable advantages over conventional DP. This is done by the application of a Kalman filter for reducing the distortion caused by the Laplace noise used in DP and, therefore, giving more useful and efficient results regarding route planning, scheduling, and maintenance, demand side management, battery management, and system advancements. The practical applications are particularly interested in this aspect because both the performance of EVs and users are dependent on the proper input of data. The combination of differential privacy and the Kalman filter strikes an optimal balance where privacy is guaranteed with no loss of critical, high-quality data needed by the vehicle functions.

In this paper, we explore the approach towards event-wise differential privacy in electric vehicles and how the integration of the Kalman filter will drastically mollify the error in the data to enhance the utility of the distorted data (Langer et al. 2013). We begin by discussing the basics of differential privacy and its importance in protecting user data in the context of EVs (Zhang et al. 2021). Next, we outline the basics of a Kalman filter, detailing the usefulness of the approach for improving the accuracy of noisy data points via filtration. The objective set forth here is to use this approach to demonstrate how mechanisms related to preserving privacy can effectively be embedded in smart transport systems without compromising their effectiveness (Quinn and Malgieri 2021).

2. Literature Review

A number of researchers strived to come up with a model to defend these sensitive parameters of electric vehicles (EV_s) connected to charging station (CS_s), deploying the appropriate models based on differential privacy. Some of them deployed user-level Local Differential Privacy protecting the sensitive information at binary level (Islam et al. 2023). This study has some short coming, it was not considering the dynamic nature of Electrical vehicles changing erratically. Moreover, this study was implemented on the binary system hence, significant work is considered to be done to deal with the multiclass divisions.

Another study (Qiu et al. 2021a) has contributed to a similar domain protecting privacy using the Event Wise Approach by making the events in the form of sliding windows or events and then applying the differential privacy overlooking the value of error in the results which was excessively high causing a huge deviation from the raw data. Then these existing studies were taken further by (Chen et al. 2024) focusing on the multiclass structure of data by proposing the interval tree structure embracing the heteroscedastic noise strategy based on differential privacy. However, this approach was only for the statistical data. Literature (Kellaris et al. 2014) proposed a technique combining the user-level differential Privacy and Event Wise Privacy on an infinite stream protecting the user's data but in different domains not in the vehicular domain. Another literature (Yong et al. 2018) propounded an approach which was using ω- Event Differential privacy. This approach did not taking account of error at each sampling point.

The work (Chen et al. 2017) proposed the PeGasus technique which perturbates a group or event resulting in drastically significant noise deteriorating the quality of utility. This problem was solved by another study (Ren, Zhang, and Zhang 2019) by the introduction of Kalman filter which resulted error in noise added in the acceptable window. Literature (Wang et al. 2016) deployed ResueDP approach which aimed to protect the privacy of user using the Event Wise Differential Privacy in different domain. This approach was not dealing with and considering the data dynamically. Hence, all aforementioned research gaps would be mitigated in this proposed approach. Numerous other researchers and engineers have contributed to resolving this Electric Vehicle privacy issue with their different approaches. To begin with, a researcher in the article (Kumar et al. 2020) focused on the privacy prevention framework based on the concept of market matching and cryptography. In this mentioned approach the system delves for the most suitable charging point while giving the vehicle security and privacy by cryptography. This technique is often referred to as the most efficient in terms of computations, more specifically the researcher focused on the verification (Sign) and encryption in Electric Vehicles parallelly while charging process. This method was perceived to be efficient in terms of cost involved in communication, calculations involved (less iterative) and latency rate. Likewise, When the user is locating the nearest charging station, while processing transactions, charging the vehicle from the grid and performing the vehicle-assisted charging process it could become vulnerable to any malicious threat.

Therefore, this work (Unterwger et al. 2021) studied the privacy of electric vehicles and aimed to provide a secure and built-in payment system using the unique protocol in the competitive environment using a blockchain strategy. Similarly, blockchain strategies were further extended by introducing the five privacy-preventing techniques such as anonymity, differential privacy, private contract, encrypting the data, and mixing (Hassan et al. 2019). This study was done with the objective of laying the basic foundation related to these five privacy-preventing techniques. The researcher discussed certain limitations that need to be addressed before implementing this research approach in block-chain and systems based on IoT such as complex power networks, electric vehicles and small portable devices. Moreover, privacy preservation by differential approach was also studied which deals with the introduction of a Laplace signal in the form of noise and then combines this signal with the public information (Kato et al. 2021). Resultantly, this approach was tested for the random mechanism of allocation, and the results related to data collection explicitly supported the successful implementation of this strategy.

