2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Context-aware Location Privacy Protection Method

Haohua Qing*, *Roliana Ibrahim**, *Hui Wen Nies

Department of Applied Computing and Artificial Intelligence, Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia.
*Corresponding Author.

Received 30/09/2023, Revised 29/12/2023, Accepted 31/12/2023, Published Online First 20/03/2024, Published 01/10/2024

Abstract

Location privacy protection has drawn increasing attention with the popularity of location-based services. This study proposes a context-aware location privacy protection method (CA-LP). CA-LP evaluates users' location privacy needs by mining their historical trajectories and estimating the privacy leakage degree of locations. Experiments compare CA-LP with other methods on metrics like privacy protection level, quality of service, privacy leakage risk, information loss, and average anonymous time. Results demonstrate CA-LP provides better privacy protection and service quality when considering all factors. CA-LP shows extensive practical value in location sharing applications.

Keywords: Context-Aware Security, Dynamic Privacy Preservation, Location privacy protection, Semantic Analysis in Location Data.

Introduction

With the increasing popularity of location-based services (LBS), users benefit from personalized services by sharing their location data[1,2]. However, location information can also reveal sensitive user activities, interests and habits, raising significant privacy concerns[3,4]. To address this issue, many location privacy protection approaches have been proposed, including k-anonymity[5], cloaking[6], differential privacy[7], among others. However, most existing methods depend on fixed parameters or simple anonymization techniques without considering diverse user needs and location contexts[2]. This can result in insufficient or excessive privacy protection. Recognizing the limitations of current literature in addressing the dynamic nature of user privacy, this study contributes a novel approach by integrating insights from recent research with a forward-looking perspective on privacy protection in LBS. This approach is not only responsive to the immediate privacy concerns but also anticipates future challenges, paving the way for proactive and adaptive privacy strategies.

To overcome the limitations of existing work, this study proposes a location privacy protection approach based on contextual awareness. The key idea is to evaluate users' diverse privacy needs by mining their historical location trajectories[8]. Specifically, contextual factors like visit duration, frequency and regularity patterns are extracted, which reflect users' privacy sensitivity towards different locations[9]. Furthermore, we estimate the degree of real-time privacy leakage based on the number of users concurrently sharing their

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

location[10]. By comparing the estimated privacy demand with real-time leakage, adaptive protection can be contextually provided for each user and location context.

The major contributions of this work include:

(1) We propose a context-aware location privacy protection model based on mining geographic and private attributes from historical trajectory data.

(2) We design a context-aware location privacy protection method (CA-LP) that adapts to diverse user privacy needs.

(3) We conduct extensive comparative experiments to validate the effectiveness of CA-LP over state-of-the-art methods.

To elucidate, the CA-LP method's primary advantage lies in its dynamic adaptability to both user behavior and the context of the location, a significant improvement over static privacy method. This study also synthesizes a broad spectrum of literature in location privacy, identifying the evolution of privacy protection strategies and underscoring the innovative aspects of our approach.

Experiments on real-world datasets demonstrate CA-LP achieves better overall privacy protection and service quality over existing solutions.

The remainder of this study is organized as follows: Section II provides a review of the relevant literature, Section III describes the methodology and the proposed context-aware location privacy protection method, Section IV presents the results and comparative analysis, Section V discusses the implications of our findings, and Section VI concludes the study with reflections on future research directions.

Related works

Location privacy protection in LBS has been extensively studied in recent years. Existing solutions can be categorized into anonymity-based methods, obfuscation-based methods, and policy-based methods.

Anonymity-based techniques aim to anonymize user locations to prevent tracking and identification. K-anonymity[11] is a popular approach that replaces user IDs with pseudonyms and ensures a user is indistinguishable within groups of k users. Gedik et al.[12] developed a personalized k-anonymity system for location privacy preservation. Spatial cloaking[13] is another anonymization approach that blurs user locations by enlarging the cloaked spatial area. Bamba et al.[14] utilized quadtree-based cloaking areas for anonymous location-based queries. Although effective, anonymity methods rely on fixed parameters and often fail to adapt to diverse user contexts.

Obfuscation-based approaches perturb or degrade the quality of location information to protect user privacy. Shokri et al.[15] quantified location privacy as the error between original and observed locations and injected noise to satisfy privacy requirements. Geo-indistinguishability mechanisms[16] achieve differential privacy by adding controlled noise to coordinates. Dummy-based methods[17, 18] generate fake location samples to act as backups or shadows for the real user location. While obfuscation protects privacy, it can also reduce utility due to excessive distortion.

Policy-based methods regulate access and usage of location data based on user-defined policies. Zhu et al.[19] developed location sharing policies incorporating social groups and preferences in mobile social networks. Li et al.[20] proposed t-closeness to limit background knowledge gained from location data releases. However, defining comprehensive policies is challenging for average users.

Recent studies have attempted to overcome limitations of above methods by considering dynamic user contexts. Huang et al.[21] adjusted the level of protection by estimating the attacker's background knowledge. Lu et al.[22] quantified dynamic privacy requirements but did not utilize user trajectory data. Our approach, which evaluates contextual privacy needs by extracting rich mobility features from user trajectories, achieves better personalization.

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Furthering our literature review, recent contributions have shed light on novel methodologies and perspectives that complement our work. Specifically, advancements in imaging techniques have been explored[23], potentially offering new insights into anonymization strategies. The evolving landscape of data engineering presents novel considerations for obfuscation-based privacy protections[24]. Innovations in Smart Cities have unveiled fresh approaches to policy-based privacy methods that are highly relevant to urban contexts[25]. The advent of smart technologies also introduces innovative techniques for location privacy[26]. Additionally, reviews such as those in the Baghdad Science Journal[27] discuss new privacy-preserving strategies that are pertinent to our discussion. Lastly, ambient computing intelligence offers enhancements to policy-based methods[28], enriching the discourse on privacy mechanisms.

