International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Maintaining Privacy in Location Sharing Using LOCX

Syeda Maimuna Afreen[1], Shameem Akther[2]

[1]Master Of Technology, Department of Computer Science and Engineeing , Visvesvaraya Technological University, Khaja Bamda Nawaz College Of Engineering Gulbarga, Karnataka, India

[2]Associate Professor, Department of Computer Science and Engineeing , Visvesvaraya Technological University, Khaja Bamda Nawaz College Of Engineering Gulbarga, Karnataka, India

Abstract: ***Four Square is one of the Geosocial application in which lots of communities interrelate with their surrounding environmentthrough their friends and their recommendations. Regarding the security issues Geosocial application can simply misused, for instance to trace the user or target them for home invasions. Therefore providing the privacy to the Geosocial application is the research issue, existing system provides location privacy without adding uncertainty into the query results or relying on strong assumptions about server security. In existing system user will share only the location with its other users but this sharing is not up to the mark secure. Therefore in the proposed system which provides the security to the user's location as well as the contents will also be shared with the other users. By using our proposed system cost of the server database will decrease and the time required for transmitting the message is also decreases. The system encrypts the message for the security purpose. The proposed method provides privacy and improves the performance of the Geosocial application.***

Keywords: Location privacy, Security, Location-based services, Geo-social applications, location transformation, efficiency**.**

1. Introduction

Geo-social networks (GeoSNs) provide a context-aware service that helps to associate location with users and content. The proliferation of GeoSNs indicates that they're rapidly attracting users. GeoSNs currently offer different types of services, including photo sharing, friend tracking, and "check-ins." However, this ability to reveal users locations causes new privacy threats, which in turn call for new privacy-protection methods. The authors study four privacy aspects central to these social networks - location, absence, co-location, and identity privacy - and describe possible means of protecting privacy in these circumstances.

In today's world, Smartphone applications have become popular among the users enhancing computing platform. A type of application is coming into line light that can be put under the category of geo-social application. Examples of this social application are local friend recommendation for dining and shopping, as well as games and collaborative network services. But, it has been noticed that these application prove disadvantages as there is a risk of losing users privacy, at present due to minimal privacy mechanism. User's all know about the "places" feature of facebook which was misused by some thieves. Hence, there is a real need for stronger privacy properties in order to make it more-friendly to the users.

Now-a-days, Geo-social application have become part and parcel of human lives. But, these may be misused by someone to extract user's personal information. LocX tends to provide with improved privacy and with result quite certain. The primary thing that is done is to use secure coordinate transformation. This transformation would be used only by friends of a particular user. It allows the server to work properly and correctly without accessing the private data of the user. There are users where there is not a need for arbitrary pairs of users to be resolved. Hence, by distinguishing such location data through users social groups and further transformation can be used on location coordination. The coordinate transformations preserve distance metrics, enhancing the task of server to perform queries on transformed data. The transformation is a safe one, since the key is secret which knows only to the users group.

The proposed system uses the LocX technique. LocX algorithm is used for securely sharing. This technique is fast and simple to apply. Since this is a lossless compression technique, none of the contents in the file are lost during or after compression. Sender first sends GPS location. Like the LocX technique use transforms the co-ordinates and save those on to the index sever .The compression method is used the compress the file and then apply the encryption. This technique has advantages of being able to send large files to the mobile devices which has less memory than the normal computers The system in which the compression technique is used while user send the message to the another user so the another user initially user encrypt the message by the encryption algorithm and after that compress the message and send to another user. Additionally user adds key hash and random hash tags for improving the privacy and performance of the system. Key hash is significantly more efficient than no tags in terms of processing time on the user's device, while providing the same, strong privacy. The random hash provides both high privacy and high efficiency.

2. Existing System

In the existing system the basic design of LocX is used but this design is not up to the mark secure because the location that is been shared with the users is prone to be attacked by the users for the purpose of invasions. The main drawback of this system is security is not maintained. Here only

location sharing is been done whereas the proposed work involves sharing of location along with its associated contents. Earlier an application called as Foursquare was used by the users for carrying out location sharing with the other users using the normal text messaging concept provided by the mobile companies but this application is not maintaining security due to which we had to move to a model called as LocX. With the help of this model it is possible to share the location in a systematic and sophisticated manner with the other users in an encrypted format by retaining privacy to the location that is being shared by the users. Along with location sharing this model also provides the facility of sharing the contents also. Using the FourSquare application it was not possible to share the contents of the location and another major drawback of this application was privacy was getting violated. To overcome all these drawbacks a model called as LocX is used which fulfils all the drawbacks of the above application FourSquare. This model supports point queries, circular range queries, and nearest neighbour queries. Point queries are the queries which will provide only a particular information location. Circular range queries are the queries which will provide all types of location information and lastly the nearest neighbour queries are the queries which will provide the nearest location information. With the help of this model it is possible to find as well as share all types of locations. The challenge faced by the users is to maintain privacy while carrying out sharing of location in such a way that it should not affect the actual location information.

The following figure 1 shows the basic design of LocX. In this figure there are two users Alice and Bob and one server LBS. Alice shares some location with bob which will first get transformed into co-ordinate values and in an encrypted format gets stored in the LBS server. Bob will fetch the encrypted results from the LBS server and decrypts it using the secret key sent through email by Alice. This is how locations were shared using the basic design of LocX.

