2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) | 979-8-3503-2385-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/TPS-ISA58951.2023.00015

Preserving Location Privacy in the Modern Era of Pervasive Environments

Tyler Nicewaner
Computer Science
Vanderbilt University
tyler.j.nicewarner@vanderbilt.edu

Alian Yu
Computer Science
Vanderbilt University
alian.yu@vanderbilt.edu

Wei Jiang
Oracle Labs
wei.wj.jiang@oracle.com

Dan Lin
Computer Science
Vanderbilt University
dan.lin@vanderbilt.edu

***Abstract*—The rapid expansion of location-based services gives rise to significant security and privacy apprehensions. While these services deliver convenience, they accentuate concerns regarding widespread location tracking via web services, mobile apps, IoT devices, and autonomous vehicles. In this study, we comprehensively assess the merits and constraints of prevalent techniques in location privacy protection, including spatial-temporal cloaking, k-anonymity, differential privacy, and encryption. Furthermore, we delve into emerging applications like intelligent traffic planning and virus contact tracing which introduce novel complexities to the pursuit of robust location privacy safeguards.**

I. Introduction

We are experiencing the rapidly expanding use of location-based services which has an estimated market growth from 20 billion in 2021 to 48.5 billion by 2026 [1]. While we enjoy the convenience and benefits brought by location-based services ranging from GPS navigation, friend locator to recent infectious disease contact tracing, location tracking is becoming a vital security and privacy concern among the majority of people.

A huge amount of our location information is continuously being collected by companies and organizations through various types of services that request users to provide their locations or collect users' locations automatically. As illustrated in Figure 1, people living in modern life have been or will be tracked almost everywhere via web services, mobile apps, Internet of Things (IoT), smart vehicles, etc. It is never clear to an end user how much and how long one's location data has been stored and when or whether the data has been sold to third parties. Unexpected location disclosure can lead to a series of consequences, some of which could be severe. To name a few, kids sharing their locations on social media could put themselves at risk of unwanted contact from strangers and sometimes even cause kidnapping; potential employers or insurance companies may take advantage of the obtained rich location data of a person to infer their social relationship, health, religion, etc., making decisions that may be unfair to that person; hackers who compromise location-based service providers could utilize the target's daily travel habits to conduct social engineering attacks. Fortunately, there is light at the end of this tunnel. More and more countries have tightened their privacy laws to enhance privacy protection for their people. Still, this would not be an easy journey to accomplish without the necessary techniques to preserve the privacy while ensuring the same level of service delivery.

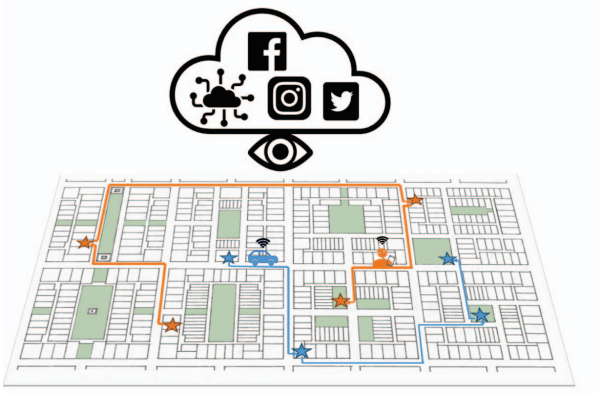

Fig. 1: Location Privacy in Pervasive Environments

Research on location privacy protection has a long history in the literature since decades ago. Popular techniques being proposed include spatial-temporal cloaking, k-anonymity, differential privacy, and encryption. However, it remains an extremely challenging task to achieve the ideal location privacy protection without degrading the quality of location-based services. Moreover, the emergence of novel applications within pervasive environments, including vehicular ad-hoc networks, IoT applications, crowdsourcing/sensing, and virus contact tracing, has introduced a fresh array of challenges to location privacy protection.

In the remaining of the paper, we will first give an overview of location privacy classifications (Section II), and then discuss location privacy protection techniques in traditional settings (Section III), and the modern era of pervasive environments (Section IV), followed by a series of open challenges (Section V). Finally, we will conclude the paper in Section VI.

II. Location Privacy Classifications

The risk of location privacy breach occurs at the moment when a user gives out his/her exact location information in plain text to another party which could be the service provider, a broker agent, a peer user, etc. Any location-based service is essentially conducting some kind of spatial-temporal queries. Based on the location sensitivity of the

979-8-3503-2385-6/23/$31.00 ©2023 IEEE
DOI 10.1109/TPS-ISA58951.2023.00015

query input and output, we can classify location-based services into the following three categories: (i) private-input-private-output (RIRO), (ii) public-input-private-output (PIRO), and (iii) private-input-public-output (RIPO).