2.1 Problem Definition

In this research, we have an open question of how we can tackle the above privacy issue in Electrical Vehicles.

- To elaborate, How can event-wise differential privacy be effectively implemented in the context of electric vehicle (EV) data systems to provide protection against adversary for sensitive user information, while maintaining a good trade-off between data utility and error through the application of a Kalman filter to mitigate the impact of privacy-preserving noise?
- Specifically, how can the balance between privacy (using differential privacy) and accuracy (using the Kalman filter) be achieved in real-time scenario electric vehicle applications such as navigation, energy management, and diagnostics, where both data protection and precision are critical?

2.2 Our Contribution

The major contribution to this research has been listed below.

- This research aimed to tackle the privacy issues as discussed in the literature and the introduction of this work.
- We have proposed an intelligent approach in which we are implementing the extending differential privacy on the dynamic dataset generated in the charging station.
- We have preserved the private parameters of the electrical vehicle and charging station.
- We have proposed the filtration techniques termed as Kalman Filtration to mitigate the error and the noise to make the data more useful and applicable.

3. Methodology

3.1 System Algorithm and Architecture

In this section, we will highlight the proposed approach and the algorithm used in the approach. In order to validate the event-wise Differential Privacy model, this part implements our proposed privacy definition under various privacy budgets (ϵ) privacy budgets and offers a series of experimental results on our real-time datasets containing the sensitive and non-sensitive information of electric vehicles and charging stations.

In the system architecture given above it could be seen the operation of our approach chronologically. Firstly, the dataset containing the sensitive and non-sensitive information of the electrical vehicle and charging stations across the USA has been obtained. This dataset has approximately 62250 number of electric vehicles in total. Then we real-time time stamps *t,t1,t2,……tn* are given to these entries.

After making the time stamps we have created the groups of events *E1, E2, E3, …..En* intelligently based on our requirement and to perturb the whole event. After formulation of these events, the Laplace noise is added into the system, this is the random noise with a certain degree of sensitivity. And at this stage, we have high values of Absolute error (AE) and Mean Absolute Error (MEA), now this noisy event will undergo the Kalman filtration technique to publish the data with minimum error at each respective event of the electric vehicle and the charging station.

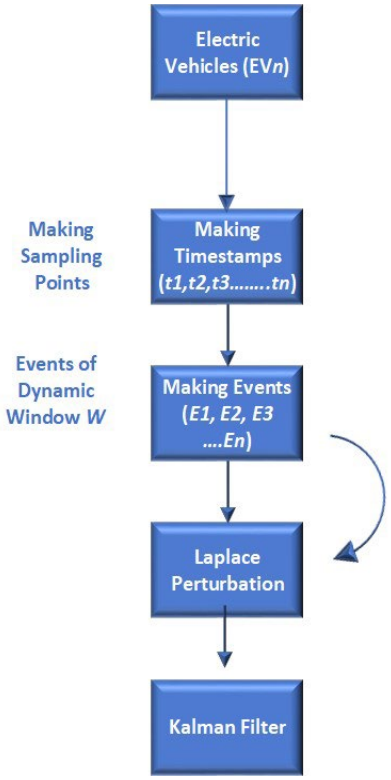

Figure 1: Proposed Architect of the System Model

3.2 System Model

In this research, we have proposed a model based on extended DP which is Event-wise Differential Privacy (EDP) in electric automobiles being charged at the charging station. A fleet of electric vehicles (EV_s) makes up the system, and these cars provide their operational real-time data to a central server after a certain interval for a variety of analytics, Battery information, milage, kilometres driven, payment methods, personal information, including predictive maintenance, energy usage monitoring, and traffic management.

