Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 9340 - 9347

Research Article

Privacy Preservation Of Mobile Users Using L-Diversity

R.Srikanth[a], Dr.Y. Rama Devi[b], B. Nandana[c]
[a] Assistant Professor, Dept of CSE, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad,Telangana,India
[b] Professor, Dept of CSE, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad,Telangana,India
[c] M.Tech Student, Dept of CSE, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad,Telangana,India
Email: [a]rsrikanth_cse@cbit.ac.in, [b]yramadevi_cse@cbit.ac.in, [c]Pgs19015_cse.botla@cbit.org.in

Abstract

Due to the increased availability of locality-based cyber services in mobile applications seclusion protection for users is critical and stands one of the major difficulties of study. The aim of the paper is to propose algorithm to maintain the privacy position of mobile device users on location based cyber services in a region of concern algorithm based on division Privacy Position of Mobile Users on Cyber Services (PPCS). In contrast to existing draw breath methods, our PPCS methodology is dumb places and the semantically information of these places is taken into account. The PPCS algorithm allows the locations created to exclude or decrease exposure to the actual location of a user. We show that PPCS is impervious to conniving and inferential abuse. We also examine the effectiveness of our proposed approach and demonstrate the usefulness of comprehensive simulations.

Keywords: *Location, Privacy, Location-based service*

Introduction

Mobile applications and apps (apps) are increasing quickly in use with location-based service (LBS) applications [3]. LBSs, however, have problems with privacy and security to be resolved. In order to promote harmful acts for instance it has been proven that user locality details can be attacked [2], [4].The research community is not surprisingly interested in the design of location-based data protection systems, including:

• Dummy generation: making phone doubts and localities to disguise authentic user locality [5], and
• Seclusion data recovery: penetrating from data base without the need to leak query text or user identity [6].
• Send user information instead of a single actual location.
• Dummy generation. Since GPS is included in many mobile devices (e.g. Smart phone, tablet and smart vehicle entertainment)

User modules can readily receive accurate place information [7]. The specification, Point of Interest (POI), actual place and Region of Interest (ROI) of the user may be included in an LBS query. For instance, an access provider provides a Point of Interest on the user's Region of Interest, like a petrol bunk or health care centers or grocery, for a user while answering a query from the user.

1.1 Location Based Services (LBS)

Location Based Servers (LBS) include location information and users send queries to LBS servers for local information such as the market, cinema hall, train station, etc. Location Based server. Mobile users retrieve current user locations from GPS when sending queries and send them to LBS to determine the nearest place. LBS servers take user locations and locate nearby places and provide them to the user based on distance. Sometimes these LBS servers may misuse user location data so that the user location author uses the following technologies for security.

1.2 Problem Statement

The privacy preservation of user spatial information and query resilient to the location injection attacks is the challenging factor in Location based services.
The aim is to develop a system which is to preserve the user data using l-diversity technique.

1.3 Formation Of The Report

The formation of the report is categorized as follows. We discuss the introduction and problem statement in section 1 We discuss our system design analysis and evaluation in security achievement in section 2 and section 3, eventually in section 4 the conclusion of this study

1.4 Existing System

Services based on Today location rely solely on user devices to establish their place, e.g. utilizing GPS. But malevolent users can falsify their STP data. Consequently, in order to accomplish the completeness of STP proofs, we must include third parties in creating STP evidence. But this opens up a variety of challenges relating to security and privacy.
We proposed a system based on both wired AP proofs and Bluetooth-enabled mobile pairs to allow no users to falsify evidence at the same time, without interacting with both wireless APs and other mobile partners. System uses its private corroborator technology to produce alibi (i.e. location proof) for mobile users in the immediate vicinity.

1.4.1 Disadvantages of Existing System:

• In most STP evidence systems, the wireless infrastructure is used to create evidence for mobile users, for example, through WiFi APs. However for all kinds of applications it can surely not be possible, for example, to have STP proof for green commuting and battlefield instances from wireless APs.
• A multiple trusted or semi confident third parties are required for most present schemes.

Homomorphic RSA Encryption:

The mobile server user will encrypt a query using Homomorphic RSA Encryption before submitting a query to LBS and sending it to LBS and LBS will execute the scanning search directly with encrypted data.

1.5 L-Diversity:

We employ L-Diversity algorithms to ensure security for user locations (latitude and longitude) by setting up a group with specific traits that will anonymise data so that no hackers can recognize any information there from.

Advantages

•Ensure more user location security.

