Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 04 (April -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i04.pp40 - 45*

UBLS - USER-BASED LOCATION SELECTION SCHEME FOR PRESERVING LOCATION PRIVACY

Dr.S.Suresh [1],Bollineni Surya Prabha [2],Sunkara Lakshmi Sri Nitya [3],Rednam S Sai Venkata Siva Satya Narendra [4],Kadali Vamsi Kiran [5],Addepalli Satya Bhaskar [6]
ASSOCIATE PROFESSOR
DEPT OF COMPUTER SCIENCE AND ENGINEERING
PRAGATI ENGINEERING COLLEGE(A),SURAMPALEM(EAST GODAVARI)A.P,INDIA

To Cite this Article
Dr.S.Suresh ,Bollineni Surya Prabha ,Sunkara Lakshmi Sri Nitya ,Rednam S Sai Venkata Siva Satya Narendra [4],Kadali Vamsi Kiran ,Addepalli Satya Bhaskar **UBLS - USER-BASED LOCATION SELECTION SCHEME FOR PRESERVING LOCATION PRIVACY"** *Journal of Science and Technology, Vol. 08, Issue 04,-April 2023, pp40-45*
Article Info
Received: 22-02-2023 Revised: 15-03-2023 Accepted: 22-03-2023 Published: 14-04-2023

Abstract:

Due to the wide availability of location-based services (LBSs) that enable many applications to provide user tailored services, it becomes possible to trace the locations of an individual by an adversary, especially when the LBS server is distrusted, which violates the user's privacy. Therefore, we propose, in this project, a user-based location selection scheme (UBLS) to hide the users' locations using k-anonymity to preserve users' privacy. The proposed scheme uses the concept of dummy locations to hide the real locations of the users, but on top of that, it selects the dummy locations based on the users that exist in these locations. Moreover, we propose an attacker location exclusion (ALE) algorithm that can be used to attack the existing location privacy-preserving schemes. We also propose a new metric, namely location privacy level (LPL), to qualify the ability of the malicious LBS server to reduce the privacy level of the requester. Our envisioned UBLS scheme is evaluated with extensive computer-based simulations. Comparing to the existing schemes in the literature that preserve location privacy, our proposed UBLS demonstrates performance improvement in terms of entropy, cloaking region, and location privacy level metrics.

I. Introduction

Recently, the dependency of the smartphones' applications on location has been dominating the Google play and Apple stores. Therefore, the location-based services (LBSs) are becoming essential in everyone's life because, for example, in Google map application, the user must reveal his/her location to request the route to a certain location. Moreover, the need for the location information is not limited to the location-based applications, but also it is used in some social network applications such as Facebook and Twitter. Facebook uses the location information to let the user know about nearby friends, while Twitter uses the location to find tweets posted by nearby people. Although disclosing the personal location information enables many applications to provide user-tailored services, this practice might threaten the user privacy. For instance, when acquiring the location of a user, an adversary can use this information for tracking the user and identifying the locations the user visits, which can reveal the activities of the users. Therefore, preserving location privacy is an essential requirement in mobile applications and social networks. The existing approaches that are used to protect location privacy can be classified into cryptographic-based and k-anonymity based. Therefore, we address, in this project, the limitations in the existing schemes, formally present a proposed adversarial model, and envision an efficient privacy-preserving user's location selection approach.

II. LITERATURE SURVEY

1. A survey of app store analysis for software engineering

App Store Analysis studies information about applications obtained from app stores. App stores provide a wealth of information derived from users that would not exist had the applications been distributed via previous software deployment methods. App Store Analysis combines this non-technical information with technical information to learn trends and behaviors within these forms of software repositories. Findings from App Store Analysis have a direct and actionable impact on the software teams that develop software for app stores, and have led to techniques for requirements engineering, release planning, software design, security and testing. This survey describes and compares the areas of research that have been explored thus far, drawing out common aspects, trends and directions future research should take to address open problems and challenges.