- **Private-input-private-output (RIRO)**: An RIRO type service takes private user location data as query input and compares that with private location data of other users. For example, the contact tracing application collects users' trajectory information and then identifies trajectories of other users that are within a certain vicinity of an input trajectory (i.e., a patient's trajectory). Family and friend locator is another popular application in this category.
- **Public-input-private-output (PIRO)**: Examples of PIRO type services are emerging crowdsourcing applications such as the Apple Map incident report feature that prompts questions to users at a certain location where an incident took place earlier and asks for an update of an incident status from the users who are currently driving towards the scene. Similarly, the envisioned crowdsensing applications require the server to recruit users who are near a designated workplace to use their mobile devices to report the sensing data about the location. Also, with the increasing adoption of IoT (Internet of Things) devices in public venues, servers may now track users whenever they access those IoT devices. For example, cars equipped with an RFID-enabled pass can go by a toll station faster without stopping whereas the car's location is recorded automatically by the server at the same time. In the future, there may be more electric charging stations that can serve cars automatically without individual payment but a monthly charge to their registered online accounts. Other envisioned public IoT services such as Internet-enabled printing services could also disclose users' location information to the service providers whenever the users use the service. In these PIRO applications, the query input (e.g., the incident location, the workplace, the charging location) is publicly known while the users' locations are private.
- **Private-input-public-output (RIPO)**: The RIPO type services have been widely adopted nowadays. Finding a nearby gas station, a nearby hotel, or a nearby restaurant all fall in this category, where the query input is the user's private location while the query results are public locations.

Existing location privacy preserving algorithms can be classified into three main categories based on the underlying techniques: (i) Spatial-temporal cloaking and k-anonymity; (ii) Differential privacy based approaches; and (iii) Encryption based approaches. In the next section, we will review the representative works in each category.

III. Location Privacy in Traditional Mobile Applications

In traditional mobile applications such as finding gas stations, map navigation, weather inquiry, and traffic flow analysis, various privacy preserving approaches have been proposed.

A. Spatial-temporal Cloaking and K-anonymity

The core concept of spatial-temporal cloaking involves generating a cloaking region encompassing the actual location of a user along with $K-1$ other users, thereby rendering the service provider incapable of distinguishing among the K users within the same area, ensuring a level of K-anonymity. This concept was initially introduced by Gruteser et al. [2] and has since undergone various extensions by others [3]–[8], each employing distinct methods for creating these cloaking regions. However, while these approaches effectively obscure the precise user location, they fall short in safeguarding coarse location data, such as user movement patterns. To illustrate, attackers may be unable to pinpoint a user's exact home location, but they could still deduce the city of residence and approximate user trajectory by connecting these cloaking regions. To address this limitation, Lin et al. [9], [10] propose a remedial solution involving the transformation of all real locations into a new domain, providing comprehensive protection against the exposure of precise and continuous locations. It is important to note that this approach is primarily suited for RIRO (Private Input Private Output) type services such as location queries about friends.

In addition to the utilization of cloaking regions, Besides using cloaking regions, dummy trajectories are also often used to achieve k-anonymity for privacy preservation. Notably, various strategies have been devised to achieve this objective. For instance, Niu et al. [11], [12] introduced strategies like dummy swapping and dummy selection. Similarly, Xue et al. [13] put forth the idea of deploying multiple virtual probes to differentiate between user locations and fabricated GPS positions. Addressing the queries related to top-k Points of Interest (POIs), Zhang et al. [14] proposed two algorithms for selecting dummy-POIs. Fei et al. [15] took a distinct approach by categorizing users into groups, selecting dummies based on these groups, and subsequently sharing the outcomes from the service provider. Nonetheless, a shortcoming of these dummy trajectories lies in their lack of coherent movement patterns. This vulnerability makes them susceptible to detection by malicious entities analyzing the dummies collected at different timestamps. To address this limitation, Wang et al. [16] proposed a fog structure to generate partial information and dummy trajectories. Hara et al. [17] incorporated geographical constraints into the dummy generation process. Similarly aligned with the goal of obscuring actual user locations, Liu et al. [18] introduced a filtering mechanism to eliminate dummies that could be discerned based on spatiotemporal correlations. Hayashida et al. [19] proposed a method to estimate user movement by utilizing inputted visiting points. On a different note, Pingley et al. devised a strategy that generates dummy queries with diverse service attributes, effectively preventing adversaries from linking a query to a specific user.

Yet, these methods fall short in considering the behavioral rationale of the generated dummies. Their lack of adherence to daily routines renders them easily distinguishable from

genuine human trajectories through conventional data mining techniques. In a recent advancement, Kang et al. [20] introduced the concept of generating decoys that emulate human behaviors throughout the day. These decoys discreetly submit identical location-based service requests as the genuine user, thereby camouflaging the user's actual requests.

The above discussion focuses on mainly real-time location based services. There is a line of research which looks into the privacy protection when historical location data is published for general use. Collected location data have great potential for statistical usage in various applications such as traffic congestion prevention, infrastructure and evacuation planning, analysis of social behavior, advertising campaigns, and control of spread of diseases. While the benefits provided by location datasets are indisputable, preserving the location privacy of the data owners remains a challenging task. Most of existing approaches in this field [21]–[27] adopt the k-anonymity concept and output anonymized trajectories in the form of cloaking regions or centers of clusters. More advanced approaches [24], [28]–[30] generate anonymized trajectories following the road networks. The most recent efforts also look into scalability issues brought by the rapidly expanding volume of location data. Addressing this challenge, Katrina et al. introduce an innovative solution called MELT [31], which leverages the MapReduce computing paradigm to facilitate concurrent processing of trajectory anonymization tasks.