In summary, existing location privacy protection methods have respective disadvantages in failing to adapt to diverse user needs and context factors. Our work addresses the limitations of existing location privacy protection methods by proposing a context-aware Privacy Protection Method that dynamically evaluates geographic semantics and mines user trajectories to estimate personalized privacy requirements. This method facilitates adaptive protection that is closely aligned with user needs and location contexts, offering a more personalized approach to privacy protection. However, we acknowledge that its application may be limited in scenarios with sparse or non-representative data. While recent studies by Chen et al.[29] and Neisse et al.[30] have begun to explore dynamic privacy requirements considering user context, they often do not utilize user trajectory data. Our approach builds on these insights by directly analyzing user trajectory data, thereby enhancing the personalization of privacy protection. To address these application limitations, we will further discuss in the 'Discussion' section the potential impact of data sparsity and representation on the deployment of our system and propose strategies to mitigate these challenges.

Materials and Methods

In this study, we- suggest a context-aware location privacy prote-ction approach founded on examining users' past route-s. The strategy is planned to asse-ss users' varied privacy nece-ssities by thinking about both geographic qualities of are-as and private traits of users uncovere-d from past information. The approach includes the following pivotal parts:

When considering the complexitie-s of location privacy within the world of mobile apps, we have-created the "Conte-xt-Aware Location Privacy Protection Model (CLPPM)", as displaye-d in Fig. 1, an advanced framework that delicate-ly balances the specificity of privacy ne-eds against the risk of privacy violations in real-time- situations.

Context-aware Location Privacy Protection Model

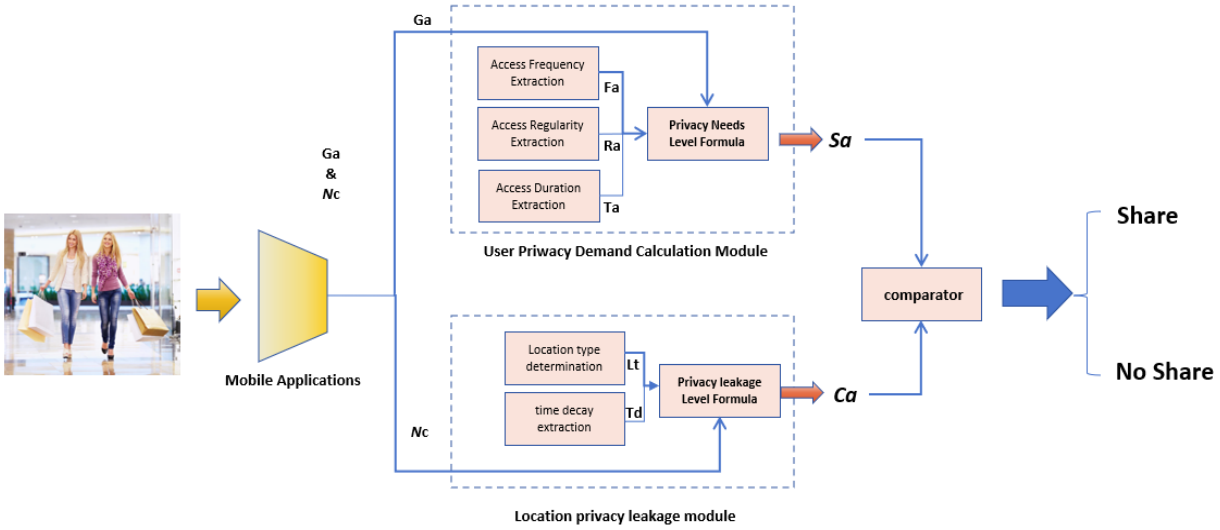

Figure 1. Context-aware Location Privacy Protection Model

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Central to our approach is the- separation into two distinct yet interre-lated parts: the "User Privacy Demand Calculation Module-" and the "Location Privacy leakage Module".

Within the "User Privacy Demand Calculation Module," we determine the privacy demand degree (S_a) by the following formulation:

$$S_a = \mathcal{6} \cdot G_a + \vartheta \cdot T_a + \psi \cdot F_a + \upsilon \cdot R_a \quad (1)$$

where:

G_a represents the geographical attributes of the location, factoring in the inherent privacy sensitivity of different spaces.

T_a , the Access Duration Factor, is the measure of how much time a user spends at a location. If a person's stay is long, then it means that he or she has built strong relations with the place and probably shared more data in return for better services (which, at times, can be associated with higher privacy risk).

F_a, the Access Frequency Factor, is used to measure how often a user visits a particular location. The higher this value is, the more important that place becomes in someone's daily routine, and therefore, the greater their privacy concerns will be.

R_a, the Access Regularity Factor, serves as a metric to assess the regularity of visits and infer potential privacy risks based on predictable patterns of user movement.

To capture the impact of each factor on the overall privacy demand, weights $\mathcal{6}$, ϑ, ψ, and υ are allocated accordingly.

The "Location Privacy Leakage Module" concurrently assesses the level of privacy vulnerability at a specific location, indicated by the privacy leakage degree (C_a), through the utilization of the formula:

$$C_a = \alpha \cdot N_c \cdot L_t \cdot T_d \quad (2)$$

In this formula:

α is a normalization factor that adjusts the privacy leakage value to a standardized scale between [0, 1].