2. Geo-location identification of fakebook pages

Online Social Network (OSN) communities serve as different platforms for multiple users' interaction - people behaving diversely among distinctive communities - such as entertainment, global and local discussion communities. However, attribute identification among online discussion communities remains largely unexplored. In this paper, we describe and analyze the geo-location property of large-scale Facebook public pages (15M pages). We propose a framework utilizing the connectivity of the page-like graph to predict the missing geo-location information based on Breadth-First Search (BFS). Our method achieves a satisfyingly high accuracy (89 %) on identifying the state location attribute of unknown United States (US) pages. Our empirical results offer a better understanding of regional social analysis and target audience broadcasting.

3. Detecting citizen problems and their locations using twitter data

Twitter is a social network, which contains information of the city events (concerts, festival, etc.), city problems (traffic, collision, and road incident), the news, feelings of people, etc. For these reasons, there are many studies, which use tweet data to detect useful information to support the smart city management. In this paper, the ways of finding citizen problems with their locations by using tweet data is discussed. Tweets in Turkish language from the Aegean Region of Turkey were used for the study. It is aimed to form a smart system, which detects problems of citizens and extracts the problems' exact locations from tweet texts. Firstly, the collected data was analyzed to get information of any city event, citizen's complaint or requests about a problem. After the possibility of detecting tweets, which have any city problem, was ensured, two datasets were created. The first one consists of the tweets that have an event information or a problem and the second one has the tweets, which have other information not related to our study. Then Naive Bayes classifier was trained on the annotated tweets and was tested on a separate set of tweets. Accuracy, precision, recall, and F-measure of the classifier is given. A location recognizer, which finds the Turkish place names in a text, is created and applied on the tweets that are marked as information-containing by the classifier to detect the location of the problem precisely. The first findings of the project is promising. The high accuracy, which is obtained by the classifier, shows that it is proper to use this classifier for our study. The location recognizer is planned to be improved and place names on the real-time tweet data is to be detected.

4. Location privacy-preserving mechanisms in location-based services: A comprehensive survey

Location-based services (LBSs) provide enhanced functionality and convenience of ubiquitous computing, but they open up new vulnerabilities that can be utilized to violate the users' privacy. The leakage of private location data in the LBS context has drawn significant attention from academics and industry due to its importance, leading to numerous research efforts aiming to confront the related challenges. However, to the best of our knowledge, none of

relevant studies have performed a qualitative and quantitative comparison and analysis of the complex topic of designing countermeasures and discussed the viability of their use with different kinds of services and the potential elements that could be deployed to meet new challenges. Accordingly, the purpose of this survey is to examine the privacy-preserving techniques in LBSs. We categorize and provide an inside-out review of the existing techniques. Performing a retrospective analysis of several typical studies in each category, we summarize their basic principles and recent advances. Additionally, we highlight the use of privacy-preserving techniques in LBSs for enabling new research opportunities. Providing an up-To-date and comprehensive overview of existing studies, this survey may further stimulate new research efforts into this promising field.

III.SYSTEM ANALYSIS

3.1. EXISTING SYSTEM

The existing approaches that are used to protect location privacy can be categorized into cryptographic-based and k-anonymity-based. In the cryptographic-based approaches, the user requests the LBS provider's public-key to encrypt his/her location. Then, the LBS provider decrypts the location by the private-key of the LBS provider. Although this approach is secure against eavesdroppers, location privacy may be violated when the LBS server is malicious or distrusted. Moreover, it also suffers from high computation overhead needed to encrypt and decrypt the messages.

On the other hand, the k-anonymity approaches are used to preserve the location privacy by using an anonymous set that consists of k locations (one is real and k − 1 locations are dummy) with the aim of making any location that belongs to this set indistinguishable from all other k − 1 locations, so that the adversary cannot identify the dummy locations. This approach has some advantages such as lower communication and computation overhead comparing to the cryptographic based approaches. Niu et al. proposed a scheme, named fine-grained spatial cloaking "FGcloak", which uses k-anonymity technique. This scheme adapts the idea of the Hilbert curve to effectively achieve privacy preservation using the k-anonymity concept. However, the proposed scheme suffers from high cloaking region compared to other existing solutions such as EDLS, which makes the response of the server inaccurate. Moreover, the entropy value of the EDLS is better than its value of the FG cloak algorithm. Note that entropy is a metric that is used to measure the privacy level.