B. Differential Privacy

An alternative strategy for hiding precise locations of users from service providers involves employing the principles of differential privacy to introduce controlled perturbations to users' actual locations. This approach, which adds an element of randomness to the data, seeks to obscure individual details while maintaining aggregate data utility. Andres et al. [32] applied Laplacian noise to location data on a discrete Cartesian plane. This framework empowers users to calibrate their desired privacy levels, enabling them to modulate the extent of noise applied to their location data. A similar concept is presented by Chen et al. [33], who suggest adapting noise levels based on the concepts of unobservability and a Kalman filter. Xiao et al. [34] propose a method that adjusts privacy protection levels according to users' location profiles and historical mobility patterns. Ngo and Kim [35] introduce the notion of differential privacy geo-indistinguishability, which contributes to diminishing the average size of cloaking regions. Similarly, Wang et al. [36] employ differential geo-obfuscation as a means to obscure exact user locations.

However, a caveat remains that even with differential-based mechanisms, the noises introduced to the location data must be judiciously managed to avoid degradation of service quality. Consequently, adversaries may still glean certain information, such as the user's residing city, approximate movement trajectories, and daily routine patterns, from the perturbed data. This susceptibility to profiling arises because these approaches do not fully eliminate recognizable patterns in the data. Furthermore, adversaries might exploit non-sensitive contextual information to deduce sensitive user particulars, as pointed out in [37]. As a result, achieving an ideal balance between privacy preservation and data utility remains a challenge in these differential privacy-based techniques.

C. Encryption-based Privacy Preserving

Encryption-based strategies represent a robust avenue for safeguarding location privacy, as they revolve around encrypting location data and facilitating queries directly on the encrypted data, thereby ensuring comprehensive privacy preservation. A prominent example of this approach is exemplified by the work of Ghinita et al. [38], who devised a framework centered on Private Information Retrieval to enable private nearest neighbor queries. Puttaswamy and Zhao [39] propose an approach where location coordinates are encrypted prior to sharing, guaranteeing that only authorized users possess the decryption keys to access location information.

Leveraging the computational capabilities of smartphones, Huang et al. [40] introduced secure multi-party computation for processing users' location data. Addressing the context of sharing location among trusted peers and unfamiliar individuals, Wei et al. [41] created MobiShare, a system that meticulously maintains user location privacy. Guha et al. [42] designed a cloud-based matching service that offers encrypted attributes and their values. Li and Jung [43] engineered a protocol for privacy-preserving location queries using Pallier encryption to obstruct adversaries from intercepting transmitted data. Puttaswamy et al. [44] subsequently extended their efforts to protect location privacy within geo-social applications.

For optimizing query efficiency, Paulet et al. [45] combined oblivious transfer and private information retrieval techniques. Building upon enhanced homomorphic encryption, Zhu et al. [46] introduced a query framework that empowers users to retrieve Location-Based Service (LBS) outcomes within a specified polygon range without disclosing the precise query polygon information. These encryption-based strategies substantially fortify user location information privacy. Nevertheless, their adoption necessitates substantial modifications to the existing architecture of both LBS servers and clients, a transition potentially encumbered by the associated capital costs.

While encryption-based techniques undeniably provide the most potent shield for location privacy, the main obstacle in this realm is the considerable computational complexity they entail. However, there is an optimistic outlook on the horizon: the continuous evolution of computing power. This trajectory suggests that as computing capabilities advance, an increasing number of encryption-based methodologies are likely to transition from theoretical constructs to practical solutions for real-world applications.

IV. Location Privacy in Modern Applications

The rapid proliferation of Internet of Things (IoT) devices and the advancement of autonomous driving technology have catalyzed the emergence of a diverse range of innovative

location-based services. In the subsequent sections, we will delve into a selection of these contemporary applications. These include but are not limited to: leveraging Vehicular Ad-hoc Networks (VANETs) for efficient information dissemination, orchestrating intelligent traffic management for autonomous vehicles, and enabling robust virus contact tracing mechanisms.

In the context of these modern applications, safeguarding location privacy has become a paramount concern. As a response, novel privacy-preserving strategies are being employed, transcending the boundaries of conventional methods. One notable trend is the integration of cutting-edge technologies like blockchain into the realm of location privacy protection. This fusion of approaches not only reflects the dynamic nature of these new applications but also underscores the multifaceted efforts to ensure the confidentiality of location-based data in today's evolving technological landscape.

A. Location Privacy in Vehicular Ad-hoc Netoworks

The continuous advancements in self-driving and connected vehicles, along with the emerging concept of smart cities, offer a glimpse of a dramatically different transportation future [47]. Envisioning a smart city where vehicles are equipped with autonomous driving systems, the potential to completely eradicate traffic jams becomes a reality through seamless, coordinated traffic planning, enabling autonomous cars to smoothly navigate at high speeds without collisions [48]–[51]. While the transition to smart cities may require time, the immense benefits of highly efficient transportation make it imperative to start studying various algorithms and strategies needed for this transformation which include the critical security and privacy issues.

