ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

Security in Geo-Social Applications Through Preserving Location Privacy

Dhanashree Patil[1], Yogeshwari S. Borse[2]

P.G. Student, Department of Computer Engineering,SSBT's COET, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering,SSBT's COET, Maharashtra, India[2]

ABSTRACT: Location privacy protection is an imperative issue in day by day life. The user needs to takecare of their information. A large number of individuals collaborate with their surroundingsthrough their companions and their suggestions. Without satisfactory protection, however,these frameworks can easily abuse, e.g., to track users or target them. The proposed protocolgives a simple approach to secure location information. Silent features of location privacyprotection protocol are to give security to location data with enhancing the performance. Itpermits all location queries to be evaluated effectively by the server, the proposed securitysystem ensure servers can't see or construe the real location information from the changedinformation. Results, thus obtained, shows the proposed protocol uses less query processingtime, less server processing time for location privacy in geo-social application.

KEYWORDS: LBS, LocX, Longitude, PIR, kNN.

I. INTRODUCTION

With the advance of location technologies, people can now determine their location in various ways, for instance, with GPS or based on nearby cellphonetowers. These technologies have lead to the introduction of location based services, which allow people to get information relevant to their current location. Location privacy is of utmost concern for such location based services, since knowing a persons location can reveal information about activities or interests. Location based Services (LBS), for example, are used by millions of users every day to obtain location specific information. Two popular features of location based services are location check ins and location sharing. By checking into a location, users can share their current location with family and friends or obtain location specific services from third party providers. The obtained service does not depend on the locations of other users.

Privacy is generally the information that don't want others to know. Location privacy is defined as the ability to prevent other unauthorized (or malicious) parties from learning ones current or past location. With the popularity of LBS, users privacy information has aroused much concern. The location information shared by LBS may be text based or it may be map based, where the users location is represented as a dot on a map. To display location information, users can manually enter a street address or longitude and latitude coordinates. Location based services can be categorized into three types based on their location privacy requirements. The first type of LBSs refers to those location based servicesthat can operate completely anonymously, the second type of LBSs refers to the location based services that cannot work without the user's identity, and last Private Information Retrieval (PIR) techniques, which allow a user to issue a service request to a service provider without the service provider learning the content of the request [1].

A complete LBS system comprises of various players such as content providers, network operators, virtual operators, service administrators, financial parties and other service providers etc. The user has to expose its location information against the services provided by the LSPs and at the same time user has a risk of disclosure of its personal information also. For obtaining a complete location based service, many parties are involved and thus the personal information of user is potentially known by many different services or content providers or other parties. Thus, proliferation of personal information among the different parties is difficult to control. It requires a sophisticated access control mechanism along with an appropriate authentication system [2].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

