A Privacy Recommending Data Processing Model for Internet of Vehicles (IoV) Services

Ali Alqarni
Department of Computer Science and Artificial Intelligence, College of Computing and Information Technology, University of Bisha, Bisha 67714, P.O Box 551, Saudi Arabia
aqrni@ub.edu.sa (corresponding author)

Received: 4 May 2024 | Revised: 25 May 2024 and 29 May 2024 | Accepted: 30 May 2024

 DOI: https://doi.org/10.48084/etasr.7743

ABSTRACT

The Internet of Vehicles (IoV) faces security challenges in maintaining privacy due to the presence of open networks and diverse services. Ensuring privacy is essential in transportation networks to provide users with a long-lasting driving, navigation, and communication experience. In this paper, the proposed Privacy Recommending Data Processing Model (PRDPM) is deployed to handle the huge amount of data accumulated in this field. The proposed model adopts data processing techniques that are dependent on user demand and are influenced by either neighboring entities or service providers. The various application requirements are analyzed to minimize the potential privacy consequences. The data from various intervals are utilized to validate the parameters in the operational plane. Thus, data balancing is performed using plane differentiation to prevent privacy leaks in either of the vehicular services. This is useful for neighbors and infrastructures across various applications/users.

Keywords-IoV; privacy-preserving; privacy leak

I. INTRODUCTION

Big data is a scientific area that analyzes or identifies amounts of data. Big data technology is widely used in various fields to improve the efficiency of systems. Big data is deployed in the Internet of Vehicles (IoV) to enhance the effectiveness of management processes [1]. IoV faces various privacy and security issues that cause severe damage to the network. Big data-based privacy-preserving schemes which provide feasible privacy services to the users are employed in IoV [2, 3]. IoV connects the vehicles with the people using an internet connection [4]. The big data-based technique identifies the key privacy issues which occur during the authentication process [5]. Big data solve privacy issues improving the network performance. The actual goal of big data in privacy issues is to increase the safety and security level of users from third-parties [6]. Various privacy-preserving schemes are implemented to ameliorate the mobility and security ratio of IoV systems. Authentication and Key Agreement (AKA) schemes are mostly used in IoV systems [7]. An AKA scheme utilized during the authentication process provides a secret key value to the users. The secret key values contain important values that reduce the complexity of the authentication process [8]. The AKA scheme ensures the privacy and security level of user data from unauthorized persons in IoV networks. A privacy-preserving data-sharing scheme is also used in IoV [9]. The privacy-preserving scheme collects the data which are captured via vehicular sensors. The sensors produce optimal information for the authorization process that reduces the authentication error [10]. A blockchain (BC) based privacy-preserving policy which preserves users' data from hackers can be employed in IoV [2, 11, 12]. Machine Learning (ML) algorithms are applied in IoV to identify privacy issues [13]. Long Short-Term Memory (LSTM) algorithm-based privacy framework models are mainly implemented to detect intrusions in IoV. The LSTM models enhance the quality of experience (QoE) range of the systems [14, 15]. A Deep Reinforcement Learning (DRL) algorithm has been also put into service in the privacy management process. The DRL algorithm uses a task offloading scheme that provides an effective architecture for IoV [16, 17]. In [18], a privacy-preserving-based secured framework (P2SF) for IoV provides an efficient enclosure technique for securing users' data from third-party members and maximizes the performance range of the systems [18]. In [19], the privacy-preserving and scalable authentication protocol for the IoV aims to provide effective services to IoV users. The proposed model increases the security level of IoV systems. Physical unclonable functions are utilized to reduce the complication ratio in the authentication process. A privacy-preserving protocol for Location-Based Service (LBS) in IoV is mainly employed to provide optimal services to drivers [20]. LBS identifies the exact location of the vehicles and enhances the performance of IoV. The proposed protocol maximizes the privacy and safety range of IoVs.