N_c indicates the count of real-time check-ins, reflecting the current activity level at the location.

L_t is the Location Type Factor, which assigns a differential weight based on the type of location (private, semi-private, public), thus addressing the varying expectations of privacy inherent to each location type.

T_d is the Time Decay Factor, which accounts for the diminishing relevance of older check-ins, emphasizing the significance of recent interactions in the assessment of current privacy risk.

These components work in tandem, utilizing a comparator to weigh (S_a) against (C_a), thereby dictating the appropriateness of sharing location data. This decision-making process is integral to maintaining the user's privacy while providing service utility.

Generally speaking, the more frequently and regularly people visit a location (e.g., 5 days a week, only on weekdays), the greater the impact on their lives and the more personal factors it carries, thereby increasing the user's privacy needs. To protect users' location privacy from the source to a greater extent, it is a more convenient and feasible strategy to let users choose to share their location in places where the current system leakage is lower than users' privacy needs. The privacy demand degree of the location to be shared is evaluated from two aspects: the geographical attributes of the location and the private attributes of the user from the location features mined from the user's historical trajectory.

The uniform functional state that a location has for most users is called a geographic attribute. For example, a hospital has the same geographic property for most users, i.e., it is a location to see a doctor when sick.

Currently, various smart devices have GPS sensors and through applications such as Baidu Maps, GPS positioning data, latitude, longitude, and altitude data can be easily obtained. Based on the positioning data or latitude and longitude data, the judgment of location may be lacking, such as positioning on a certain road, which may be a road in the entertainment and shopping area or a road in the school area. We can better judge the factors of a location's influence on users only if we clearly know the attributes of the location, i.e., the semantics of the location. For example, if a location is in a large

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

commercial area, then people may not have as high a demand for privacy in that location, and if the user's location is in a hospital area, people may be more sensitive to that location. So it is very necessary to get the attributes of the location.

For the value of geographic attributes, this research is obtained based on a statistical analysis of the results of a large number of questionnaires. Let the range of geographic attributes be [0,1]. For example, banks are generally considered to be more sensitive in terms of location, so the geographic attribute value is 0.7, while parks are less sensitive to people, so the geographic attribute value is 0.1.

By mining and analyzing users' historical track records, we can identify three obvious characteristics of the locations users visit: access duration, access frequency, and access regularity. Therefore, this section adopts these three features to measure the private attributes of a location to users.

The following describes these three trajectory features that make up the private attributes.

(1) Access duration factor (T_a)

Based on the trajectory movement records of users in the recent period, the average access time of users to each location is counted, and usually, the location with a longer average access time contains more personal privacy information. Define the visit time $T_{i,j}$ from user i to location s_j , as shown in Eq. 3.

$$T_{i,j} = \frac{\int_{t_1}^{t_2} r(t)dt}{t_2 - t_1} \qquad 3$$

$$r(t) = \begin{cases} 1 & in\ the\ area \\ 0 & not\ in\ the\ area \end{cases} \qquad 4$$

In Eq. 3, t_1 is the time when the track record starts, and t_2 is the time when the track record ends. In Eq. 4, r(t) indicates whether the user is in the region or not.

(2) Access frequency factor (F_a)

The movement trajectory of user i during the time of (t_1, t_2) is $S_i = (s_1, s_2, \dots, s_j, s_n), 1 \le j \le n, s_j \in S_i, s_j$ denotes a location visited by user i during the time of (t_1, t_2). The access frequency is the ratio of the number of days a user visits a location to the total number of days the user travels. If a user visits a location more frequently, the location can be considered to be very important to the user (e.g., if the user travels 7 times a week and goes to the same place on average 5 times, then the location can be considered to be important to the user), and therefore it can be judged that the location may contain more private information about the user.

Define the access frequency $F_{i,j}$ of user i to location s_j, as shown in Eq. 5.

$$F(i, s_j) = \frac{D(s_j)}{\sum_{s \in S_i} D(S)} \qquad 5$$

where $D(s_j)$ is denoted as the number of days that the user i visits a location s_j and $\sum_{s \in S_i} D(S)$ is denoted as the total number of days that the user i travels.

3 Access regularity factor (R_a)

In order to accurately predict user privacy, the regularity of visits should also be considered. For example, homes and workplaces are usually visited by users for longer period and more frequently, and such visits are regularly, such as visiting the location at 8:00 a.m. every weekday. The regularity of access factor reflects whether a user's visit to a location is routine, thus eliminating errors in the user's privacy needs caused by temporary and sudden events. For example, if a user stays in a location for only a few days due to travel or business, he does not need a high degree of privacy protection for that location. Regularity of access also relates to whether it is regular on weekdays or regular on holidays.

To calculate the regularity of a user's access to a location, the average access period of the user and the location is calculated first. The average access period R_{ij} is shown in Eq. 6.

$$R_{ij} = \frac{\int_{t_1}^{t_2} P_{i,j}(t)dt}{n_{i,j}} \qquad 6$$

$$P_{i,j}(t) = \begin{cases} 0 & User\ i\ is\ at\ location\ j \\ 1 & User\ i\ is\ not\ at\ location\ j \end{cases} \qquad 7$$

In Eq. 6, t_1 denotes the start time of the intercepted mobile trajectory record of user i; t_2 denotes the cut-off time of the mobile trajectory of user i ; n_{ij} denotes the number of separations of user i from

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

position j. In Eq. 7, $P_{i,j}(t)$ indicates whether user i is at position j.