II. RELATED WORK

Location privacy of the users is a very big concern. Location privacy has been the area of interest of many researchers. Many solutions have been propounded in regard to location privacy. Without privacy protection, these systems can be easily misused. So privacy must be provided in order to preserve the location of the users. This section summarizes the main contributions of other researchers on location privacy in geo-social application.BlessyRajra M B and A J Deepa, in [3], presents system and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Igor Bilogrevic et al., in [4], presents the problem of predicting a users perceived utility loss due to obfuscation is highly intertwined with the problem of identifying why the user shares her location in the first place. It propose to infer the motivation of the user in sharing her location, and then to predict the utility implications of a privacy-protection mechanism on the users experience with respect to that particular motivation. Arvind Narayanan et al., in [5], propose a privacy-preserving tests for closet location: Alice test if she is near to Bob without either party revealing any other information about their location. It describe several secure protocols that support private proximity testing at various levels of granularity. A proximity testing protocol with a synchronous communication pattern requires both parties to be online at the same time. Chow et al., in [6], presents the distributed approach for location k-anonymity. A user who wants to access a location based service broadcasts a message with Bluetooth or WiFi. Nearby users respond to the message with their current location. Ghinita et al., in [7], presents the approach often fails to achieve location privacy, since the query issuer tends to be in the center of the cloaked area. The same authors later show that their earlier approach can be slow and propose an approach based on a distributed hash table. Kapadia et al., in [8], proposed a statistical k-anonymity. They assume the global availability of statistical data about the number of people who are present in an area with high probability at a particular time of the day. Zhong et al., in [9], presents a scenario where database records are horizontally distributed among different sites. They present an algorithm that allows a data miner to learn the sensitive part of a record only if there are least k-1 other records, maybe at different sites, whose non-sensitive part is identical to the non-sensitive part of the record in question. AmirrezaMasoumzadeh and James Joshi, in [10], proposed a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing. Jia-Dong Zhang and Chi-Yin Chow, in [11], proposed a reciprocal protocol for location privacy (REAL) in WSNs. In REAL, sensor nodes are required to autonomously organize their sensing areas into a set of non-overlapping and highly accurate k-anonymized aggregatelocations. Changyu Dong and NarankerDulay, in [12], proposed LocX is longitude which also transforms locations coordinates to prevent disclosure to the servers. However, in longitude, the secrets for transformation are maintained between every pair of friends in order to allow users to selectively disclose locations to friends. Stavros Papadopoulos et al, in [13], presents methods for arbitrary kNN search with strong location privacy. Krishna P. N. Puttaswamy et al., in [14], proposed a LocX Protocol. LocX uses the inexpensive symmetric encryption. The closest work to LocX is Longitude, which is transforms locations coordinates to prevent disclosure to the servers. Matt Blaze et al., in [15], proposed the design of Longitude is based on proxy re-encryption. In a proxy re-encryption scheme, a ciphertext encrypted by one key can be transformed by a proxy function into the corresponding ciphertext for another key without revealing any information about the keys and the plaintext. Janice Y. Tsai et al., in [16], observed existing location sharing services do offer the users some form of controls over their privacy. The authors examine 89 location sharing services and the most widely adopted privacy controls are white list, being invisible, blacklist, groupbasedpermission and providing less detailed location. Alastair R. Beresford and Frank Stajano, in [17], presents previous research on location privacy has focused on anonymisation. Julien Freudiger et al., in [18], proposed a location sharing services, the provider usually acts as a broker to disseminate the location information to the authorised receivers.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

III. PROPOSED APPROACH

The proposed protocol is designed to less number of transactions in query for location privacy. In proposed approach there are two algorithms. The algorithms are as follows.

A. *Algorithm for storing data*

Algorithm for storing data takes inputs as dataset. It generate the key value. Latitude and longitude are encrypted. These records are placed at index server. Then venue and revieware encrypted and return result.

Require: U : User, K : Key for user, R : Single record from dataset, I : Index Server, S : Data Server, Lat : Latitude, Lng : Longitude, Vid : Venue id, Rn : Review, Ed : Encrypted Data, Ln : List of dataset records
Step 1: Input dataset
Do
Step 2 : Read record R
Step 3 : Clean or remove invalid data record
Step 4 : Generate Key value, K
Step 5 : Encrypt data Ed
Ed= E(lat), E(lng)
Step 6: Place records at Index Server I
I= Ed
Step 7: Generate venue id Vid and store to Data Server
Step 8: Encrypt data Ed at Data Server S
Ed=E(Vid), E(Rn)
Step 9: Display Values to user U
While
all records are uploaded successfully
i.e. while Ln=0

B. *Algorithm for Retrieving data*

In algorithm for retrieving data, user login using user id and password. Validate user credentials. User request location data. User gives secret key. If secret key are correct retrieve venue index from index server. Then retrieve reviews information from data server. Display decrypted data review to user.