In [21], the Concerted Silence-based Location Privacy-Preserving Scheme (CSLPPS) for IoV detects unlinkable attacks which occur during traveling. The CSLPPS identifies the cyber-attacks and minimizes the latency in performing tasks. The privacy-preserving data scheduling in the incentive-driven Vehicular Network (VN) provides an effective data scheduling algorithm for VN vehicles. An incentive mechanism is used in [22] to offer efficient data security

services. Another mechanism based on the decentralized and privacy-preserving reputation system for Social Internet of Vehicles (SIoV) guarantees the safety and privacy range of users from third-party members [23]. The privacy-preserving route planning scheme for IoVs provides effective routing plans to the users. The designed scheme in [24] provides graph-based location-sharing services among the vehicles.

A BC-enabled data access method using attribute-based encryption for IoV was followed in [25] to produce optimal data for privacy-preserving policies. In [26], the Location Entropy-based Privacy Protection (LEPPV) algorithm for SIoV was proposed to provide proper location entropy entities to the users. In [27], the location privacy-preserving algorithm for Cloud-Enabled IoV (CE-IoV) reduces the linking and tracking latency in IoV systems. A game theoretic approach, which identifies the exact functionalities of the privacy-preserving process, was employed. Masking technology is deployed in [28] to encrypt the data used for the authentication process that enhances the overall performance and feasibility range of IoVs. In [29], the Roadside Unit (RSU) supplies with relevant datasets for the querying process that provides effective codes for the authentication procedure. The designed scheme enhances the performance level of virtual cloud systems. Authors in [30] developed a trust-based privacy-preserving friend-matching scheme for the SIoV. Bloom filters are used in the scheme to handle the malicious vehicles. The developed scheme maximizes the accuracy in a matching process that enhances the efficiency level of SIoV. The Efficient Distance-based Privacy-Preserving Authentication (EDPPA) protocol for Vehicular Ad-hoc Networks (VANETs) [31] can minimize energy consumption in the authentication process while maximizing the safety and security range of users from third-party members.

The contributions of the current article are:

- A privacy recommending processing model for the IoV is proposed that improves service sustainability under secure application conditions.
- Comparative analysis is conducted using different metrics and methods related to security and data handling for validating the proposed model's consistency.

II. THE PROPOSED MODEL

IoV is a network of vehicle accouters with sensors, software, and technologies that intercede between these to associate and transact information over the Internet in consonance with consent conventionalities. Privacy-preserving automation approves the users to ensure the privacy of their personalized attributable information provided to and managed by service providers, while allowing them to organize the components of the information to be used in the privacy-preserving processes. Cloud services enhance the building of services according to user necessities and the complaisance of working in the cloud. Data preservation and production to the users is the procedure of executing a determined impersonation of either a whole information system or parts of it to narrate connections between users and the service providers. Figure 1 presents the schematic representation of the proposed model. The IoV demands the application for the following neighbor and the service providers. There are two application demands, namely service response and privacy, which are based on the previous service response. These outputs are given as the input to the Support Vector Machine (SVM) algorithm for the determination of existence and sustainability, which are identified based on the cloud/IoT services. The information from the different acquired time intervals is utilized for authenticating the pre-mentioned characteristics in the operational plane by distinguishing the hyperplane for min-max recommendations. Depending on these application demands, further processes take place and then the services are provided for the users with high privacy preserving data.

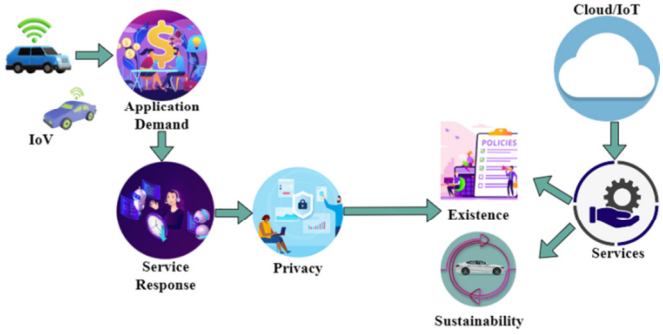

Fig. 1. The authentication procedure.