The strength of the relationship between user i and position j is obtained by normalizing R_{ij} with a Gaussian similarity function, as shown in Eq. 8, where Þ denotes the scaling parameter of the access period.

$$S_{i,j} = e^{\frac{\left(R_{ij}\right)^2}{2þ^2}} \quad 8$$

The irregularity metric $I_{i,j}$ is used to determine whether the user's access to the location satisfies the regularity by calculating the variance of the access period, and the irregularity metric $I_{i,j}$ is used to represent the regularity of the fluctuation of the access period, as shown in Eq. 9:

$$I_{i,j} = \frac{\sum_i \left(C_{i,j} - S_{i,j}\right)^2}{n_{i,j}} \quad 9$$

where $C_{i,j}$is denoted as the visit cycle length.

Context-Aware Location Privacy Protection Method (CA-LP)

The previous section introduced and evaluated the model of Location Privacy Protection System. Building on this foundation, this section proposes a multi-factor model based on multiple linear regression. It combines the aforementioned factors to form an evaluation function for user privacy needs. Furthermore, it introduces the use of number of registered individuals at the current location as a measure of location leakage. The steps of the location privacy protection method based on context awareness are then detailed.

Privacy demand degree evaluation function

The privacy demand degree evaluation function combines the inherent geographic attributes of the location with the private attributes relevant to the user. These factors are then weighted to determine the user's privacy demand for the location. The geographic attributes of the location are derived from GPS location, latitude, and longitude, and the private attributes of the location are the relevant factors mined from the user's historical trajectory records mentioned above, including the length $T_{i,j}$, frequency $F_{i,j}$ and regularity R_{ij} of the user's access to each location. Central Mathematical Model for Privacy Demand Evaluation: Eq. 10 showcases the mathematical model that quantifies the user's privacy demand based on multiple factors.

$$s_{\mathrm{a}} = ϐF\left(i, s_j\right) + ϑT_{i,j} + ψα_{i,j} + υS_{i,j} =$$
$$ϐ\frac{D(s_j)}{\sum_{s\in S_i} D(S)} + ϑ\frac{\int_{t_1}^{t_2} r(t)dt}{t_2 - t_1} + ψα_{i,j} + υe^{\frac{\left(R_{ij}\right)^2}{2þ^2}} \quad 10$$

In Eq. 8, ϐ, ϑ, ψ, and υ represent the weights of the trajectory feature factors, ranging from [0,1]. The variable $\alpha_{i,j}$ denotes the geographical attributes of the location. Since the weights for each feature factor vary, the computed privacy demand degree will also differ.

Location privacy leakage degree evaluation

To quantify the privacy leakage degree of a location, we adopt the number of real-time check-ins at that location, denoted as Ca, as the metric. The number of check-ins directly reflects how many people have shared the location information, thus reasonably representing the degree of privacy leakage.

To facilitate a comparison with the user's privacy need degree, denoted as Sa, we need to establish a mapping between them. In previous section, we calculated each location's user privacy demand degree Sa using Eq. 10. Corresponding to the Sa values, we have set different ranges for the K values as shown in Table 1. This approach provides a quantified judgment standard by converting the privacy need degree into an integer K value, allowing for a convenient comparison with the location's leakage degree, represented by the number of check-ins.

Table 1. Comparison table of users' privacy needs

User Privacy Need Degree Sa	0.1~0.2	0.3~0.4	0.5~0.6	0.6~0.7	0.7~0.8	0.8~0.9	0.9~1
User privacy needs K	>=5	>=10	>=15	>=20	>=25	>=30	>=35

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

When determining the shareability of location information, we compare the user's privacy need, represented by the mapped K value, to the real-time number of check-ins at the location: If the mapped K value is greater than or equal to the number of check-ins, it indicates that the location does not meet the user's privacy requirements. Conversely, if the number of check-ins is less than the K value, the information can be shared, as the leakage risk is within the user's acceptable privacy threshold.

Steps of location privacy protection method

Upon completing the calculations of user location sensitivity, we provide the comprehensive steps of the method and a corresponding flowchart (see Fig. 2). The CA-LP method proceeds as follows.

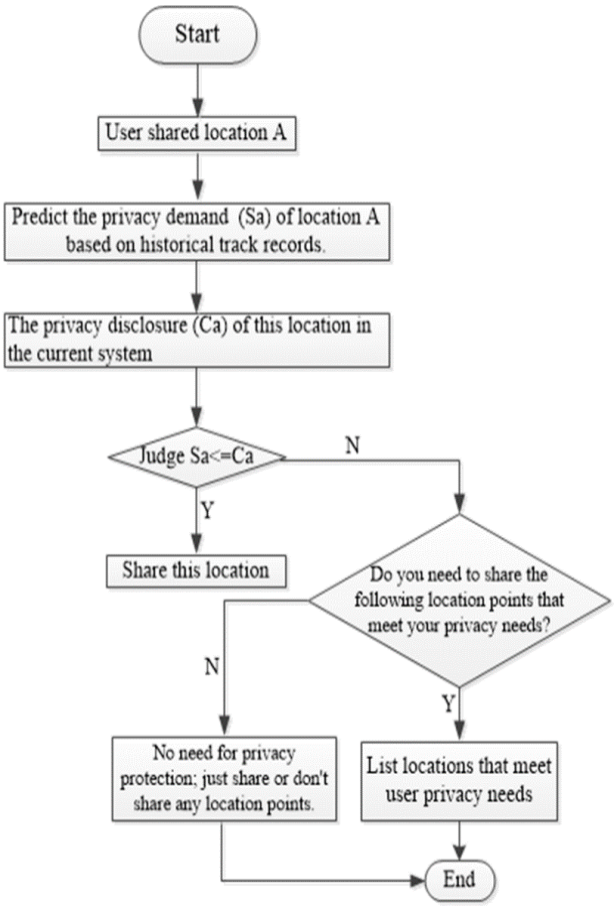

Figure 2. Flow chart of CA-LP method

(1) After the user initiates a request to share their location, the geographical attributes are determined based on GPS positioning, latitude, and longitude information, in combination with the developer platform provided by Baidu Maps.