The coordination among vehicles requires the establishment of a trust relationship [52]–[55] which in turn may give away individual vehicle's location privacy. Existing works on privacy preservation in VANETs focus on anonymizing vehicle identities. By keeping their identities anonymous, the vehicles also achieve location privacy. One common approach is to enable vehicles to use different pseudonyms during communication rather than using their real identities. An initial contribution in this particular field was made by Raya and Hubaux [56]. Their proposal involves a mechanism where a vehicle, when needing to sign a message, randomly selects a private key from an extensive collection of certificates issued by a central authority. The recipient of the message then verifies the authenticity of the sender's signature by validating the associated public key certificate. However, a notable drawback of this protocol is that during the verification of each received signed message, vehicles are required to examine an extensive list of revoked certificates. This process is inherently time-consuming. Later, various alternative pseudonym-based protocols have been developed [57]–[60]. These protocols offer differing levels of enhancement in addressing the challenge of key revocation. Nevertheless, a common aspect among most of these approaches is the necessity for the identity management authority to keep certificates linked to each vehicle. This enables the authority to recover the genuine identities of vehicles in cases of disputes. However, this practice also brings about a notable concern. The continuous maintenance of these certificates could potentially lead to the tracking of vehicle movements by the authority. Consequently, the fundamental issue of preserving the location privacy of the vehicles remains inadequately addressed in these protocols.

Another category of privacy preserving protocols is group-based [61], [62]. The core concept behind these protocols involves the utilization of group managers to organize and validate vehicles, thereby enabling vehicles to communicate anonymously within their respective groups. Many protocols in this category make use of a group signature scheme. Within this scheme, vehicles possess the ability to verify the authenticity of messages originating from valid group members, without gaining knowledge of the actual sender's identity. This inherent anonymity within groups is exemplified by the ECPP protocol introduced by Lu et al. [61], where Roadside Units (RSUs) act as group managers. These RSUs allocate group keys to passing vehicles. The security and privacy aspects of ECPP are subsequently enhanced by Jung et al. [62], whose protocol ensures both unlinkability and traceability even when multiple RSUs are compromised. Given the substantial computational burden associated with the group signature scheme, various techniques have been proposed to enhance efficiency. For instance, Hao et al. [63] present a distributed key management framework, and Wang et al. [64] introduce a decentralized certificate authority coupled with a biological-password-based two-factor authentication.

In addition to the group-based signature scheme, alternative techniques have been put forth to achieve anonymity within groups. For example, Zhang et al. [65] adopt the concept of k-anonymity to uphold user privacy. This ensures that a given vehicle remains indistinguishable from $k-1$ other vehicles. However, k-anonymity demands a minimum of k vehicles in close proximity, a requirement that may not always be feasible in regions with limited vehicle presence. In the work by Squicciarini et al. [66], a PAIM protocol is proposed, which dynamically forms groups through direct vehicle-to-vehicle communication. This protocol employs Pedersen commitment and secret sharing schemes to realize anonymous vehicle authentication.

In general, the group-based protocols have several notable disadvantages. Primarily, there is the concern that the group manager possesses comprehensive knowledge about the identities of group members, thereby enabling potential tracking capabilities. Secondly, the task of managing group updates and revoking membership can become prohibitively expensive due to the substantial number of vehicles involved and the rapid movement patterns exhibited by these vehicles. A third limitation arises from the inherent constraint that communication within these protocols is confined solely to group members. This, in turn, underscores the necessity for a robust and dynamic grouping algorithm, which currently remains a challenge. Furthermore, protocols reliant on infrastructure support, such as Roadside Units (RSUs), may encounter feasibility

challenges in real-world scenarios where RSUs are sparse and infrequently deployed. To address these concerns, the most latest techniques for preserving privacy of vehicles in VANETs employ homomorphic encryption and cloud servers that enable vehicles to self-generate random IDs and minimize the reliance on RSUs [67]–[69].

B. Location Privacy in Contact Tracing

Infectious diseases have posed a significant threat to public health for centuries. The COVID-19 pandemic, in particular, has demonstrated the devastating repercussions on human lives and economies. In response to the urgent need to mitigate the spread of highly contagious viruses like COVID-19, identifying and isolating individuals potentially exposed to the virus through contact tracing has become paramount. Since the inception of the pandemic, numerous efforts in privacy-preserving contact tracing have emerged [70].

The majority of these existing endeavors employ short-range wireless technologies like WiFi and Bluetooth to detect instances of human-to-human contact. However, these approaches share a common limitation: they may overlook indirect contacts that occur when an individual encounters residual virus particles after an infected person has departed the area. Because of the inherent design involving localized storage of direct encounter information on users' devices, this category of approaches encounters challenges when extending to identify indirect contacts or conducting comprehensive contact tracing queries using diverse location data collection methods (such as GPS or QR codes). An early illustration of these efforts is the EPIC system introduced by Altuwaiyan et al. [71]. In this system, the server calculates a matching score based on encrypted connection signals between users. Nonetheless, the encryption scheme utilized in this method is intrinsically computationally intensive. More recently, Trieu et al. [72] have proposed a Bluetooth-based approach named Epi-one, allowing users to exchange and store randomly generated tokens during close proximity interactions. In case a user tests positive, they inform the server, which then broadcasts a set of tokens associated with that user. Other users subsequently compare the tokens received from the server with their own collected tokens to assess potential exposure risk. Similarly, building on a comparable concept, Pinkas and Ronen [73] present the Hashomer system that relies on Bluetooth for detecting close contacts among users. This system records pseudo IDs of encounters within the application and enables health authorities to broadcast reported patient IDs to all users.