Require: U : User, K : Key for user, I : Index Server, S : Data Server, Ld : Location Data, Rn : Review, Vi : Venue index, Dd : Decrypted Data, Un : Username of user, Pn : Password for user, Vid : Venue id, Rid : Requested user

Step 1 : User login using credentials Un &Pn
Step 2 : Validate user credentials
Step 3 : Request for location data Ld
Ld=Request(Vid)
Step 4 : Enter key value, K for validation
Step 5 : Validate key
Step 6 : Retrieve Venue Index from Index Server I
Vi=I(Vid)
Step 7: Retrieve reviews information from Data Server S
Rn=Dd(Rid)
Step 8 : Display decrypted data Dd to user U

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

IV. EXPERIMENTS AND EVALUATION

Experimental result present the effectiveness of proposed system, in which involvement of proposed protocol is proved better by carrying out experiment. Results are carried out using java. Brightkite dataset includes long-term (about 10 months) check-in data. The results shows the proposed protocol provide location privacy. In proposed protocol it uses less query completion time, less server processing time & less message size. The graphical representation is shown in Figure 1, Figure 2 and Figure 3.

Figure 1 shows Message Size. When the no. of data location is 5, message size is 51 KB. When the no. of data location is 10, message size is 55 KB. & when the no. of data location is 15, message size is 55 KB. When the no. of data location is 20, message size is 47 KB.

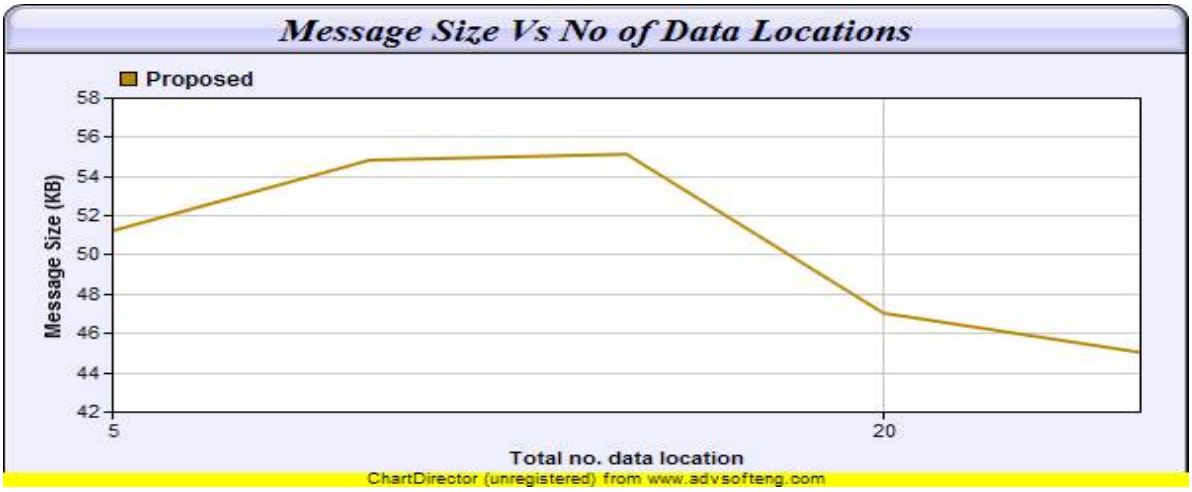

Figure 1: Message Size

Figure 2 shows Query Completion Time. When the no. of data location is 5, query completion time is 51 ms. When the no. of data location is 10, query completion time is 54 ms.& when the no. of data location is 15, query completion time is 39 ms. When the no. of data location is 20, query completion time is 38 ms.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