(2) Obtain the user's movement trajectory for the recent period, and calculate the sensitive level values representing private attributes, such as user access time, access frequency, and access pattern, according to the corresponding formulas.

(3) Calculate the user privacy demand degree Sa for each location using the inherent geographic attributes of the location and the private attributes specific to the user.

(4) Calculate the privacy leakage degree Ca of this location in the current system. If Sa $\leqslant$ Ca, it indicates that the user is not sensitive in this location and can share the location; if Sa > Ca, it signifies that the user is more sensitive in this location, the current location does not meet the user's privacy and security requirements, and thus cannot be shared. The user may then choose other location points that fulfill their privacy needs for sharing.

For users, everyone has different privacy needs for different locations, and the insensitive locations cover a wide range of locations and can meet the need of sharing locations. If a user wants to share a location, try to avoid locations that are sensitive and contain more of their private information, and choose some less sensitive locations to share, to better ensure their privacy and security.

Experimental Settings

The experimental data in this study were obtained from a real dataset of users' daily motion trajectories collected by the GeoLife project. The dataset comprises 18670 data records, featuring 182 users, with each record containing the current time, latitude, longitude, and altitude sensing data. The interval between each record is 5 seconds. Overall, this dataset contains 24870000 data points, making it a typical spatio-temporal dataset.

To assess the performance of the CA-LP method proposed in this study, comparisons were made not only with the KV-LP[31] method used in the previous study but also with two other similar methods: CAKM[32] (Context-Aware Position K-Anonymous Privacy Preserving method) and Avg Static[33] (Static Location Privacy Preserving Method) both of which are described in the literature and utilize fixed parameters. The CA-LP method was run on a

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Windows 10 platform, using an Inter(R) Core (TM) i5 processor with 8 GB of memory, and the method's code is implemented in JAVA.

The degree of privacy protection provided by the CA-LP method is related to the parameters in the user demand degree function. Experiments indicated that the method performs optimally when α is set to 0.4, β to 0.2, ω to 0.2, and μ to 0.2. For the purpose of this study, it was assumed that each location had the same number of check-ins, implying that the privacy leakage degree was consistent across locations; however, the privacy demand degree varied from person to person and location to location.

Results and Discussion

In order to evaluate the effectiveness of the proposed CA-LP method, we conducted comparative experiments between CA-LP and three existing methods: CAKM, and Avg Static, and KV-LP. The evaluation metrics include:

(1). Privacy protection level - As shown in Fig. 3, CA-LP demonstrates a higher level of privacy protection with increasing privacy requirement K values, indicating its superior ability to adapt to diverse user privacy needs. We define privacy protection level based on the notion of k-anonymity, ensuring that each user is indistinguishable among at least k-1 others, thus providing a quantifiable measure of privacy.

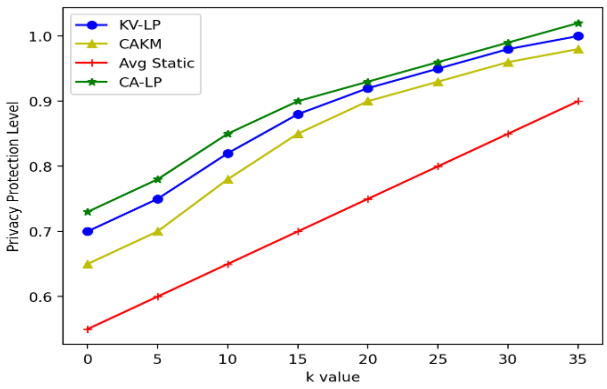

Figure 3. Privacy protection level changes with K value

(2) Quality of service - As shown in Fig. 4, the response time of CA-LP is slightly longer than KV-LP and Avg Static, but it is comparable to CAKM. The marginal difference in response time does not noticeably affect the user experience. Quality of service is measured by the response time and accuracy of the location information provided, ensuring that our system delivers high-quality location-based services while upholding stringent privacy standards.

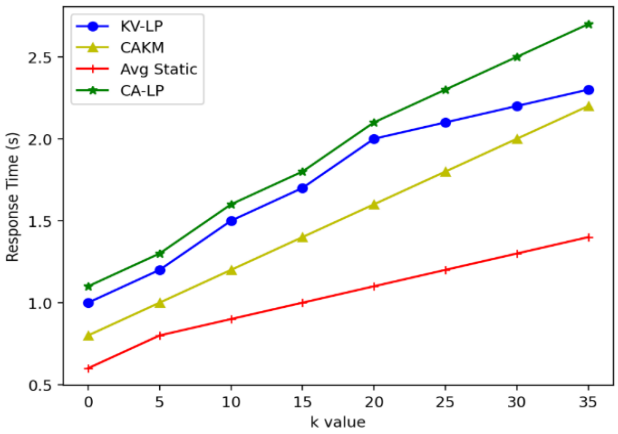

Figure 4. Response time changes with K value

(3) Privacy leakage risk - As shown in Fig. 5, CA-LP has a lower privacy leakage risk due to its contextual computation approach, which makes it more difficult for adversaries to infer user information. This risk is assessed by the probability of an adversary correctly inferring a user's location, with a lower score indicating stronger privacy.