2.1.1 Principle Of L-Diversity:

A k-anonymous table is said to be l-diverse if each compatibility class in the table has at least 'l' "well represented" values for each sensitive attribute [19][22].
The term "well-represented" can be illuminated as per the following principles:

2.1.2 Distinct l-diversity:

A value shows more repeatedly than alternative values within the compatibility class. The downfall in this is that the attacker can guess that this value is fare to represent the individual based on the anticipation of existence.

2.1.3 Entropy l-diversity:

The unified table should have at least log(l) as degenerate to meet entropy l-diversity for every compatibility class. This approach may be too expensive in the case of low degeneration of unified table when only a few values are the same.

2.1.4 Recursive (c, l)-diversity:

The susceptible values of each correlation class do not occur either too habitually or too scarcely. This approach is stronger than the previous two approach mentioned above [21] [22]

System Design

2.1 System Design

A diagram is a graphical portrayal of an item interaction situation showing what happens first and next in a time-based sequence. Sequence diagrams define item roles and assist select classrooms and interfaces with critical information. Sequence diagrams depict time-based item interaction, whereas collaborative diagrams explain how objects associate each other. There are two primary differences between sequence and collaboration diagrams; a diagram with sequence has two dimensions: vertical positioning normally symbolizes time and horizontal positioning is different.

2.1.1 Object

The object has state, conduct and identity object. In your common class, the structure and conduct of related objects are defined. Each diagram object identifies a particular class instance. An unnamed object is called a class instance.
The icon of the object resembles an icon for class but underlines its name: Competition of an object is determined by its class competitor.

2.1.2 Message

The communication between two things which trigger an event is a message. A message brings information from the control source to the control target. The message synchronization can be changed by specifying the message. Synchronization means a message to wait for the results of the transmitting item.

2.1.3 Link

A connection should only exist if there is a link between their respective classes between two objects, including class utilities. A connection exists between two classes and signifies a method of communication between class instances: an object can send messages to another. The connection is represented in a collaboration diagram as a direct line between objects or objects and class instances. Use the loop version of the icon if an object is linked to itself.3

Proposed Approach

Analysis class identification: a class is a set of items that share a common formation and behavior (the same attributes, operations, relationships and semantics). A class is a summary of the real things of the world. The class identification approaches are four:

a. Noun phrase approach
b. Common Class Pattern Approach
C. Collaboration approach
d. Classes Responsibilities and Collaboration Approach
Noun Phrase Approach
The guidelines for identifying the classes:
•See for nouns and noun expressions in the use cases.
•Some classes are indirect. Avoid computer implementation classes-defer them to the design stage.
•Carefully choose and define the class names .After identifying the classes we have to eliminate the following types of classes:
•Adjective classes.

3.1 Common class pattern approach

The following are pattern for finding the candidate classes:

- Concept class
- Event class
- Formation class
- People class
- Places class
- Tangible things and device class
- Common class pattern approach

3.2 CRC approach

The following stages are taken: The process:

- Name the responsibility of the classes (and identify the classes.)
- Collaborator identification.

Identifying each class's responsibilities:
The questions to identify the class characteristics and methods are:
The following questions should be answered:

a. What should we maintain track of information on an object?
b. How should the services be provided by a class?
c. Identification of class relationships:

There are three sorts of relations between the objects:

- Association: How are related objects?
- Super-sub structure: How may things be classified into classes?
- Aggregation: How are the complex classes composed?
- Association: The following questions will enable us to determine the associations:
    a. Can the class perform the needed task on its own?
    b. What do you need if not?
    c. What classes may it obtain from what other classes?

Algorithm-1: ppcs algorithm

Input: (1) Actual doubt prospect T;
(2) Frame work:option,k,l;
(3) LBS doubt d=(uid,{(x,y),S,T}).
Output: LBS doubt d*.
Gauge the current doubt prospect Q according to T and the correct info;
classify elements in Q confer to locality type;

if(option= =1)then
Call Action-i;
else
Call Action-ii;
if a user has a seclusion protection essential,
Select([l/2]-1) dope Point Of Interests based on k dope;
return d*=(uid,{(x1,y1),...,(xk,yk)},S,{P1,...,P[l/2]})
else
return d*=(uid,{(x1,y1),...,(xk,yk)},S,T)

Action-i:Provoke dope that add authentic location of a users
Input:(1) Location (x, y) of a user;
(2) Draw breath doubt probabilities;
(3) Frame Work:m,n.
Output: k dopes{(x1,y1),...,(xk,yk)}.
Choose an additional n-1 types of locality seeing the correct locality info;
for(n:n-1)
Select m-1 aspirant locality in each type of locality;
Accept m-1 locality from the aspirant locality based on their decay values;
return