With the aim of granting users greater authority over their privacy, Song et al. [74] introduce the concept of self-sovereign identity. This notion empowers individuals to dictate when and under what circumstances they share their identities during interpersonal encounters. To enhance privacy protection even further, certain strategies eliminate the need for a central server and instead leverage blockchain techniques. For instance, Ahmed et al. [75] propose a mechanism where individuals who test positive for a disease can opt to upload their pseudo IDs to a blockchain. Subsequently, other users can query the blockchain to ascertain whether they have encountered any of the diagnosed patients. However, this approach necessitates users to proactively and consistently monitor the blockchain, a task that inevitably consumes time and energy.

It is important to note that the aforementioned human-to-human contact-based approaches may not be energy-efficient in large-scale settings without sacrificing users' location privacy. In cases where the server is unaware of a patient's region (e.g., city), broadcasting the patient's pseudo IDs to a large number of users throughout the country for self-checking may result in the unnecessary consumption of phone batteries for those who are geographically distant from the patient. To narrow down the range of users to be notified, the patient must be willing to surrender some location privacy by providing information such as the cities they have visited.

V. Open Challenges and Future Directions

In this section, we discuss the open challenges and potential future research directions.

A. Open Challenges

Providing location privacy protection for a single location-based service is no longer sufficient as attackers could make use of combined knowledge garnered from other services that pertain location information to infer the users' real locations. Thus, it is important to investigate all location-based services that a user has subscribed to in order to develop a holistic protection plan that prevents potential privacy breach caused by correlations of information from different services. An even more challenging task is to also look into the user's contacts who may have shared the user's location information online.

It is expected to take time for service providers to adopt privacy protection mechanisms. During the transitional period, users should have the necessary tools to sustain partial burden of the privacy protection of their own data.

Finally, there is still a huge gap between the theoretical solutions and the real-world implementations in terms of location privacy protection. To enable the wide adoption of the privacy protection mechanisms, it is important to bear in mind the efficiency and scalability as well as the feasibility and usability.

B. Future Directions

As discussed earlier, advancement in pervasive computing has fostered a new realm of location-based services especially those related to smart cities. We envision the possibly biggest platform for the next generation of LBS applications could be vehicular ad-hoc networks (VANETs) as it is the backbone of communication infrastructure in future smart cities. In this large scale and highly dynamic environment, preserving vehicle's location privacy would be on the top of the list to address participants privacy concerns when subscribing to the service.

For future VANET applications, robust and promising privacy preserving algorithms are likely to be developed using encryption-based approaches like blockchain and secure

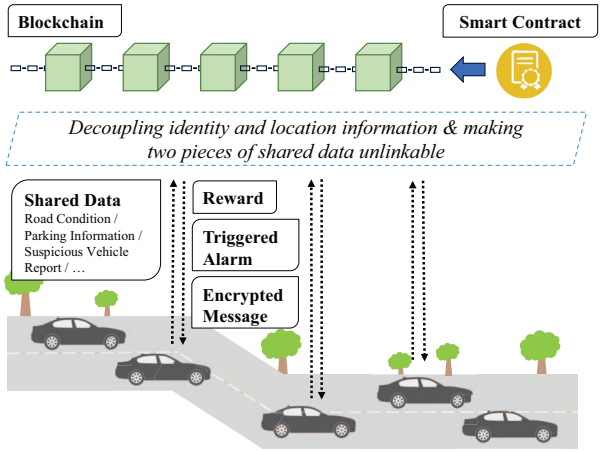

Fig. 2: Blockchain-based Location Privacy Protection Strategies

multiparty computation because they offer the undoubtedly strong privacy guarantee and their computational efficiency is improving constantly.

1) Blockchain-based Location Privacy Protection Strategies: To improve road safety and traffic management, one crucial aspect of the future VANET applications is the need for vehicles to share important information (e.g. road conditions and vehicle abnormal behaviors for road safety applications, parking information, and charging station information to enhance convenience and efficiency of the drivers, multi-media data for social sharing application, etc.) [47], [76]. To improve the usability and quality of the service, these applications ensure the precision of location information in the data shared by vehicles while preserving location privacy. The conventional location privacy-protecting methods, such as K-anonymity and regional cloaking methods, fall short of providing precise location data while preserving location privacy.

Moreover, to incentivize vehicles to actively participate in information sharing, it is imperative to introduce a reward system that necessitates the ability to prove ownership of the shared information. Additionally, the data shared, such as road conditions, and reports of misbehaviors, must remain immutable to ensure its integrity and prevent malicious tampering. Traditional centralized methods fall short in guaranteeing immutability while preserving location privacy, as they risk exposing the identity of the reporting vehicle and, in some cases, can link multiple reports to reveal the vehicle's trajectory.

To address these issues, we can leverage blockchain technology as a robust foundation and lay the foundation for secure and privacy-preserving data sharing in VANETs. As illustrated in Figure 2, first, when sharing a piece of information along with a precise location, vehicles can use randomized identifiers and transmit the information as a digital asset to the blockchain. It allows vehicles to prove ownership without revealing their real identities, thus unlinking the real identity and location to protect location privacy. Vehicles can generate new identifiers when sharing new information and only use the used identifiers to get the reward.

Second, in some application scenarios, we can also utilize smart contracts to trigger specific actions when predefined conditions are met (e.g. produce an alarm when the number of road hazard condition reports reaches a threshold, or trigger a transaction when a piece of information has been verified as valuable). By doing that, no centralized management unit is needed to collect and process user location information.