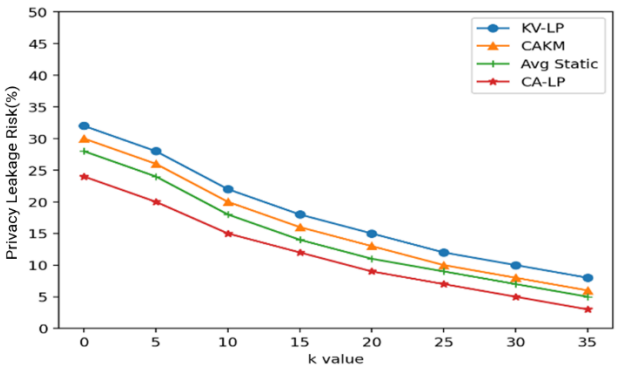

Figure 5. Privacy leakage risk changes with K value

(4) Information loss - Although CA-LP introduces some information loss due to contextual protection, as indicated in Fig. 6, the amount of loss is acceptable when considering the privacy protection benefits that

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

CA-LP provides. Information loss is quantified as the deviation from the actual information caused by the privacy protection mechanism, and is kept within acceptable limits to maintain usability.

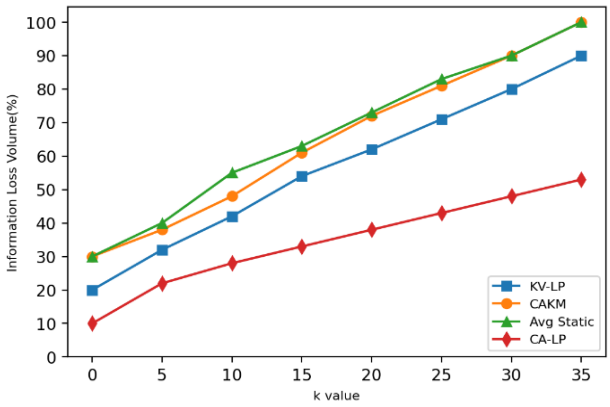

Figure 6. Information loss volume changes with K value

(5) Average anonymous time - As exhibited in Fig. 7, the average time taken by CA-LP is highly comparable to the other three methods, suggesting that its efficiency is sufficient for practical usage. This metric reflects the time a user's location remains anonymous, with a higher value indicating better privacy preservation over time.

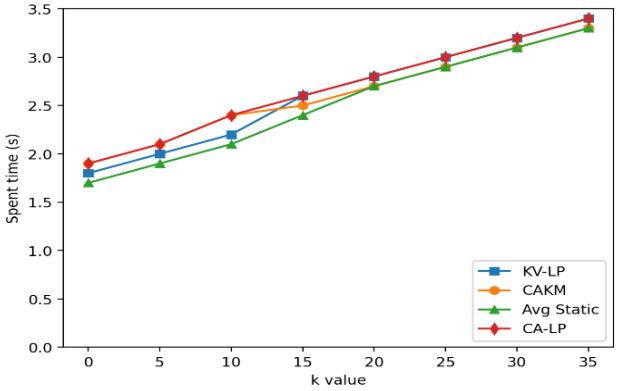

Figure 7. Average anonymous time changes with K value

In conclusion, the experimental results validate that CA-LP provides superior overall privacy protection performance and service quality when weighed against existing methods. Despite minor disadvantages in certain metrics, CA-LP demonstrates extensive practical value for location sharing applications that demand both privacy protection and quality of service.

Conclusion

Our work here reveals a location privacy protection method that is context-aware and based on different users' needs. The underlying principle is to assess the numerous privacy requirements of individuals through the extraction of environmental aspects such as visited time spans, frequency of visitations, and also the regularity as observed from their historical trajectories. However, we realize that some drawbacks exist in the technique proposed.

In particular, our methodology's reliability may be impaired under conditions with thin or non-standard information that could restrict the privacy requirement determination precision as well as the feasibility of our protective measures. In future investigations, we propose to resolve these obstacles through the introduction of new, sophisticated data analysis methods and accounting for even more contextual elements which can compensate for data scarcity.

A context-aware method is designed to estimate personalized privacy demand degrees. By comparing the estimated demand with real-time leakage degree, our approach contextually provides adaptive protection for each user and location context.

Extensive experiments on real-world datasets demonstrate our method outperforms state-of-the-art methods, achieving better overall privacy protection with comparable service quality. The main contributions of this research are the trajectory mining-based context-aware approach and the contextual protection method. From this work, we can consider establishing in future studies a correlation between the user's privacy demand level and the level of location privacy leakage, so that it would be possible to make a quantified assessment. This could offer a clear visual and impartial criterion for regulating your choice about sharing data on your whereabouts. While this is important, we need to recognize the value of user acceptance and the

pragmatism that comes from the use of our own method. Future versions of this technique will also include these dimensions so that the result is not just a good solution in theory but also one that is suitable to end-users' expectations on how usability can be maximized while privacy is protected as well. The next steps will include exploring the adaptation of our method for cloud-based infrastructures and the cloud-specific parameter mappings necessary to enhance the accuracy and effectiveness of privacy protection. In addition to these developments, we emphasize the importance of securing the method against potential security threats. We are conscious of the importance of protecting against DoS attacks and maintaining our system, which will not allow intruders to track the location through a DDoS attack. Some of the future improvements would include the incorporation of more advanced security measures coupled with extensive testing to assess our system's resilience against these adversarial threats. We anticipate that the method will be capable of handling the current scale of data processing and user volume, and it will be flexible enough to scale up as the user base and data volume grow, ensuring that our privacy protection measures can adapt to future changes in technology and market demands.