A. Application Demand

The process of acquiring the application demand from the users through the IoV is explained by (1):

$$\left.\begin{gathered}\langle a,b\rangle x^2=\langle a^x,b^x\rangle x+\langle a^{x_1},b^{x_2}\rangle x \\ a=a^x+x_1a^1 \\ b=b^x+x_1b^1 \\ x_1\langle a,b\rangle=\begin{bmatrix} x_1a & x_1b & \dots & x_1ab \\ x_1a_1 & x_1b_1 & \dots & x_1(a_1b_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_na_n & x_nb_n & \cdots & x_n(a_nb_n)\end{bmatrix}\end{gathered}\right\} \quad (1)$$

where a represents the application demands from the users, b represents the procedure of the IoV in this application production, and x represents the classification of the application demands.

B. Service Demand

The validation of the application demands from the users is based on the service responses and the privacy of the previous processes. The PRDPM procedures take place with the help of the outcome of the validation procedures. The process of service response in the application demand is explained by (2):

$$\begin{gathered}\varphi_C(Z)=\varphi_C(a+b) \\ =\varphi_C(a,b) \\ =\varphi_{C_1}(a,b)+x\varphi_C(a+b) \\ \varphi_C(a+b)=x_1\big(\cdot\,(a,b)\big) \\ C=a+x_1b \\ \langle\varphi_x(C),\varphi_{x_1}(C')\rangle x=\langle\varphi_C(a+b),\varphi_{x_1}(a',b')\rangle x \\ =\varphi_C\big((a',b')\cdot(a,b)\big)\end{gathered} \quad (2)$$

where φ denotes the service response, C the previous processes, and Z the response of the service in the previous processes.

C. Application Authentication

The authentication of the application demand from the user is explained by:

$$\begin{gathered} b_c^T(Z,Z') = b_c^T(Z',Z) \\ b_c^x(Z,Z') = b_c^x(Z',Z) \\ \sum_{n,x=1}^{n} C_n C_x b_c^T(Z_n, Z_x) = 0 \\ where, \\ n > 0, \quad C_1 \ldots\ldots C_n \in C \\ Z_1 \ldots\ldots Z_n \in X \end{gathered} \tag{3}$$

where T represents the authentication process. Now the privacy of the procedure is verified for the further processes.

The authentication for privacy is led by using registration to validated phases. First, the request relies on C for the existing vehicle and any a for new vehicles Z. Therefore, the authentication process requires Z_1 to $Z_n \in X$ to maximize ψ as shown in Figure 2. Those outcomes are associated with enhancements in the privacy-preserving process in the existing service production procedures. Based on the previous service response, the privacy level of the present method is validated in the application demands. Then, this output is given as the input to the SVM algorithm to estimate existence and sustainability. L denotes the present privacy level based on the previous service response explained by (1):

$$\left.\begin{gathered} L_c^T = \left(\binom{x}{y}, \binom{x'}{y'}\right) = \sum_{n=1}\left(b_c(Z,Z')\right) \\ = \sum_{n=1}^{x}\left[\binom{b_1}{b_2} \times \binom{Z_1}{Z_2}\right] \\ Z = x + Ty \\ Z' = x' + Ty' \\ n > 0, \quad b_1 \ldots\ldots b_n \in T \\ Z_1 \ldots\ldots Z_n \in X \end{gathered}\right\} \tag{4}$$

where Z is the privacy of the previous response of the service providers. The validation process takes place depending on the outcome of the service providers and the privacy of the previous response. Now, the present privacy level L_c^T is acquired based on the previous response Z. This process is explained in Figure 2.