3.2. PROPOSED SYSTEM

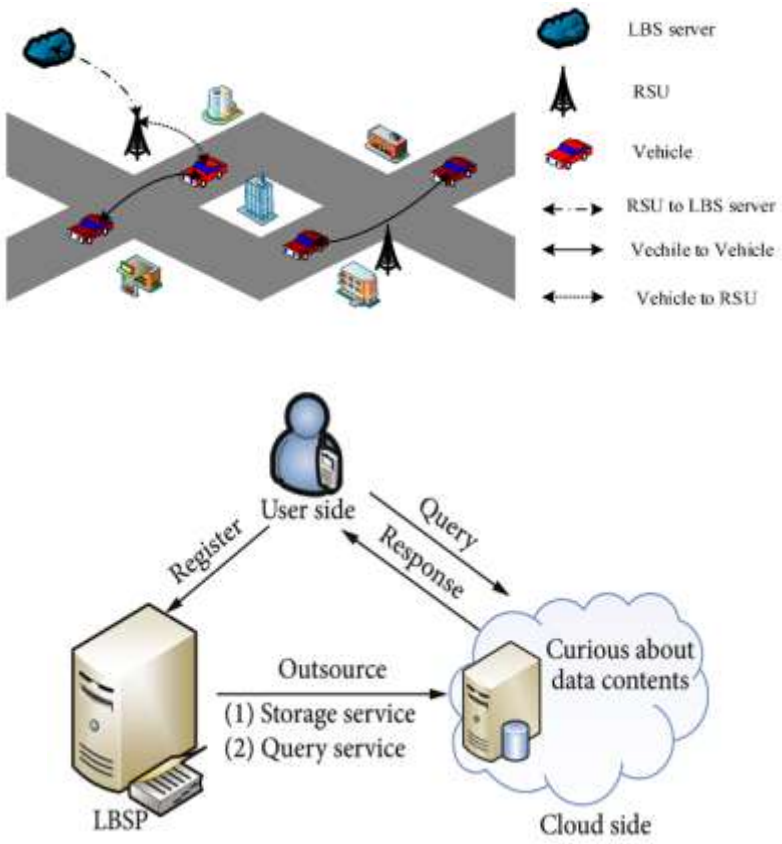
We propose a User-Based Location Selection (UBLS) scheme to preserve the privacy of the users' locations using k-anonymity and taking user's query probability into consideration. Our scheme chooses k − 1 dummy users who have query probabilities which are close to the query probability of the requester, i.e., the user who requests a service from the LBS server. Then, it uses the k − 1 dummy users' locations to hide the requester's location. We propose an attacker location exclusion (ALE) algorithm that can be used to attack the existing privacy preserving schemes. This attacker algorithm attempts to find the real location of the requester in the k locations he sends by excluding the locations that have low probabilities to be the requester's location.

We propose a new metric, namely location privacy level (LPL), to qualify the ability of the malicious LBS server to reduce the privacy level of the requester. We extensively evaluate the proposed UBLS scheme and compare it with different benchmarks. We run the ALE algorithm against our UBLS scheme and the existing schemes to assess the ability of these schemes in preserving location privacy when the LBS server is malicious. The results demonstrate that the proposed UBLS scheme outperforms the existing schemes in terms of cloaking region, entropy, and LPL.

IV.SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture of The User-Based Selection Scheme for Preserving Location Privacy.



4.1. System Architecture

V. SYSTEM IMPLEMENTATION

5.1. MODULES

There are 2 modules:

1. User
2. Location Based Server

5.1.1 User:

A user module in a user-based location selection scheme is a component that allows users to choose their preferred level of location privacy. It typically operates by providing users with different options or settings to control how their location data is collected, processed, and shared.