Third, in case of the application scenario that vehicles need to share information that is only accessible to a specific set of vehicles, we can further introduce more encryption methods, such as ciphertext policy attribute-based encryption (CP-ABE), on the blockchain so that only the vehicles with required attributes can decrypt the information.

By utilizing blockchain to decentralize the process, vehicles can provide only a minimized set of information and make it difficult for the attacker to link two pieces of shared information and reveal the location and trajectory of the vehicles.

2) Secure Multi-Party Computation Based Location Privacy Protection Strategies: As illustrated in Figure 3, secure multi-party computation could be employed to enhance VANET's traffic prediction, thereby facilitating optimal vehicle routing. This would involve utilizing secret sharing to calculate incoming car numbers for each Road-Side Unit and direction.

We could achieve this by employing vehicle grouping and designating a group leader. Each On-Board Unit would determine a one-hot vector indicating the next neighboring Road-Side Unit on the vehicles route. Subsequently, On-Board Units would divide the vector into shares, sending one share to the current Road-Side Unit and the other to the group leader. The group leader would send the sum of the shares received and their own location vector to the Road-Side Unit. Next, the Road-Side Unit will aggregate all received shares and reveal the result. Afterwards, the Road-Side Unit will possess a vector indicating the number of vehicles heading to each neighboring Road-Side Unit. The Road-Side Unit can then relay this information to the location service provider potentially improving short-term traffic prediction, more efficient traffic

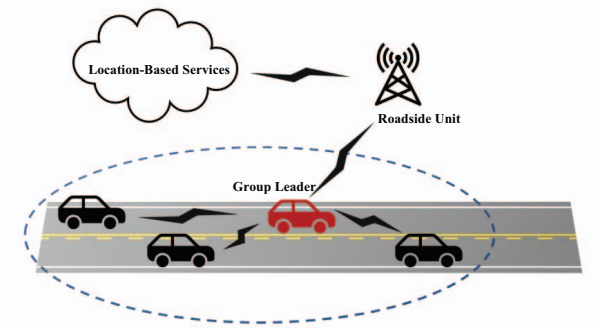

Fig. 3: Secure Multi-party Computation Based Location Privacy Protection Strategies

routing, and smart traffic light scheduling.

In considering the viability of this prospective work, some issues need to be addressed. Primarily, small groups of vehicles could weaken any privacy guarantees. Due to the risk of tracking individual vehicles along the route between the two RSUs if there are too few vehicles in the group. Additionally, the integrity of group leader would be crucial. This could potentially be mitigated by appointing multiple co-group leaders. On-Board Units would need to generate additional shares as the number of group leaders increased.

VI. Conclusion

In the booming era of pervasive computing, safeguarding location privacy requires a comprehensive approach. Protection must extend beyond individual services, considering potential data correlations and user contacts. While various location privacy protection algorithms have been proposed, the gap between theory and real-world implementation remains a challenge, demanding efficient, scalable, and user-friendly solutions. The quest for comprehensive and robust location privacy protection continues, uniting researchers, providers, and users in a collaborative journey.

Acknowledgments

This work is partially supported by NSF project DGE-1946619 and CNS-2301014.

References

[1] MarketsandMarkets, "Location-based services and real-time location systems market by component, location type, application, vertical and region - global forecast to 2027," *https://www.marketsandmarkets.com/Market-Reports/location-based-service-market-96994431.html*, 2023.

[2] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the international conference on Mobile systems, applications and services*, 2003, pp. 31–42.

[3] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructures," in *Proc. Workshop on Privacy Enhancing Technologies*, 2006.

[4] M. F. Mokbel, C. Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. VLDB*, 2006, pp. 763–774.

[5] T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in *Proceedings of the ACM conference on Computer and communications security*, 2009, pp. 348–357.

[6] M. K. Domenic, Y. Wang, F. Zhang, I. Memon, and Y. H. Gustav, "Preserving users' privacy for continuous query services in road networks," in *International Conference on Information Management, Innovation Management and Industrial Engineering*, 2013, pp. 352–355.

[7] X. Ju and K. G. Shin, "Location privacy protection for smartphone users using quadtree entropy maps," *Journal of Information Privacy and Security*, vol. 11, no. 2, pp. 62–79, 2015.

[8] F. Abbas and H. Oh, "A step towards user privacy while using location-based services." *JIPS*, vol. 10, no. 4, pp. 618–627, 2014.

[9] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Location privacy in moving-object environments," *Transactions on Data Privacy*, 2009.

[10] ——, "Position transformation: a location privacy protection method for moving objects," in *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, 2008, pp. 62–71.

[11] B. Niu, X. Zhu, H. Chi, and H. Li, "3plus: Privacy-preserving pseudo-location updating system in location-based services," in *IEEE Wireless Communications and Networking Conference*, 2013, pp. 4564–4569.

[12] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *IEEE INFOCOM*, 2014, pp. 754–762.

[13] M. Xue, Y. Liu, K. W. Ross, and H. Qian, "I know where you are: thwarting privacy protection in location-based social discovery services," in *IEEE Conference on Computer Communications Workshops*, 2015, pp. 179–184.

[14] H. Zhang, Z. Xu, X. Yu, and X. Du, "Lpps: Location privacy protection for smartphones," in *IEEE International Conference on Communications*, 2016, pp. 1–6.