The process of determining the present privacy level of the method based on the previous response is analyzed by (5):

$$\left.\begin{gathered} L_c^T = \left(\binom{x}{y}, \binom{x'}{y'}\right) = \sum_{n=1}\left(b_c(Z,Z')\right) \\ = \sum_{n=1}^{x}\left[\binom{b_1}{b_2} \times \binom{Z_1}{Z_2}\right] \\ Z = x + Ty \\ Z' = x' + Ty' \\ n > 0, \quad b_1 \ldots\ldots b_n \in T \\ Z_1 \ldots\ldots Z_n \in X \end{gathered}\right\} \tag{5}$$

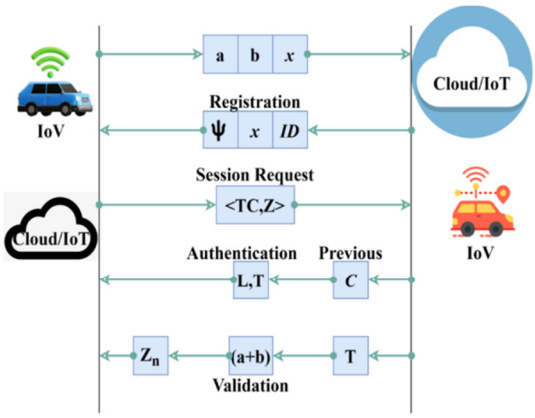

Fig. 2. Application authentication.

The existence of privacy helps in the data's privacy preservation and then the outputs of the previous privacy of the service providers help in the enhancement of the privacy-preserving processes. A new privacy existence algorithm is introduced based on the above discussed equations.

1: $\forall\, a \; in \; X$
$do\{$
2: compute $x_1\langle a,b\rangle$ using equation (1)
3: $if\{(a+b) = x_1(\cdot\,(a,b))\}$ then
4: Compute $Z\ \forall C$
5: $if\{\frac{Z}{C} || \frac{\varphi}{C} == 1\}$ then
6: Perform $Z_n Z_x b_c^T(x_n, x_c)\ \forall\, x = 1\ to\ n$
7: Estimate L until C is completed
8: Goto Step 2
9: else Compute $b_c^T(Z,Z') = b_c^T(Z',Z)$
10: Validate $\langle \varphi_x(C), \varphi_{x_1}(C')\rangle x$ until $\frac{\varphi}{C} == 1$ is true
11: end if
12: Update $C = a + x_1 b$
13: else $\sum_{n,x=1}^{n} c_n c_x b_c^T(Z_n, Z_x) = 0$
14: end if
15: end do

III. RESULTS AND DISCUSSION

The proposed model is validated putting into service the NS3 experiments that consider an OpenSource map in SUMO [32, 33]. A scenario with 3 km long highway with 4 intersections and 2 parallel paths is used for simulation. The vehicle density is varied between 10 and 120 at an average speed of 45 km/hr. The vehicles are calibrated to exchange information employing 15 intervals for a maximum span of 30 min within their 250 m communication range. The accumulated data are validated utilizing WEKA 3.0 tool. The levels of data filtering discussed in the previous sections are feasible implementing this tool-based analysis. With this simulation setup, the metrics of privacy leaks and privacy recommendations rates are validated. The authentication is provided applying the conventional SHA algorithm. The methods EPDQD [29], EDPPA [31], and PPDS [22] are considered for the proposed model in the metric comparisons.

A. Privacy Leak

The application demands are extracted from the users through the IoV and then the service response and privacy of the previous service providers are determined. The service responses are the ones that detect whether the services are accomplished on time during the previous service production processes. The application demands are validated through two perspectives: service response and then privacy. By this, the privacy leak is reduced with the help of the outcome of the service response and then the privacy of the previous procedures as evidenced in Figure 3.

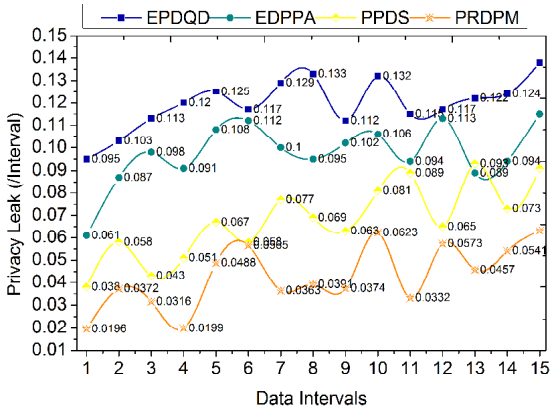

Fig. 3. Privacy leak vs data intervals.

