User-Based Location Selection (UBLS): A Method for Protecting Users' Location Data

Dr. E Mohan[1], Dr. G Ahmed Zeeshan[2], Mrs. Noore Ilahi[3]
Professor[1], Associate Professor[2], Assistant Professor[3]
Department of CSE
Global Institute of Engineering and Technology

Abstract:

The proliferation of location-based services (LBSs) has opened the door for numerous apps to create personalized experiences for users, but it also opens the door for malicious actors to potentially track users' whereabouts—especially if they have reason to mistrust the LBS server—infringing on their privacy. Hence, to protect users' privacy, we provide a user-based location selection technique (UBLS) in this project that uses k-anonymity to conceal users' whereabouts. In addition to concealing users' actual locations, the proposed approach also chooses fictitious places according to the number of people present there. To further undermine the current location privacy-preserving approaches, we provide an attacker location exclusion (ALE) algorithm. Additionally, we provide a novel measure called location privacy level (LPL) to assess the potential for a malevolent LBS server to compromise the requester's privacy. Robust computational modeling is used to assess our proposed UBLS system. When we compare our proposed UBLS to other location privacy preservation techniques in the literature, we find that it outperforms them in terms of entropy, cloaking region, and location privacy level metrics.

I. Introduction

The location-based smartphone apps have recently taken over the App Store and Google Play. Thus, LBSs are rapidly becoming indispensable in many aspects of life. This is due to the fact that, for instance, in order to request a route to a certain place in the Google Maps application, the user is required to disclose his or her position. Also, social media apps like Facebook and Twitter make use of users' location data, so it's not only location-based apps that require it. Similarly to how Facebook utilizes a user's location to show them friends who are nearby, Twitter uses a user's location to show them tweets that individuals in the immediate area have sent. Many apps rely on users' personal location data to provide individualized experiences, but this approach raises concerns about users' right to privacy. For example, if an adversary gets a user's location data, they may use it to follow the user and see what places they frequent, which can expose their actions. This highlights the critical need of location privacy protection for social media and mobile apps. There are currently two main schools of thought when it comes to safeguarding users' location data: cryptography and k-anonymity. Consequently, we officially provide a suggested adversarial model, imagine an efficient method for user location selection that preserves anonymity, and solve the shortcomings of the current techniques in this project.

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

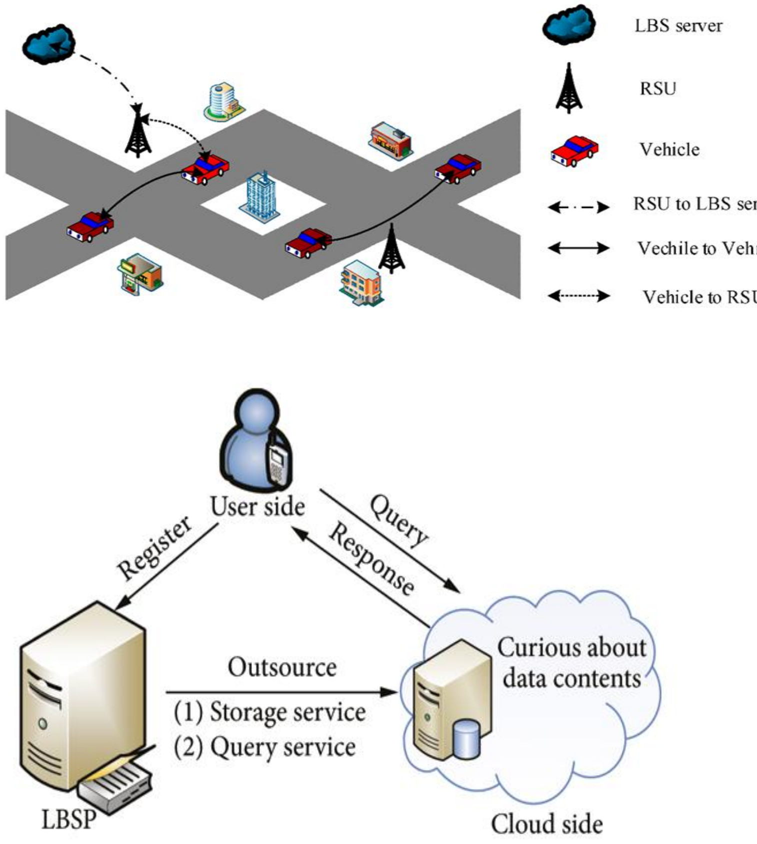
We propose a User-Based Location Selection (UBLS) scheme to preserve the privacy of the users' locations using k-anonymity and taking user's query probability into consideration. Our scheme chooses k − 1 dummy users who have query probabilities which are close to the query probability of the requester, 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:

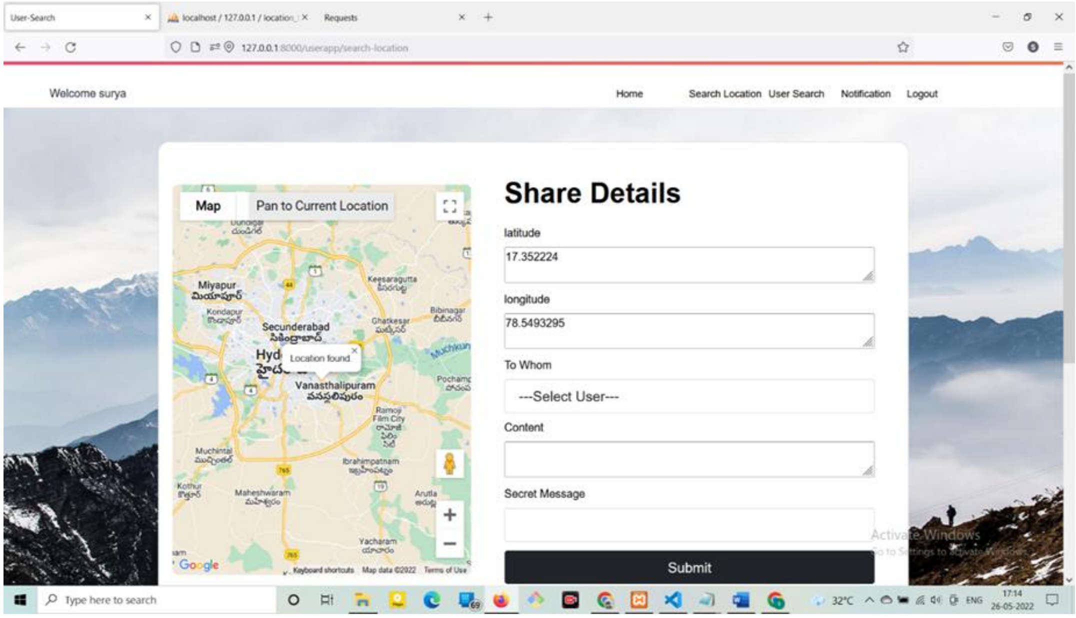
A user module in a user-based location selection scheme is a component that allows users to choose their preferred level of location privacy. It typically operates by providing users with different options or settings to control how their location data is collected, processed, and shared.