[15] F. Fei, S. Li, H. Dai, C. Hu, W. Dou, and Q. Ni, "A k-anonymity based schema for location privacy preservation," *IEEE Transactions on Sustainable Computing*, 2017.

[16] T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.

[17] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," *IEEE Access*, vol. 4, pp. 673–687, 2016.

[18] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services," in *INFOCOM 2017*, 2017, pp. 1–9.

[19] S. Hayashida, D. Amagata, T. Hara, and X. Xie, "Dummy generation based on user-movement estimation for location privacy protection," *IEEE Access*, vol. 6, pp. 22 958–22 969, 2018.

[20] J. Kang, D. Steiert, D. Lin, and Y. Fu, "Movewithme: Location privacy preservation for smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 711–724, 2020.

[21] M. Ghasemzadeh, B. C. M. Fung, R. Chen, and A. Awasthi, "Anonymizing trajectory data for passenger flow analysis," *Transportation Research Part C*, vol. 39, pp. 63–79, 2014.

[22] P.-I. Han and H.-P. Tsai, "SST: Privacy Preserving for Semantic Trajectories," *2015 16th IEEE International Conference on Mobile Data Management*, vol. 2, pp. 80–85, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7264377

[23] G. Poulis, S. Skiadopoulos, G. Loukides, and A. Gkoulala-Divanis, "Select-organize-anonymize: A framework for trajectory data anonymization," *Proceedings - IEEE 13th International Conference on Data Mining Workshops, ICDMW 2013*, pp. 867–874, 2013.

[24] G. Poulis, S. Skiadopoulos, G. Loukides, and A. Gkoulalas, "Apriori-based algorithms for k m -anonymizing trajectory data," *Transactions on Data Privacy*, vol. 7, no. 2, pp. 165–194, 2014.

[25] G. Poulis, S. Skiadopoulos, G. Loukides, and A. Gkoulalas-Divanis, "Distance-based km-anonymization of trajectory data," *Proceedings - IEEE International Conference on Mobile Data Management*, vol. 2, pp. 57–62, 2013.

[26] M. E. Nergiz, M. Atzori, Y. Saygin, and B. Guc, "Towards Trajectory Anonymization A Generalization Based Approach," *Transactions on Data Privacy*, vol. 2, no. 106, pp. 47–75, 2009.

[27] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," *Proceedings of the 1st international conference on Mobile systems applications and services MobiSys 03*, no. 3, pp. 31–42, 2003.

[28] R. G. Pensa, A. Monreale, F. Pinelli, and D. Pedreschi, "Pattern-preserving k-anonymization of sequences and its application to mobility data mining," *CEUR Workshop Proceedings*, vol. 397, pp. 44–60, 2008.

[29] S. Gurung, D. Lin, W. Jiang, A. Hurson, and R. Zhang, "Traffic Information Publication with Privacy Preservation," *ACM Trans. Intell. Syst. Technol.*, vol. 5, no. 3, pp. 1–26, 2014.

[30] D. Lin, S. Gurung, W. Jiang, and A. Hurson, "Privacy-preserving location publishing under road-network constraints," in *Database Systems for Advanced Applications*, 2010, pp. 17–31.

[31] K. Ward, D. Lin, and S. Madria, "Melt: Mapreduce-based efficient large-scale trajectory anonymization," in *Proceedings of the 29th International Conference on Scientific and Statistical Database Management*, 2017, pp. 1–6.

[32] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," *arXiv preprint arXiv:1212.1984*, 2012.

[33] Z. Chen, X. Hu, X. Ju, and K. G. Shin, "Lisa: Location information scrambler for privacy protection on smartphones," in *IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 296–304.

[34] Q. Xiao, J. Chen, L. Yu, H. Li, H. Zhu, M. Li, and K. Ren, "Poster: Locmask: A location privacy protection framework in android system,"