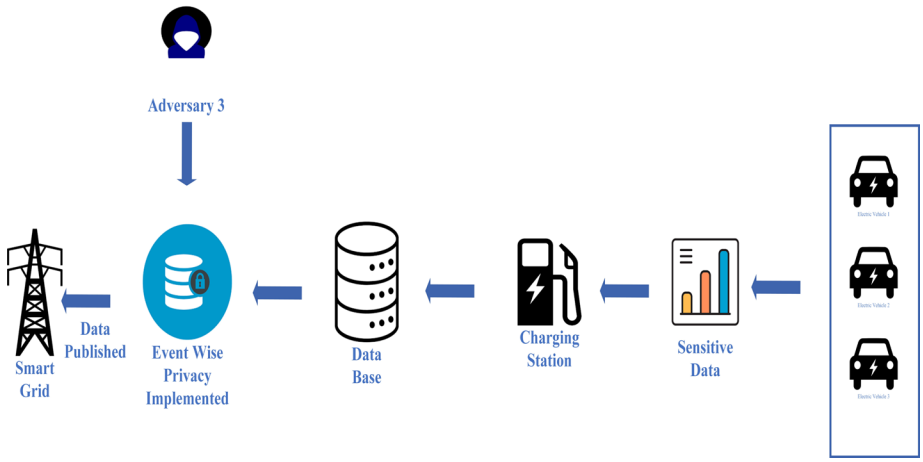

Figure 2: Proposed System Model

Every electric car in the fleet has a data gathering device installed that gathers the data on things like location, entry and exit time of vehicle, payment method, electrical range, vehicle ID, speed, battery status, and energy usage. Each successive discrete event in this specific time-stamped *(T)* data set represents a significant operation state of charging or activity of the charging station and vehicle. These discrete events are then perturbed to the data before getting published.

4. Experimental Evaluation

4.1 About Dataset

The dataset used in this research is a real-time dataset for all the Electric Vehicles connected across the USA for charging. This dataset comprises of 52200 rows or entries or vehicles and the 15 columns that contain the information in regard to that specific individual/vehicle such as the model, make, year, charging station, registration, entry and exit time of the vehicle, and the payment details of users.

4.2 Evaluation Metrics

This presented research is evaluated on the basis of absolute error for all the event and the Mean absolute error (MAE). In this subsection, we will hightlight the definition of these two evaluation metrics.

- Absolute error (AE)
- Mean Absolute error (MAE)

4.2.1 Absolute error

The above term refers to the estimation of possible difference between the actual and true value of the dataset. The expression for this term has been given below:

$$\text{Absolute Error} = |\text{Measured Value} - \text{True Value}|$$

4.2.2 Mean absolute error

Mean absolute Error is used in the measurement of the average value of error in a dataset having the predictor or noisy value. In our case, the predicted value is the random noise added in the dataset to obscure the original identifiers of the EV users.

The mean Absolute error has been given in the expression below:

$$MAE = (1/n) \sum |z^i - z'^i|$$

In the above expression:

- n is the total number of data points depending on the number of events formed
- z^i is the true value of the dataset or the original value of the attributes
- z'^i is the noisy value of the dataset after injecting the noise in our system
- The difference between noisy and the true value is the absolute error as discussed previously.

This means absolute error play an important role in reflecting the accuracy of the utility in our dataset.

4.2.3 Significance of mean absolute error

Mean Absolute error is useful due to following rationales in comparison to other error-finding techniques.

- MAE is very convenient and easy to understand in relation to other techniques, it does not involve the tedious transformations.
- In MAE there is no magnification of errors unlike mean squared error (MSE).
- Since it does not play its part in squaring the error, hence it is a more robust metric.
- MAE drastically mitigates the median errors.
- This MAE have the tendency to be applied to different datasets regardless of the parameters.
- We can make the direct comparison using this approach in comparison to other error finding approach.

5. Results

All the experimentation has been done using the Lenovo ThinkPad Core i7(855OU) CPU @ 1.80GHz 8th Generation. The Results obtained from our technique were efficient and showcased the superiority of our approach over other unconventional approaches like traditional differential privacy and Local differential privacy. The effectiveness of our model has been boosted by deploying the filtration approach termed as Kalman Filter. Moreover, in other methods discussed in the literature review, part had a huge error. This section will show the results of our approach before and after implementing the Kalman filter approach and it will give the comparison between other technique such as Pegasus and Resue DP approach.