Action-ii : Provoke dopes that blocks the authentic locality of a users
Input:(1) Locality (x, y) of a user;
(2)Frame work:m,n,z,R;
(3)Present doubt prospect.
Output:k dopes and new radius{(x1,y1),...,(xk,yk)},R)}.
Cross the Region Of Interest into n sectors;
Achieve n oblique locality to cover the Region Of Interest;
z*number of locality classes;
if(z* < l)
Accept an further z-l* classes of localities;
for(z:z-1)
Exclusive m-z aspirant localities;
Meanly accept further k-n locality against the aspirant localities;
return

Result

Location based servers (LBS) have information about where the users are located and can send requests to those LBS servers in order to know about local areas such as the market, the cinema hall and the train station. Mobile users will extract from GPS the current user position during query sending and submit them to LBS to locate nearby users. LBS servers accept user locations and locations nearby and send to the user based on distance. In some cases this LBS server may misuse the location of user data in order to provide safety for the author of the user location.

4.1 Homomorphic RSA Encryption

Prior to submitting an inquiry to the mobile LBS server, mobile user encrypts a query using the homomorphic RSA encoding, then immediately sends to the LBS system and LBS performs encrypted search operations.

4.2 L-Diversity

We utilize the L-Diversity technique to secure the user position (latitude and longitude) by generating a group that has distinct traits so that no hackers can identify information.
From the aforesaid data, the hacker may know patients' addresses as to the zip code and age but cannot still identify patients' illnesses as the patient's age and zip code are anonymous; and a patient the hacker is looking for may not be identified. The location will also be anonymous during the transfer of user latitude and longitude to LBS.
We have built two applications to implement this project
a. Service LBS: This server will hold the location dataset, then this server will receive the user's encrypted query, and then look at places using Euclidean Distance to discover nearby places and return the answer to the user.
b. Mobile users: type the query and its latitude and longitude and then encrypt the data and send it to the nearby LBS server.

Table 1. F-quota value contrast among two cities with LBS privacy "on

F-Quota Values	CITY-1	CITY-2
0.74	0.9	0.88
0.76	0.85	0.86
0.78	0.88	0.85
0.8	0.85	0.85
0.82	0.85	0.83
0.84	0.87	0.86
0.86	0.88	0.87
0.9	0.89	0.88
0.92	0.9	0.88

Higher F-quota values were noted in city 1. Because city 2 has more

population, properties and vehicles than city 1, the authority and strength of the

quota beliefs can be familiar to modify.

Table 2. F-quota value contrast among two cities with LBS privacy "off

F-Quota Values	CITY-1	CITY-2
0.34	0.46	0.45
0.36	0.43	0.42
0.38	0.45	0.43
0.4	0.43	0.42
0.42	0.42	0.41
0.44	0.44	0.43
0.46	0.45	0.44
0.48	0.46	0.44

When the rejection that the F-quota values are close to half of the F-quota values. Our proposed LBS seclusion protection access provides automatically better locality seclusion and user invisibility.

Conclusion

In an increasingly linked society, ensuring the privacy of LBS users is vital. In order to safeguard user privacy efficiently, we build an efficient PPCS approach which efficiently generates foolish places for

which we take into account the semanticities of the locations that hackers can utilise. Our suggested PPCS approach can produce stupid spots that do not include a user's real location and prevent collusion and inference attacks. Our PPCS technique can be seen in the outcomes of the simulation. Our PPCS approach has an average optimization of 85% and 60% on E(X) and Region of Interest metrics, in comparison with previous approaches. However, preserving the privacy of the trajectory in LBS is a challenge for mobile users. We will design effective frames and algorithms for protecting the privacy of users in LBS in our future work.

References

[1] G. Sun, S. Sun, J. Sun, H. Yu, X. Du, and M. Guizani, ‘‘Security and privacy preservation in fog-based crowd sensing on the Internet of vehicles,’’ J. Netw. Comput. Appl., vol. 134, pp. 89–99, May 2019.

[2] R. Gupta and U. P. Rao, ‘‘An exploration to location based service and its privacy preserving techniques: A survey,’’ Wireless Pers. Commun., Int. J., vol. 96, no. 2, pp. 1973–2007, 2017.

[3] G. Sun, Y. Xie, D. Liao, H. Yu, and V. Chang, ‘‘User-defined privacy location-sharing system in mobile online social networks,’’ J. Netw. Comput. Appl., vol. 86, pp. 34–45, May 2007.