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

VI. RESULTS



Welcome surya

Share Details

latitude: 17.352224

longitude: 78.5493295

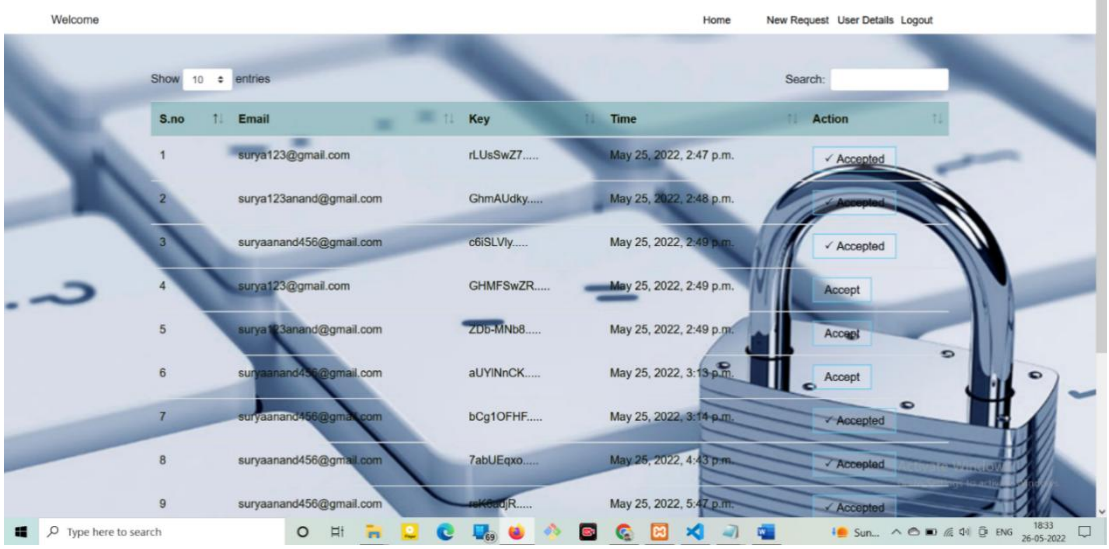
To Whom: ---Select User---

Content

Secret Message

Submit

Fig 6.1 Search Location



S.no	Email	Key	Time	Action
1	surya123@gmail.com	rLUsSwZ7.....	May 25, 2022, 2:47 p.m.	✓ Accepted
2	surya123anand@gmail.com	GhmAUdky.....	May 25, 2022, 2:48 p.m.	✓ Accepted
3	suryaanand456@gmail.com	c6iSLVly.....	May 25, 2022, 2:49 p.m.	✓ Accepted
4	surya123@gmail.com	GHMFSwZR.....	May 25, 2022, 2:49 p.m.	Accept
5	surya123anand@gmail.com	ZDb-MNb8.....	May 25, 2022, 2:49 p.m.	Accept
6	suryaanand456@gmail.com	aUYINnCK.....	May 25, 2022, 3:13 p.m.	Accept
7	suryaanand456@gmail.com	bCg1OFHF.....	May 25, 2022, 3:14 p.m.	✓ Accepted
8	suryaanand456@gmail.com	7abUEqxo.....	May 25, 2022, 4:43 p.m.	✓ Accepted
9	suryaanand456@gmail.com	reK6adjR.....	May 25, 2022, 5:47 p.m.	✓ Accepted

Fig. 6.1 New Requests coming from user

VII.CONCLUSION AND FUTURE WORK

I. Here, we provide a new method, "UBLS," that, supposing the LBS server is distrusted, will protect users' location privacy from attackers. By analyzing user queries and using the k-anonymity approach, the UBLS system selects a group of users whose query probabilities are similar to, or even near to, those of the users present at the actual location. This allows for the selection of a set of fake locations. Additionally, we have introduced a novel metric called "LPL" to quantify the privacy protection offered by the anonymity set. This metric gauges the degree to which an attacker may detect and exclude certain fictitious places from the anonymity set. We compared the UBLS scheme to others, such as DLS, EDLS, and MN, which are already in use. Our experimental findings show that UBLS may increase privacy with respect to entropy and LPL metrics.

REFERENCES :

[1] "A survey of app store analysis for software engineering" (W. Martin, F. Sarro, Y. Jia, Y. Zhang, and M. Harman, 2017) published in the IEEE Transactions on Software Engineering, volume 43, issue 9, pages 818–847.

An article titled "Geo-location identification of Facebook pages" was presented at the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) by Y.-C. Lin, C.-M. Lai, J. W. Chapman, S. F. Wu, and G. A. Barnett. 2018 IEEE, pages 441-446.

The paper "Detecting ˘ citizen problems and their locations using twitter data" was presented at the 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG) by G. Abalı, E. Karaarslan, A. Hurriyeto glu, and F. Dalkılıc¸. pages 30-33, 2018 (IEEE).

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

An article titled "A k-anonymity privacy-preserving approach in wireless medical monitoring environments" was published in 2014 in the journal Personal and Ubiquitous Computing and was co-authored by P. Belsis and G. Pantziou. The article spans pages 61–74.

[6] "A trajectory privacy-preserving scheme based on a dual-k mechanism for continuous location-based services," published in 2020 in the journal Information Sciences, is written by S. Zhang, X. Mao, K.-K. R. Choo, T. Peng, and G. Wang.

[7] "Attack Prevention Scheme for Privacy Preservation (apsp) using k Anonymity in Location-Based Services for the Internet of

Things," published in Computational Intelligence in Pattern Recognition, by A. K. Das, A. Tabassum, S. Sadaf, and D. Sinha. In 2020, Springer published the book on pages 267–277.

"Improved privacy preserving score-based location k-anonymity in lbs," published in Innovations in Computer Science and Engineering, was written by L. P. Yeluri and E. M. Reddy. In 2020, Springer published the book on pages 627-632.

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

"A ttp-free protocol for location 'privacy in location-based services'" was published in 2008 in the journal Computer Communications by A. Solanas and A. Mart'ınez-Balleste.

Presented at the 2014 23rd International Conference on Computer Communication and Networks (ICCCN), "A fine-grained spatial cloaking scheme for privacy-aware users in location-based services" was written by B. Niu, Q. Li, X. Zhu, and H. Li. 2014, IEEE, pages 1-8.

The paper "Epla: efficient personal location anonymity" was published in GeoInformatica in 2018 and was co-authored by D. Zhao, Y. Jin, K. Zhang, X. Wang, P. C. Hung, and W. Ji.