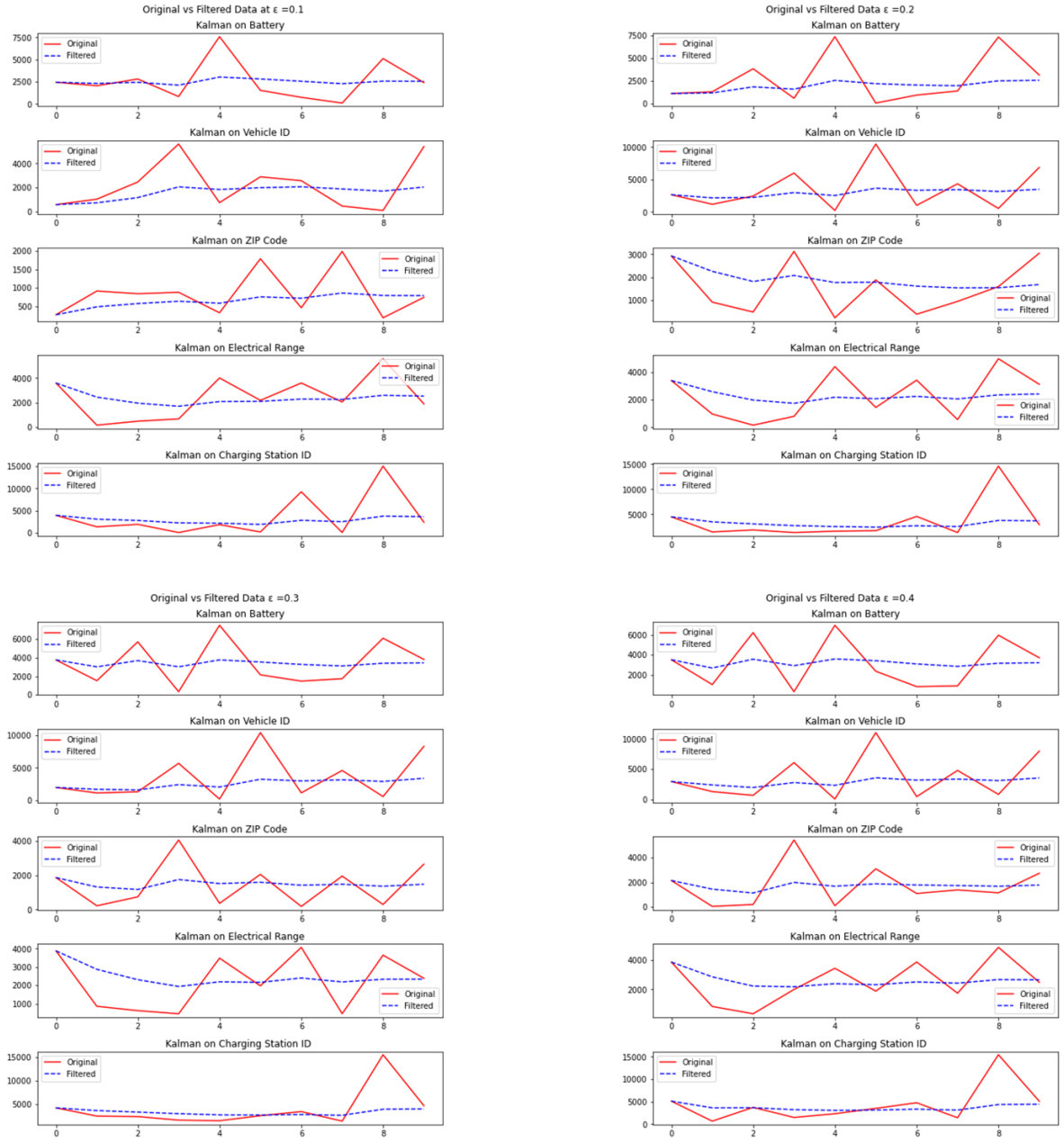

Figure 3: Results at Various Privacy Budget

As it is clearly shown above that the error in the sensitive parameters declined drastically after the implementation of the Kalman filter. The above results has been obtained implementing the Differential Privacy for different Privacy Budgets such as $\epsilon = 0.1$, $\epsilon = 0.2$, $\epsilon = 0.3$, *and* $\epsilon = 0.4$.

Then the Kalman filtration technique is implemented on the parameters of dataset pertaining sensitive dataset for the different Privacy Budgets such as $\epsilon = 0.1$, $\epsilon = 0.2$, $\epsilon = 0.3$, *and* $\epsilon = 0.4$ shown with the blue dotted line. When the dataset has extremely high error such values or dataset is not suitable for publication to any external source or cannot be used for prediction purposes. Let us suppose, if the dataset is required to be published to any department to observe the total mileage covered by people annually for any survey purpose. If that dataset has a huge error it will deviate the values from being useful. Hence, this error is mitigated by deploying the Kalman filtration technique so that particular dataset could be used for the useful purpose with revealing the identity of the user or electric vehicle.