B. Privacy Recommendations

The recommendation of privacy is efficacious in this process with the aid of the PRDPM method. The privacy of the previous service providers is estimated for the alteration of the privacy procedures in the current approach. Based on the previous service response, the privacy level of the present method is validated in the application demands. Then, this output is given as the input to the SVM algorithm. The two planes of the SVM help in the determination of the existence and sustainability at different time intervals. By this, the privacy recommendations are enhanced in this method for the better execution of the services to the users (Figure 4). The time taken for the recommendation is less and hence privacy preservation is efficacious for the accomplishment of the services with better outcomes. Sustainability is determined to identify the prolonged time of privacy in the data. Depending on this, the service is executed for the users, and improvements take place in the privacy-preserving process.

A comparative analysis is presented in Table I. The existing methods EPDQD [29], EDPPA [31], and PPDS [22] achieved privacy leak/intervals of 0.133, 0.108, and 0.086, respectively, while the proposed PRDPM surpassed them. The privacy recommendation/vehicle is 6, 10, and 15 in existing methods, respectively, while the proposed method has achieved 19.

This proposed model processes data based on the user demand following the neighbor or service provider for IoV. The different application demands are processed for the maximum and least possible privacy implications for existence and service sustainability.

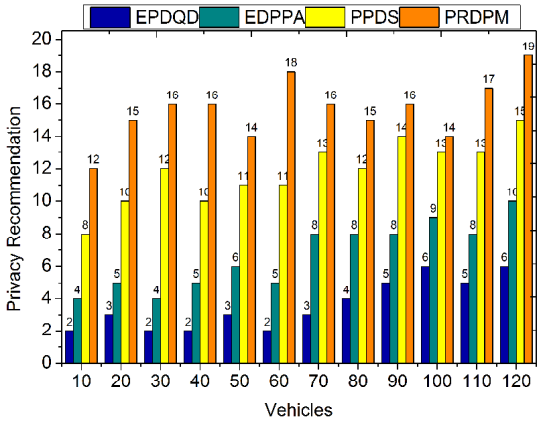

Fig. 4. Privacy recommdenation vs vehicles.

TABLE I. COMPRATIVE PERFORMANCE ANALYSIS

Metrics	EPDQD	EDPPA	PPDS	PRDPM
Privacy leak (/interval)	0.133	0.108	0.086	0.0594
Privacy recommendation/ vehicle	6	10	15	19

IV. CONCLUSION

In this paper, a privacy recommending data processing model for IoV services that leverages security features is presented. The proposed model validates privacy existence and its sustainability across various intervals. The adjustments are linear throughout the vehicle's travel intervals for which the plane differentiation for sustainability and existence is validated. This process is applicable for vehicle-to-vehicle and vehicle-to-infrastructure communication, preventing service failures. From the presented metric-based analysis, it is seen that the proposed model improves privacy leaks and privacy recommendations for different vehicle densities. A comparative analysis demonstrates that the proposed PRDPM has lower number of leaks in the give time interval and more recommendations than the existing methods.

In the future, this independent analysis is likely to be performed deploying blockchain-enabled communication systems. Such integration improves the application usage for different irregular and asynchronous intervals.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Graduate Studies and Scientific Research at University of Bisha for funding this research through the promising program under grant number (UB-Promising-33-1445).

REFERENCES

[1] F. Algarni, M. A. Khan, W. Alawad, and N. B. Halima, "P3S: Pertinent Privacy-Preserving Scheme for Remotely Sensed Environmental Data in Smart Cities," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 16, pp. 5905–5918, 2023, https://doi.org/10.1109/JSTARS.2023.3288743.

[2] T. Qamar, N. Z. Bawany, and N. A. Khan, "EDAMS: Efficient Data Anonymization Model Selector for Privacy-Preserving Data Publishing," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5423–5427, Apr. 2020, https://doi.org/10.48084/etasr.3374.