[4] C.-Y. Chow, M. F. Mokbel, and X. Liu, ‘‘A peer-to-peer spatial cloaking algorithm for anonymous location-based service,’’ in Proc. 14th Annu.ACM Int. Symp. Adv. Geographic Inf. Syst., 2006, pp. 171–178.

[5] H. Shen, G. Bai, M. Yang, and Z. Wang, ‘‘Protecting trajectory privacy: A user-centric analysis,’’ J. Netw. Comput. Appl., vol. 82, pp. 128–139, Mar. 2017.

[6] M. Ghaffari, N. Ghadiri, M. H. Manshaei, and M. S. Lahijani, ‘‘P4QS: A peer-to-peer privacy preserving query service for location-based mobile applications,’’ IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 9458–9469, Oct. 2017.

[7] K. Shi, M. Xu, H. Jin, T. Qiao, X. Yang, N. Zheng, J. Xu, and K.-K. R. Choo, ‘‘A novel file carving algorithm for national marine electronics association (NMEA) logs in GPS forensics,’’ Digit. Invest., vol. 23, pp. 11–21, Dec. 2017.

[8] M. Gruteser and D. Grunwald, ‘‘Anonymous usage of location-based services through spatial and temporal cloaking,’’ in Proc. 1st Int. Conf. Mobile Syst. Appl. Services, 2003, pp. 31–42.

[9] Z. Zhou, H. Zhang, X. Du, P. Li, and X. Yu, ‘‘Prometheus: Privacy-aware data retrieval on hybrid cloud,’’ in Proc. IEEE INFOCOM, Apr. 2013, pp. 2643–2651.

[10] G. Sun, D. Liao, H. Li, H. Yu, and V. Chang, ‘‘L2P2: A location-label based approach for privacy preserving in LBS,’’ Future Gener. Comput. Syst., vol. 74, pp. 375–384, Sep. 2016.

[11] R. Gupta and U. P. Rao, ‘‘Achieving location privacy through CAST in location based services,’’ J. Commun. Netw., vol. 19, no. 3, pp. 239–249, 2017. [12] B. Gedik and L. Liu, ‘‘Protecting location privacy with personalized k-anonymity: Architecture and algorithms,’’ IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 1–18, Jan. 2008.

[12] B. Ying and D. Makrakis, ‘‘Protecting location privacy with clustering anonymization in vehicular networks,’’ in Proc. IEEE INFOCOM WKSHPS, Apr./May 2014, pp. 305–310. [14] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, ‘‘Traffic-aware multiple mix zone placement for protecting location privacy,’’ in Proc. IEEE INFOCOM, Mar. 2012, pp. 972–980.

[13] L. Wu, X. Du, and J. Wu, ‘‘Effective defense schemes for phishing attacks on mobile computing platforms,’’ IEEE Trans. Veh. Technol., vol. 65, no. 8, pp. 6678–6691, Aug. 2016.

[14] S. Gang, S. Liangjun, L. Dan, Y. Hongfang, and C. Victor, ‘‘Towards privacy preservation for ‘check-in’ services in locationbased social networks,’’ Inf. Sci., vol. 481, pp. 616–634, May 2019.

[15] X. Zhu, H. Chi, S. Jiang, X. Lei, and H. Li, ‘‘Using dynamic pseudo-IDs to protect privacy in location-based services,’’ in Proc. IEEE ICC, Jun. 2014, pp. 2307–2312.

[16] J. Shao, R. Lu, and X. Lin, ‘‘FINE: A fine-grained privacy-preserving location-based service framework for mobile devices,’’ in Proc. IEEE INFOCOM, Apr./May 2014, pp. 244–252.

[17] Casas-Roma, J., Herrera-Joancomartí, J. and Torra, V. (2016) ‘A survey of graph-modification techniques for privacy-preserving on networks’, Artificial Intelligence Review,. doi: 10.1007/s10462-016-9484-8

[18] Jain, P., Gyanchandani, M. and Khare, N. (2016) ‘Big data privacy: A technological perspective and review’, Journal of Big Data, 3(1). doi: 10.1186/s40537-016-0059-y

[19] Li, N., Li, T. and Venkatasubramanian, S. (2007) ‘Tcloseness: Privacy beyond k-anonymity and l-diversity’, ICDE 2007 IEEE 23rd International Conference on Data Engineering, doi: 10.1109/icde.2007.367856.

[20] Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M. (2007) ‘L -diversity: privacy beyond k-anonymity’, ACM Transactions on Knowledge Discovery from Data, 1(1). doi: 10.1145/1217299.1217302.