6. Conclusion and Future Work

In this paper, we introduce a new paradigm in order to enhance the privacy of electric vehicle data systems with event-wise differential privacy using a Kalman filter. Our work developed a methodology to address the

privacy of sensitive EV data about locations and charging patterns by adding Laplace noise into individual events. This added noise, introduces significant challenges in maintaining utility and accuracy of data important for real-time operations such as navigation and energy management. In maintaining the minimum utility, we had in mind the application of a Kalman filter, which reduced the injected noise influence and further improved post-processed data accuracy while preserving user privacy. Our experimental results depicted that the proposed method gives a strong trade-off between privacy and utility, reducing overall errors in the dataset while still allowing differential privacy guarantees.

Moreover, our framework can be extended for other kinds of data streams from EVs and intelligent transportation systems. Future studies may also be performed on larger and more diverse datasets and also on more realistic deployment scenarios to further establish the scalability and generalizability of the system.

References

Bunsen, T. 2018. Global EV outlook 2018: Towards crossmodal electrification.

Chen, J.; Zhou, S.; Qiu, J.; Xu, Y.; Zeng, B.; Fang, W.; Chen, X.; Huang, Y.; Xu, Z.; and Chen, Y. 2024. A Histogram Publishing Method under Differential Privacy That Involves Balancing Small-Bin Availability First. Algorithms, 17: 293.

Chen, Y.; Machanavajjhala, A.; Hay, M.; and Miklau, G. 2017. Pegasus: Data-adaptive differentially private stream processing. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1375–1388.

Dwork, C. 2006. Differential privacy. In International colloquium on automata, languages, and programming, 1–12. Springer.

M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Futur. Gener.Comput. Syst., vol. 97, pp. 512–529, 2019.

M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 746–789, 2020.

M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.

Islam, S.; Badsha, S.; Sengupta, S.; Khalil, I.; and Atiquzzaman, M. 2023. An Intelligent Privacy Preservation Scheme for EV Charging Infrastructure. IEEE Transactions on Industrial Informatics, 19(2): 1238–1247.

F. Kato, Y. Cao, and M. Yoshikawa, "Preventing Manipulation Attack in Local Differential Privacy Using Verifiable Randomization Mechanism," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12840 LNCS, pp. 43–60, 2021.

Kellaris, G.; Papadopoulos, S.; Xiao, X.; and Papadias, D. 2014. Differentially private event sequences over infinite streams.

Kumar, G. et al., "A Privacy-Preserving Secure Framework for Electric Vehicles in IoT Using Matching Market and Signcryption," IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 7707–7722, 2020.

Langer, L.; Skopik, F.; Kienesberger, G.; and Li, Q. 2013. Privacy issues of smart e-mobility. In IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, 6682–6687. IEEE.

Morrissey, P.; Weldon, P.; and O'Mahony, M. 2016. Future standard and fast charging infrastructure planning: An analysis of electric vehicle charging behaviour. Energy policy, 89: 257–270.

Qiu, R.; Liu, X.; Huang, R.; Zheng, F.; Liang, L.; and Li, Y. 2021a. Differential privacy EV charging data release based on variable window. PeerJ Computer Science, 7: e481.

Qiu, R.; Liu, X.; Huang, R.; Zheng, F.; Liang, L.; and Li, Y. 2021b. Differential privacy EV charging data release based on variable window. PeerJ Computer Science, 7: e481.

Quinn, P.; and Malgieri, G. 2021. The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. German Law Journal, 22(8): 1583– 1612.

Ren, M.; Zhang, Q.; and Zhang, J. 2019. An introductory survey of probability density function control. Systems Science & Control Engineering, 7(1): 158–170.

Shabtai, A.; Bercovitch, M.; Rokach, L.; and Elovici, Y. 2014. Optimizing data misuse detection. ACM Transactions on Knowledge Discovery from Data (TKDD), 8(3): 1–23.

Wang, Q.; Zhang, Y.; Lu, X.; Wang, Z.; Qin, Z.; and Ren, K. 2016. Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy. IEEE Transactions on Dependable and Secure Computing, 15(4): 591–606.

Wang, Y.; Su, Z.; Xu, Q.; Yang, T.; and Zhang, N. 2019. A novel charging scheme for electric vehicles with smart communities in vehicular networks. IEEE Transactions on Vehicular Technology, 68(9): 8487–8501.

Yong, C.; Huo, Y.; Hu, C.; Lu, Y.; and Jing, G. 2018. A real-time aggregate data publishing scheme with adaptive ω-event differential privacy. Mathematical Foundations of Computing, 1(3).

Zhang, X.; Xu, M.; Da, G.; and Zhao, P. 2021. Ensuring confidentiality and availability of sensitive data over a network system under cyber threats. Reliability Engineering & System Safety, 214: 107697.