[3] E. Yilmaz and O. Can, "Unveiling Shadows: Harnessing Artificial Intelligence for Insider Threat Detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13341–13346, Apr. 2024, https://doi.org/10.48084/etasr.6911.

[4] M. A. Alqarni, A. Alharthi, A. Alqarni, and M. Ayoub Khan, "A transfer-learning-based energy-conservation model for adaptive guided routes in autonomous vehicles," *Alexandria Engineering Journal*, vol. 76, pp. 491–503, Aug. 2023, https://doi.org/10.1016/j.aej.2023.06.060.

[5] A. Khan, C. Peoples, Y. Li, M. Dianati, and A. M. Vegni, "Guest Editorial: Privacy, Trust and Reputation Management in Internet of Vehicles (IoV)," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 24–25, Jun. 2023, https://doi.org/10.1109/MIOT.2023.10145007.

[6] N. Jayakumar and A. M. Kulkarni, "A Simple Measuring Model for Evaluating the Performance of Small Block Size Accesses in Lustre File System," *Engineering, Technology & Applied Science Research*, vol. 7, no. 6, pp. 2313–2318, Dec. 2017, https://doi.org/10.48084/etasr.1557.

[7] A. Alharthi, Q. Ni, R. Jiang, and M. A. Khan, "A Computational Model for Reputation and Ensemble-Based Learning Model for Prediction of Trustworthiness in Vehicular Ad Hoc Network," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18248–18258, Jul. 2023, https://doi.org/10.1109/JIOT.2023.3279950.

[8] K. Gu, K. Wang, X. Li, and W. Jia, "Multi-Fogs-Based Traceable Privacy-Preserving Scheme for Vehicular Identity in Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 12544–12561, Aug. 2022, https://doi.org/10.1109/TITS.2021.3115171.

[9] Y. Li *et al.*, "Privacy-Preserving and Real-Time Detection of Vehicular Congestion Using Multilayer Perceptron Approach for Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 12530–12542, Sep. 2022, https://doi.org/10.1109/TVT.2022.3199407.

[10] N. Wang *et al.*, "A blockchain based privacy-preserving federated learning scheme for Internet of Vehicles," *Digital Communications and Networks*, vol. 10, no. 1, pp. 126–134, Feb. 2024, https://doi.org/10.1016/j.dcan.2022.05.020.

[11] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 75, pp. 66–86, Nov. 2020, https://doi.org/10.1016/j.trf.2020.09.019.

[12] A. Alharthi, Q. Ni, R. Jiang, and M. A. Khan, "A Formal Method of Trust Computation in VANET: A Spatial, Temporal and Behavioral Approach," in *International Conference on Smart Technologies in Urban Engineering*, Kharkiv, Ukraine, Jun. 2022, pp. 775–784, https://doi.org/10.1007/978-3-031-20141-7_69.

[13] W. U. Khan, X. Li, A. Ihsan, M. A. Khan, V. G. Menon, and M. Ahmed, "NOMA-Enabled Optimization Framework for Next-Generation Small-Cell IoV Networks Under Imperfect SIC Decoding," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 22442–22451, Nov. 2022, https://doi.org/10.1109/TITS.2021.3091402.

[14] Y. Ren, X. Li, S.-F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for Vehicular Ad-Hoc Networks," *Journal of Information Security and Applications*, vol. 58, May 2021, Art. no. 102698, https://doi.org/10.1016/j.jisa.2020.102698.

[15] L. Xu, X. Zhou, M. A. Khan, X. Li, V. G. Menon, and X. Yu, "Communication Quality Prediction for Internet of Vehicle (IoV) Networks: An Elman Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19644–19654, Oct. 2022, https://doi.org/10.1109/TITS.2021.3088862.

[16] J. Xiong, R. Bi, Y. Tian, X. Liu, and D. Wu, "Toward Lightweight, Privacy-Preserving Cooperative Object Classification for Connected Autonomous Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2787–2801, Feb. 2022, https://doi.org/10.1109/JIOT.2021.3093573.