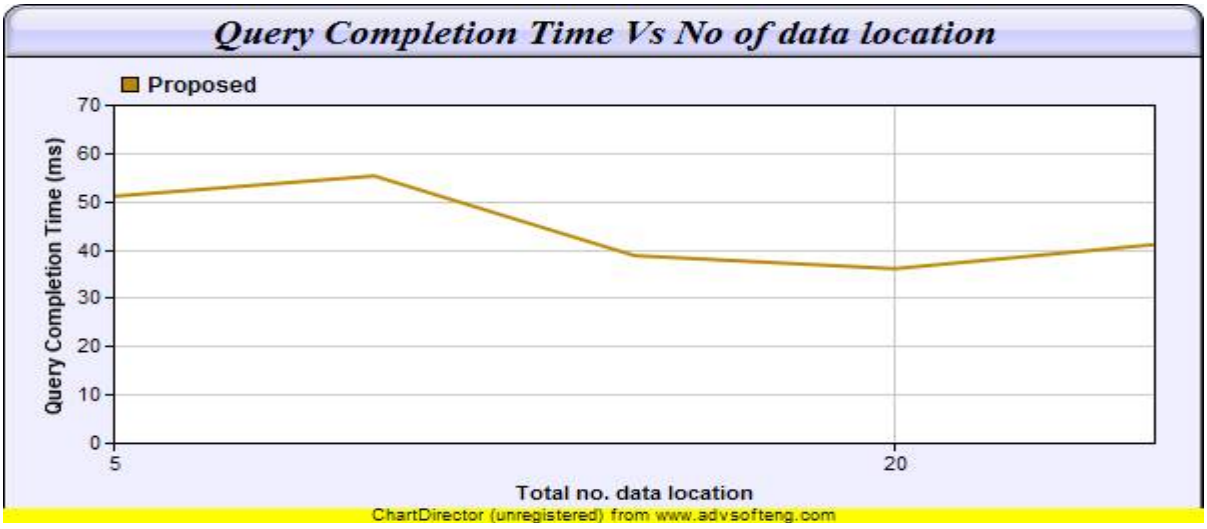

Figure 2: Query Completion Time

Figure 3 shows Server Processing Time. When the no. of data location is 5, server processing time is 50 ms. When the no. of data location is 10, server processing time is 130 ms.& when the no. of data location is 15, server processing time is 107 ms. When the no. of data location is 20, server processing time is 127 ms.

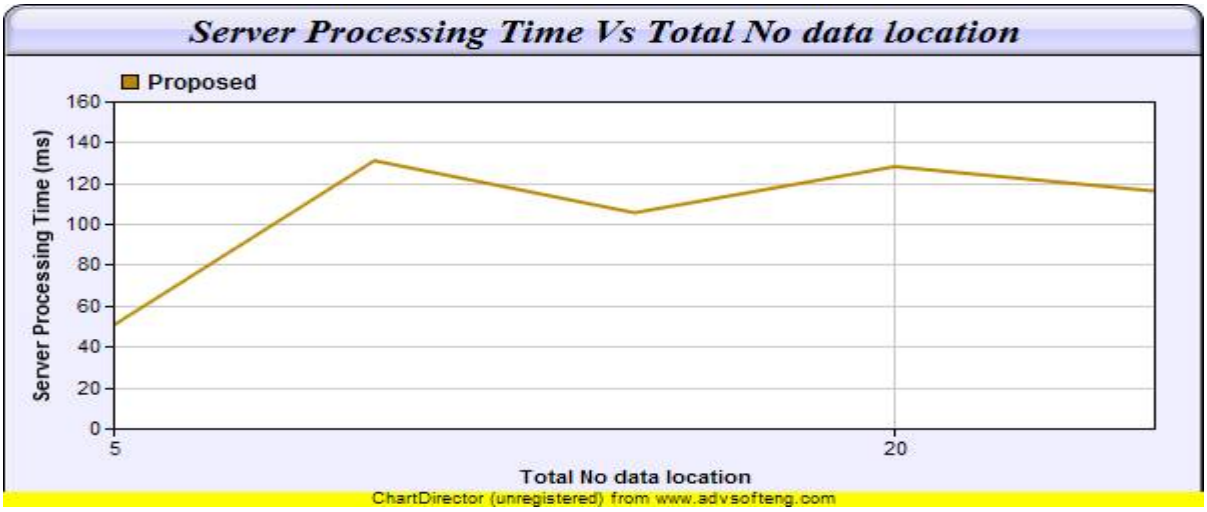

Figure 3: Server Processing Time

V. CONCLUSION AND FUTURE WORK

Proposed protocol takes a novel approach to provide location privacy while maintaining overall system efficiency. In proposed protocol, users efficiently transform all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. Only friends with the right keys query and decrypt a user data. The experiment results shows the proposed protocol it uses less query processing time, less server processing time for location privacy in geo-social application. It observe the proposed protocol give the best results in location privacy.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

It would be a point of research to increase security by extending the proposed algorithms to include cases where users have several prioritized locations preferences.