- Register
- Login
- Search Location
- User search
- Notification
- Logout

5.1.2 Location Based Server:

A location-based server module can be designed to provide location-based services to users while preserving their location privacy. In this module, the user selects the locations they want to share with the server, and

the server only receives data related to those locations. The user's precise location is not disclosed to the server, and their location privacy is preserved.

- Register
- Login
- New Request
- User Details
- Logout.

VI. RESULTS

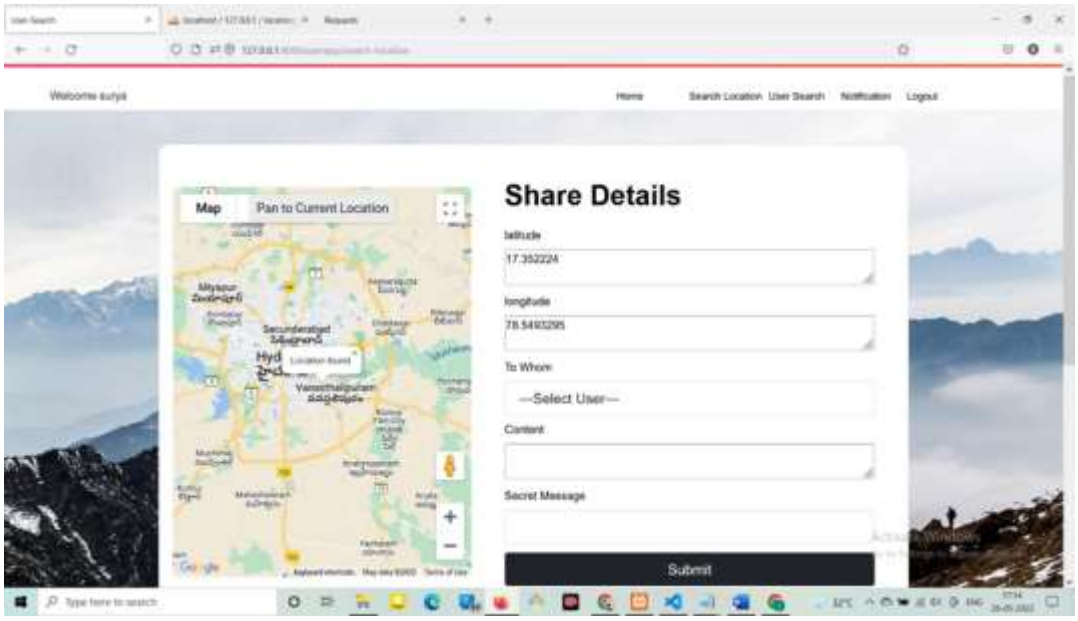


Fig 6.1 Search Location

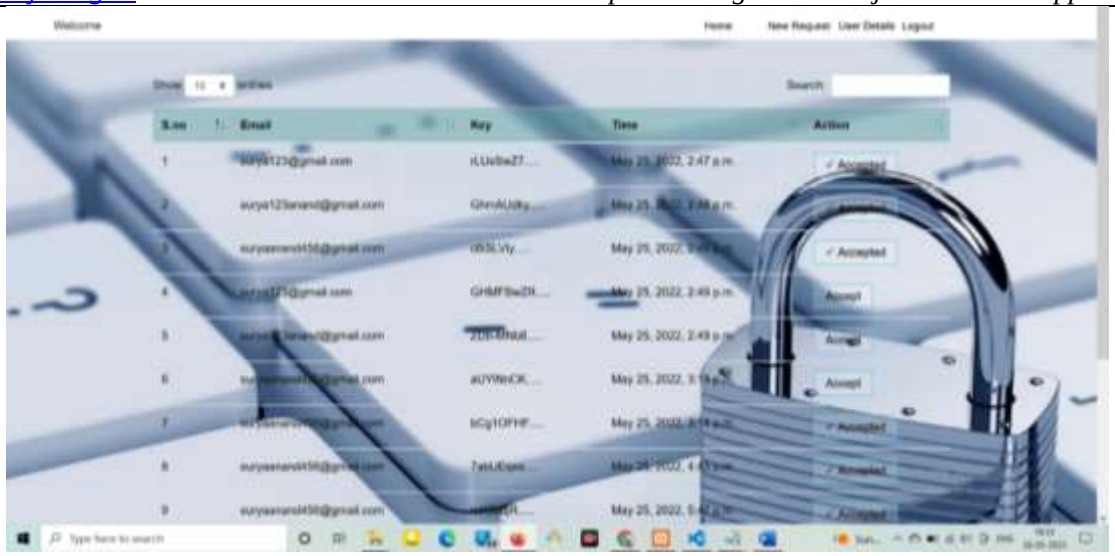


Fig. 6.1 New Requests coming from user

VII.CONCLUSION AND FUTURE WORK

In this project, a novel scheme, called "UBLS", is proposed to preserve users' location privacy against adversaries while assuming that the LBS server is distrusted. Using users' queries and the k-anonymity technique, UBLS scheme carefully chooses a set of users who have the same (or close) query probability as the query probability of the user that exists in the real location, and hence, a set of dummy locations can be chosen. We have also proposed a new metric, namely "LPL", to measure the level of privacy the anonymity set provides by measuring the attacker's ability to identify and exclude some dummy locations from the anonymity set. We evaluated the UBLS scheme against existing schemes including DLS, EDLS, and MN. The results of our experiments demonstrate that UBLS can improve the privacy level in terms of entropy and LPL metrics.

REFERENCES :

[1] W. Martin, F. Sarro, Y. Jia, Y. Zhang, and M. Harman, "A survey of app store analysis for software engineering," IEEE Transactions on Software Engineering, vol. 43, no. 9, pp. 817–847, 2017.