[17] S. Behera, M. Adhikari, V. G. Menon, and M. A. Khan, "Large Model-assisted Federated Learning for Object Detection of Autonomous Vehicles in Edge," *IEEE Transactions on Vehicular Technology*, pp. 1–10, 2024, https://doi.org/10.1109/TVT.2024.3404097.

[18] P. Hu *et al.*, "Efficient location privacy-preserving range query scheme for vehicle sensing systems," *Journal of Systems Architecture*, vol. 106, Jun. 2020, Art. no. 101714, https://doi.org/10.1016/j.sysarc.2020.101714.

[19] M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, Jan. 2021, https://doi.org/10.1109/JIOT.2020.3010893.

[20] J. Huang, Y. Qian, and R. Q. Hu, "A Privacy-Preserving Scheme for Location-Based Services in the Internet of Vehicles," *Journal of Communications and Information Networks*, vol. 6, no. 4, pp. 385–395, Dec. 2021, https://doi.org/10.23919/JCIN.2021.9663103.

[21] L. Benarous, S. Bitam, and A. Mellouk, "CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7153–7160, Jul. 2021, https://doi.org/10.1109/TVT.2021.3088762.

[22] Y. Xia, T. Zhan, L. Wu, X. Zheng, and J. Jin, "Privacy-Preserving Data Scheduling in Incentive-Driven Vehicular Network," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22669–22681, Aug. 2022, https://doi.org/10.1109/JIOT.2022.3182542.

[23] Y. Liu *et al.*, "VRepChain: A Decentralized and Privacy-Preserving Reputation System for Social Internet of Vehicles Based on Blockchain," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 12, pp. 13242–13253, Dec. 2022, https://doi.org/10.1109/TVT.2022.3198004.

[24] U. I. Atmaca, C. Maple, G. Epiphaniou, and M. Dianati, "A privacy-preserving route planning scheme for the Internet of Vehicles," *Ad Hoc Networks*, vol. 123, Dec. 2021, Art. no. 102680, https://doi.org/10.1016/j.adhoc.2021.102680.

[25] Y. Zhang, L. Zhang, Q. Wu, and Y. Mu, "Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9216–9227, Nov. 2022, https://doi.org/10.1016/j.jksuci.2022.09.004.

[26] L. Xing, Y. Huang, J. Gao, X. Jia, H. Wu, and H. Ma, "Location Entropy-Based Privacy Protection Algorithm for Social Internet of Vehicles," *Wireless Personal Communications*, vol. 130, no. 4, pp. 3009–3025, Jun. 2023, https://doi.org/10.1007/s11277-023-10413-4.

[27] L. Benarous and B. Kadri, "Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 461–472, Jan. 2022, https://doi.org/10.1007/s12083-021-01233-z.

[28] P. Hu *et al.*, "A secure and lightweight privacy-preserving data aggregation scheme for internet of vehicles," *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 1002–1013, May 2020, https://doi.org/10.1007/s12083-019-00849-6.

[29] P. Hu, Y. Wang, G. Xiao, J. Zhou, B. Gong, and Y. Wang, "An efficient privacy-preserving data query and dissemination scheme in vehicular cloud," *Pervasive and Mobile Computing*, vol. 65, May 2020, Art. no. 101152, https://doi.org/10.1016/j.pmcj.2020.101152.

[30] C. Lai, Y. Du, Q. Guo, and D. Zheng, "A trust-based privacy-preserving friend matching scheme in social Internet of Vehicles," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2011–2025, Jul. 2021, https://doi.org/10.1007/s12083-021-01140-3.

[31] J. Ren, Y. Cheng, and S. Xu, "EDPPA: An efficient distance-based privacy preserving authentication protocol in VANET," *Peer-to-Peer Networking and Applications*, vol. 15, no. 3, pp. 1385–1397, May 2022, https://doi.org/10.1007/s12083-022-01297-5.

[32] "SUMO." 2024, [Online]. Available: https://github.com/eclipse-sumo/sumo.

[33] "GEOFABRIK // Data." https://www.geofabrik.de/data/.