Acknowledgment

This work was supported by the Universiti Teknologi Malaysia (UTM) through UTMER 2021 (Grant number Q.J130000.3851.20J26).

Authors' Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at Universiti Teknologi Malaysia.

Authors' Contribution Statement

H. Q. performed the research and calculations. H. Q. and H. W. N. discussed the results and wrote this paper together. R. I. supervised the project.

References

1. Tal O, Liu Y. A Joint Deep Recommendation Framework for Location-Based Social Networks. Complexity, 2019. https://doi.org/10.1155/2019/2926749
2. Jiang H, Li J, Zhao P, Zeng F, Xiao Z, Iyengar A. Location Privacy-Preserving Mechanisms in Location-Based Services: A Comprehensive Survey. ACM Comput Surv, 2021;54 (1):1–36. https://doi.org/10.1145/3423165
3. Mehraj H, Jayadevappa D, Haleem S L A, Parveen R, Madduri A, Ayyagari M R, et al. Protection Motivation Theory Using Multi-Factor Authentication for Providing Security Over Social Networking Sites. Pattern Recognit Lett, 2021; 152: 218-224. https://doi.org/10.1016/j.patrec.2021.10.002
4. Jozani M, Ayaburi E, Ko M, Choo K.K. Privacy Concerns and Benefits of Engagement with Social Media-Enabled Apps: A Privacy Calculus Perspective. Comput Hum Behav, 2020; 107: 106260. https://doi.org/10.1016/j.chb.2020.106260
5. Gkoulalas-Divanis A, Loukides G, Sun J. Publishing Data from Electronic Health Records While Preserving Privacy: A Survey of Algorithms. J Biomed Inform. 2014; 50: 4–19. https://doi.org/10.1016/j.jbi.2014.06.002
6. Feng J, Wang Y, Wang J, Ren F. Blockchain-Based Data Management and Edge-Assisted Trusted Cloaking Area Construction for Location Privacy Protection in Vehicular Networks. IEEE Internet Things J, 2020; 8(4): 2087–2101. https://doi.org/10.1109/JIOT.2020.3038468

7. Almusaylim Z. A, Jhanjhi N. Z. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Pers Commun, 2020;111:541–564. https://doi.org/10.1007/s11277-019-06872-3
8. Talat R, Obaidat M. S, Muzammal M, Sodhro A. H, Luo Z, et al. A Decentralized Approach to Privacy Preserving Trajectory Mining. Future Gener Comput Syst, 2020; 102: 382–392. https://doi.org/10.1016/j.future.2019.07.068
9. Xu S, Fu X, Cao J, Liu B, Wang Z. Survey on User Location Prediction Based on Geo-Social Networking Data. World Wide Web. 2020; 23(3): 1621-1664. https://doi.org/10.1007/s11280-019-00777-8
10. Halimi A, Ayday E. Real-Time Privacy Risk Quantification in Online Social Networks. In Proc 2021 IEEE/ACM Int Conf Adv Soc Netw Anal Min. 2021; 74–81. https://doi.org/10.1145/3487351.3488272
11. Gangarde R, Sharma A, Pawar A, Joshi R, Gonge S. Privacy Preservation in Online Social Networks Using Multiple-Graph-Properties-Based Clustering to Ensure K-Anonymity, L-Diversity, and T-Closeness. Electronics, 2021; 10(22): 2877. https://doi.org/10.3390/electronics10222877
12. Gedik B, Liu L. Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms. IEEE Trans Mob Comput, 2007; 7(1): 1–18. https://doi.org/10.1109/TMC.2007.1062
13. Khoshgozaran A, Shahabi C. Blind Evaluation of Nearest Neighbor Queries Using Space Transformation to Preserve Location Privacy. In Proc Int Symp Spat Temporal Databases, 2007; 239–257. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-73540-3_14
14. Palanisamy B, Joshi J. Protecting Privacy in Indoor Positioning Systems. In Indoor Wayfinding and Navigation, 2015; 242–259. CRC Press. https://doi.org/10.1109/ICL-GNSS49876.2020.9115496
15. Shokri R, Theodorakopoulos G, Troncoso C. Privacy Games Along Location Traces: A Game-Theoretic Framework for Optimizing Location Privacy. ACM Trans Priv Secur. 2016; 19(4): 1–31. https://doi.org/10.1145/3009908
16. Andrés M E, Bordenabe N E, Chatzikokolakis K, Palamidessi C. Geo-Indistinguishability: Differential Privacy for Location-Based Systems. In Proc 2013 ACM SIGSAC Conf Comput Commun Secur, 2013; 901–914. https://doi.org/10.1145/2508859.2516735
17. Wang Y, Li M, Luo S, Xin Y, Zhu H, Chen Y, et al. LRM: A Location Recombination Mechanism for Achieving Trajectory k-Anonymity Privacy Protection. IEEE Access, 2019; 7: 182886–182905. https://doi.org/10.1109/ACCESS.2019.2960008
18. Ma C, Li J, Wei K, Liu B, Ding M, Yuan L, et al. Trusted AI in Multi-Agent Systems: An Overview of Privacy and Security for Distributed Learning. arXiv preprint arXiv:2202.09027. 2022. https://doi.org/10.1109/JPROC.2023.3306773
19. Zhu Q, Hu H, Xu C, Xu J, Lee W. C. Geo-Social Group Queries with Minimum Acquaintance Constraints. VLDB J, 2017; 26: 709–727. https://doi.org/10.1007/s00778-017-0473-6
20. Li Y W, Vilathgamuwa D M, Loh P. C, Blaabjerg F A. Dual-Functional Medium Voltage Level DVR to Limit Downstream Fault Currents. IEEE Trans Power Electron. 2006; 22(4): 1330–1340. https://doi.org/10.1109/TPEL.2007.900589
21. Huang L, Yamane H, Matsuura K, Sezaki K. Towards Modeling Wireless Location Privacy. Privacy Enhancing Technologies, 5th International Workshop. PET 2005, Cavtat, Croatia. Lecture Notes in Computer Science. 2005; 3856: 59–77. Springer Berlin Heidelberg. https://doi.org/10.1007/11767831_5
22. Lu Y, Yang S, Chau P. Y, Cao Y. Dynamics Between the Trust Transfer Process and Intention to Use Mobile Payment Services: A Cross-Environment Perspective. Inf Manag, 2011; 48(8): 393–403. https://doi.org/10.1016/j.im.2011.09.006
23. Yadav A S, Kumar S, Karetla G R, Cotrina-Aliaga J C, Arias-Gonzáles J L, Kumar V, et al. A Feature Extraction Using Probabilistic Neural Network and BTFSC-Net Model with Deep Learning for Brain Tumor Classification. J Imaging. 2022; 9(1): 10. https://doi.org/10.3390/jimaging9010010
24. Albouq S S, Abi Sen A A, Namoun A, Bahbouh N M, Alkhodre A B, Alshanqiti A. A Double Obfuscation Approach for Protecting the Privacy of IoT Location Based Applications. IEEE Access. 2020; 8: 129415–129431. https://doi.org/10.1109/ACCESS.2020.3009200
25. Kumar S, Samriya J K, Yadav A S, Kumar M. To Improve Scalability with Boolean Matrix Using Efficient Gossip Failure Detection and Consensus Algorithm for PeerSim Simulator in IoT Environment. Int J Inf Technol. 2022; 14(5): 2297–2307. https://doi.org/10.1007/s41870-022-00989-8
26. Kumar N, Kumar S. A Salp Swarm Optimization for Dynamic Resource Management to Improve Quality of Service in Cloud Computing and IoT Environment. Int J Sens Wirel Commun. Control. 2022; 12(1): 88–94. https://doi.org/10.2174/2210327911666210126122119