[2] Y.-C. Lin, C.-M. Lai, J. W. Chapman, S. F. Wu, and G. A. Barnett, "Geo-location identification of facebook pages," in 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2018, pp. 441–446.

[3] G. Abalı, E. Karaarslan, A. Hurriyeto ¨ glu, and F. Dalkılıc¸, "Detecting ˇ citizen problems and their locations using twitter data," in 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). IEEE, 2018, pp. 30–33.

[4] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1–36, 2021.

[5] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," Personal and ubiquitous computing, vol. 18, no. 1, pp. 61–74, 2014.

[6] S. Zhang, X. Mao, K.-K. R. Choo, T. Peng, and G. Wang, "A trajectory privacy-preserving scheme based on a dual-k mechanism for continuous location-based services," Information Sciences, vol. 527, pp. 406–419, 2020.

[7] A. K. Das, A. Tabassum, S. Sadaf, and D. Sinha, "Attack prevention scheme for privacy preservation (apsp) using k anonymity in location-based services for iot," in Computational Intelligence in Pattern Recognition. Springer, 2020, pp. 267–277.

[8] L. P. Yeluri and E. M. Reddy, "Improved privacy preserving score-based location k-anonymity in lbs," in Innovations in Computer Science and Engineering. Springer, 2020, pp. 627–632.

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

[10] A. Solanas and A. Mart´ınez-Balleste, "A ttp-free protocol for location ´ privacy in location-based services," Computer Communications, vol. 31, no. 6, pp. 1181–1191, 2008.

[11] B. Niu, Q. Li, X. Zhu, and H. Li, "A fine-grained spatial cloaking scheme for privacy-aware users in location-based services," in 2014 23rd international conference on computer Communication and networks (ICCCN). IEEE, 2014, pp. 1–8.

[12] D. Zhao, Y. Jin, K. Zhang, X. Wang, P. C. Hung, and W. Ji, "Epla: efficient personal location anonymity," GeoInformatica, vol. 22, no. 1, pp. 29–47, 2018.