REFERENCES

1. Amit Kumar Tyagi and N. Sreenath, "A Comparative Study on Privacy Preserving Techniques for Location Based Services", BJMCS, Vol. 10, No. 4, pp. 1-25, January 2015.
2. PritiJagwani and SarojKaushik, "Privacy in Location Based Services: ProtectionStrategies, Attack Models and Open Challenges", International Conference on InformationScience and Applications, Vol. 10, No. 4, pp. 12-21, 2017.
3. BlessyRajra M B and A J Deepa, "A Survey on Network Security Attacks and PreventionMechanism", Journal of Current Computer Science and Technology, Vol. 5, No. 2,pp. 1-5, February 2015.
4. Igor Bilogrevic, MurtuzaJadliwala, Vishal Joneja, KbraKalkan, and Jean-PierreHubaux, "Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices",IEEE Transactions on Information Forensics And Security, Vol. 9, No. 7, pp.1-16, July 2014.
5. Arvind Narayanan, NarendranThiagarajan, MugdhaLakhan, Michael Hamburg, andDan Boneh, "Location Privacy via Private Proximity Testing", in Proc. of NDSS, pp.1-17, 2011.
6. C.-Y. Chow, M. F. Mokbel, and X. Liu, "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services", in Proceedings of 14th ACM International Symposium on Advances in Geographic Information Systems (ACM-GIS06), pp. 171-178, November 2006.
7. Gabriel Ghinita, PanosKalnis, and SpirosSkiadopoulos, "PRIVE: AnonymousLocation-Based Queries in Distributed Mobile Systems", in Proceedings of 16th InternationalWorld Wide Web Conference (WWW2007), pp. 371-380, May 2007.
8. Apu Kapadia, Nikos Triandopoulos, Cory Cornelius, Daniel Peebles, and David Kotz,"AnonySense: Opportunistic and Privacy Preserving Context Collection", PervasiveComputing, pp. 280-297, May 2008.
9. Sheng Zhong, Zhiqiang Yang, and Tingting Chen, "k-Anonymous data collection", InformationSciences, Vol. 179, No. 17, pp. 2948-2963, August 2009.
10. AmirrezaMasoumzadeh and James Joshi, "An Alternative Approach to k-Anonymityfor Location-Based Services", Procedia Computer Science, Vol. 5, pp. 522-530, 2011.
11. Jia-Dong Zhang and Chi-Yin Chow, "REAL: A Reciprocal Protocol for Location Privacyin Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing,Vol. 12, No. 4, pp. 458-471, July-Aug 2015.
12. Changyu Dong and NarankerDulay, "Longitude: a Privacy-preserving Location SharingProtocol for Mobile Applications", IFIP International Conference on Trust Management,pp. 133-148, 2011.
13. Stavros Papadopoulos, SpiridonBakiras, and DimitrisPapadias, "Nearest NeighborSearch with Strong Location Privacy", Proc. VLDB Endowment, Volume 03, No. 1-2,pp. 619-629, Sept 2010.
14. Krishna P. N. Puttaswamy, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, AmrEl Abbadi, Christopher Kruegel, and Ben Y. Zhao, "Preserving Location Privacy inGeosocial Applications", IEEE Transactions on Mobile Computing, Vol. 13, No. 1, pp.159-173, January 2014.
15. Matt Blaze, GerritBleumer, and Martin Strauss, "Divertible protocols and atomicproxy cryptography", Advances in Cryptology-EUROCRYPT'98, pp. 127-144, 1998.
16. Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh,"Location-sharing technologies: Privacy risks and controls", ISJLP, Vol. 6, No. 119,pp. 1-26, February 2010.
17. Alastair R. Beresford and Frank Stajano, "Location privacy in pervasive computing",IEEE Pervasive computing, Vol. 2, No. 1, pp. 46-55, Jan-Mar 2003.
18. Julien Freudiger, Raoul Neu, and Jean-Pierre Hubaux, "Private sharing of user locationover online social networks", HotPETs, EPFL-CONF-152141, pp. 1-12, 2010.