2024, 21(10): 3344-3355
https://doi.org/10.21123/bsj.2024.9792
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

27. Kumar N, Kumar S. Conceptual Service Level Agreement Mechanism to Minimize the SLA Violation with SLA Negotiation Process in Cloud Computing Environment. Baghdad Sci J. 2021; 18(2 Suppl.): 1020. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).1020
28. Kumar N, Kumar S. Virtual Machine Placement Using Statistical Mechanism in Cloud Computing Environment. Int J Appl Evol Comput. 2018; 9(3): 23–31. https://doi.org/10.4018/IJAEC.2018070103
29. Chen X, Simchi-Levi D, Wang Y. Privacy-Preserving Dynamic Personalized Pricing with Demand Learning. Manag Sci. 2022; 68(7): 4878–4898. https://doi.org/10.1287/mnsc.2021.4129
30. Neisse R, Steri G, Baldini G, Tragos E, Fovino I N, Botterman M. Dynamic Context-Aware Scalable and Trust-Based IoT Security, Privacy Framework. 2022; 199–224. River Publishers. https://doi.org/10.1201/9781003338628-5
31. Qing H, Ibrahim R, Nies H W. Location Anonymous Query Algorithm Based on Road Networks. In Proc. 2022 Int Conf Augment Intell Sustain Syst. 2022; Trichy, India. 1477–1480. https://doi.org/10.1109/ICAISS55157.2022.10011062
32. Jiang H, Zhao P, Wang C. RobLoP: Towards robust privacy preserving against location dependent attacks in continuous LBS queries. IEEE/ACM Transactions on Networking. 2018;26(2):1018-32. https://doi.org/10.1109/TNET.2018.2812851
33. Phan T N, Dang T K, Truong T A, Thanh H L. A context-aware privacy-preserving solution for location-based services. Int Conf Adv Comput Appl. IEEE, 2018; 132-139. https://doi.org/10.1109/ACOMP.2018.00028

طريقة حماية خصوصية الموقع الواعية للسياق

هاوهوا تشينغ، روليانا إبراهيم، هوي وين نيس

قسم الحوسبة التطبيقية والذكاء الاصطناعي، كلية الحوسبة، جامعة تكنولوجي ماليزيا، جوهور، ماليزيا.

الخلاصة

لقد أصبحت حماية خصوصية الموقع موضوعاً يحظى بإهتمام متزايد مع شعبية الخدمات المبنية على المواقع. تقترح هذه الدراسة طريقة حماية خصوصية الموقع الواعية للسياق (CA-LP). تقوم CA-LP بتقييم احتياجات خصوصية الموقع لدى المستخدمين من خلال تحليل مساراتهم التاريخية وتقدير درجة تسرب الخصوصية في المواقع. تقارن التجارب بين CA-LP وطرق أخرى من حيث مقاييس مثل مستوى حماية الخصوصية، جودة الخدمة، مخاطر تسرب الخصوصية، فقدان المعلومات، ومتوسط الوقت المجهول. تظهر النتائج أن CA-LP توفر حماية خصوصية وجودة خدمة أفضل عند النظر في جميع العوامل. تظهر CA-LP قيمة عملية واسعة في تطبيقات مشاركة المواقع.

الكلمات المفتاحية: الأمان الواعي للسياق، حفظ الخصوصية الديناميكي، الخدمات المبنية على المواقع، حماية خصوصية الموقع، التحليل الدلالي في بيانات المواقع.