in *Proceedings of the ACM SIGSAC conference on computer and communications security*, 2014, pp. 1526–1528.
[35] H. Ngo and J. Kim, "Location privacy via differential private perturbation of cloaking area," in *Computer Security Foundations Symposium*, 2015, pp. 63–74.
[36] L. Wang, D. Yang, X. Han, T. Wang, D. Zhang, and X. Ma, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proceedings of the International Conference on World Wide Web*, 2017, pp. 627–636.
[37] W. Wang and Q. Zhang, "A stochastic game for privacy preserving context sensing on mobile phone," in *IEEE INFOCOM*, 2014, pp. 2328–2336.
[38] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the ACM SIGMOD international conference on Management of data*, 2008, pp. 121–132.
[39] K. P. Puttaswamy and B. Y. Zhao, "Preserving privacy in location-based mobile social applications," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, 2010, pp. 1–6.
[40] Y. Huang, P. Chapman, and D. Evans, "Privacy-preserving applications on smartphones." in *HotSec*, 2011.
[41] W. Wei, F. Xu, and Q. Li, "Mobishare: Flexible privacy-preserving location sharing in mobile online social networks," in *Proceedings IEEE INFOCOM*, 2012, pp. 2616–2620.
[42] S. Guha, M. Jain, and V. N. Padmanabhan, "Koi: A location-privacy platform for smartphone apps," in *Proceedings of theUSENIX conference on Networked Systems Design and Implementation*, 2012, pp. 14–14.
[43] X.-Y. Li and T. Jung, "Search me if you can: privacy-preserving location query service," in *Proceedings of IEEE INFOCOM*, 2013, pp. 2760–2768.
[44] K. P. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. El Abbadi, C. Kruegel, and B. Y. Zhao, "Preserving location privacy in geosocial applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 159–173, 2014.
[45] R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, "Privacy-preserving and content-protecting location based queries," *IEEE transactions on knowledge and data engineering*, vol. 26, no. 5, pp. 1200–1210, 2014.
[46] H. Zhu, F. Liu, and H. Li, "Efficient and Privacy-Preserving Polygons Spatial Query Framework for Location-Based Services," *IEEE Internet of Things Journal*, vol. 4, pp. 536–545, 2017.
[47] J. Kang, D. Lin, E. Bertino, and O. Tonguz, "From autonomous vehicles to vehicular clouds: challenges of management, security and dependability," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 1730–1741.
[48] D. Lin, J. Kang, A. Squicciarini, Y. Wu, S. Gurung, and O. Tonguz, "Mozo: A moving zone based routing protocol using pure v2v communication in vanets," *Ieee transactions on mobile computing*, vol. 16, no. 5, pp. 1357–1370, 2016.
[49] S. Gurung, A. Squicciarini, D. Lin, and O. K. Tonguz, "A moving zone based architecture for message dissemination in vanets," in *2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm)*. IEEE, 2012, pp. 184–188.
[50] J. Kang and D. Lin, "Highly efficient traffic planning for autonomous vehicles to cross intersections without a stop," *ACM Transactions on Intelligent Systems and Technology*, vol. 14, no. 2, pp. 1–24, 2023.
[51] ——, "Dash: A universal intersection traffic management system for autonomous vehicles," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2020, pp. 89–99.
[52] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Network and System Security: 7th International Conference, NSS 2013, Madrid, Spain, June 3-4, 2013. Proceedings 7*. Springer, 2013, pp. 94–108.
[53] S. Karumanchi, A. Squicciarini, and D. Lin, "Selective and confidential message exchange in vehicular ad hoc networks," in *International Conference on Network and System Security*. Springer, 2012, pp. 445–461.
[54] H. Cui, R. H. Deng, and G. Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 721–733, 2019.
[55] T. Wang, L. Kang, and J. Duan, "Dynamic fine-grained access control scheme for vehicular ad hoc networks," *Computer Networks*, vol. 188, p. 107872, 2021.
[56] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," in *Journal of Computer Security*, 2007, pp. 39–68.
[57] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking together efficient authentication, revocation, and privacy in vanets," in *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*. IEEE, 2009, pp. 1–9.
[58] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.
[59] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, pp. 1851–1865, 2011.
[60] J. Li, H. Lu, and M. Guizani, "Acpn: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.
[61] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, 2008, pp. 1229–1237.
[62] C. D. Jung, C. Sur, Y. Park, and K.-H. Rhee, "A robust conditional privacy-preserving authentication protocol in vanet," *Social Informatics and Telecommunications Engineering*, vol. 17, pp. 35–45, 2009.
[63] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in vanets," *IEEE Journal on selected areas in communications*, vol. 29, no. 3, pp. 616–629, 2011.
[64] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.
[65] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 246–250.
[66] A. Squicciarini, D. Lin, and A. Mancarella, "Paim: Peer-based automobile identity management in vehicular ad-hoc network," in *Proc. of the IEEE Computer Software and Applications Conference (COMPSAC)*, 2011.
[67] J. Kang, Y. Elmehdwi, and D. Lin, "Slim: Secure and lightweight identity management in vanets with minimum infrastructure reliance," in *Security and Privacy in Communication Networks: 13th International Conference, SecureComm 2017, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13*. Springer, 2018, pp. 823–837.
[68] W. Jiang, F. Li, D. Lin, and E. Bertino, "No one can track you: Randomized authentication in vehicular ad-hoc networks," in *2017 IEEE international conference on pervasive computing and communications (Percom)*. IEEE, 2017, pp. 197–206.
[69] J. Kang, D. Lin, W. Jiang, and E. Bertino, "Highly efficient randomized authentication in vanets," *Pervasive and Mobile Computing*, vol. 44, pp. 31–44, 2018.
[70] Q. Tang, "Privacy-preserving contact tracing: current solutions and open questions," 2020.
[71] T. Altuwaiyan, M. Hadian, and X. Liang, "Epic: Efficient privacy-preserving contact tracing for infection detection," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.
[72] N. Trieu, K. Shehata, P. Saxena, R. Shokri, and D. Song, "Epione: Lightweight contact tracing with strong privacy," 2020.
[73] B. Pinkas and E. Ronen, "Hashomer – privacy-preserving bluetooth based contact tracing scheme for hamagen," 2021.
[74] W. Song, R. N. Zaeem, D. Liau, K. C. Chang, M. R. Lamison, M. M. Khalil, and K. S. Barber, "Self-sovereign identity and user control for privacy-preserving contact tracing," 2018.
[75] N. Ahmed, R. A. Michelin, W. Xue, G. D. Putra, S. Ruj, S. S. Kanhere, and S. Jha, "Dimy: Enabling privacy-preserving contact tracing," 2021.
[76] J. Kang, A. Yu, W. Jiang, and D. Lin, "Nwade: A neighborhood watch mechanism for attack detection and evacuation in autonomous intersection management," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2022, pp. 1190–1200.