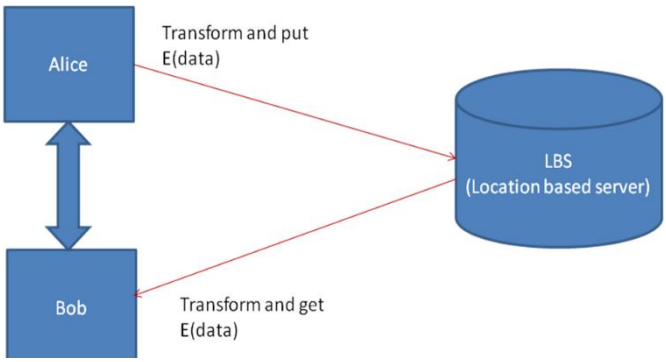

Figure 1: Basic design of LocX

3. Proposed System

The following figure 2 is the modified design of LocX

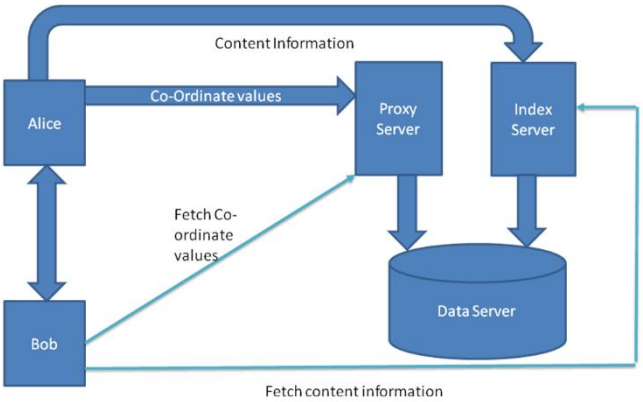

Figure 2: Modified design of LocX

In figure 2, there are two users Alice and Bob, three servers i.e. proxy server, index server and data server. The job of proxy server is to store the co-ordinate values in an encrypted format. The job of index server is to store the content information in an encrypted format. The job of data server is to maintain the history of locations that is being shared with the users. Alice first sends the location to bob before reaching to bob the location first gets converted to co-ordinate or latitude and longitude values and gets stored in an encrypted format in the proxy server. This movement of encrypted data to proxy server is possible through an application programming interface called as Put L2I. Similarly the content information will move from Alice to the index server in an encrypted format using an application programming interface called as Put D2I. The data present in proxy and index server will be stored as a copy in the data server. Now Bob has to login to both the servers one after the other to fetch the information. Once the information is fetched, Bob will use the secret key which is sent by Alice to Bob through email in order to decode the message and view the original data that is shared by Alice.

There are multiple reviews present for the same location whether from user's social group or from the unknown users, to distinguish between these two groups we can use the hash code. So the index server contains the one more field for the hash code which can be checked by the user's friend to retrieve the actual review from his social group.To resolve the name conflicts i.e. same names for the different places the system uses special tags. To improve the performance of retrieval of data from the data server we can use the compression mechanism which compresses the reviews and stores it to the data sever.

When user's friend wants to access the reviews for the specified location again he transforms the co-ordinates and sends the query to the index server. Then he retrieves the index by using secrete key .After retrieving the index a separate query will be fired on to the data server to fetch the review. The review will first decompressed and then decrypted with the same secrete key.In this way the recommendations can be securely communicated with in the user's social circle without exposing his location to the outside world.

The following figure 3 shows the overview of system operations

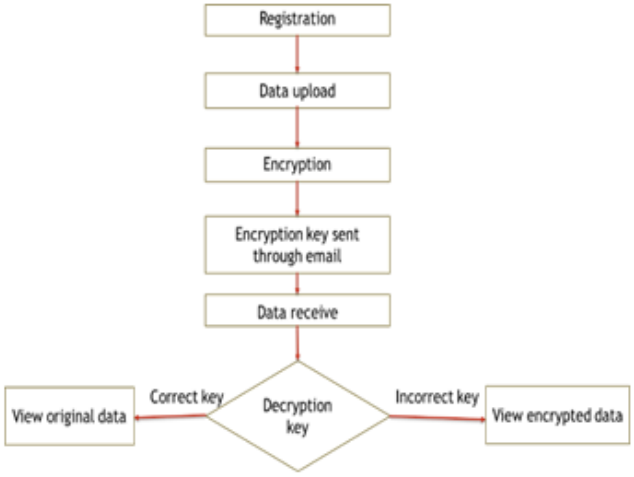

Figure 3: Overview of System Operations

The above diagram provides the complete overview of the project. First block represents registration, it means that first the user should get registration and only the registered users will be allowed to share the location with the other users. The location that is being shared with other users even those users must also be registered. Once the registration is done then the user will be allowed to upload the data. After data uploading encryption will be carried out on the data that is uploaded for the purpose of sharing. Encryption is done using the standard AES encryption algorithm. The secret key will be sent through email. The second user with whom the data is being shared needs to decrypt the message and for decryption also standard AES decryption algorithm is used. Decryption will be carried out by the user using the secret key that is sent to the mail by the sender. If the user enters the correct secret key then he will be able to view the original data. If the entered secret key is incorrect then the user will be able to view the data but in an encrypted format.

System uses following algorithms in our system:

1. AES Encryption
We are using the AES Encryption algorithm, instead of any other, is because of the security that it provides. Here, the user location information will be encrypted before it is sent to the server for storage purpose. Therefore, even if the attacker gets this information somehow, it won't be able to access it.

2. AES Decryption
The decryption algorithm is used to for decrypting the user location data, when the actual data will be necessary for the processing.

4. Related Work

(M. Motani, V. Srinivasan, and P.S. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. ACM MobiCom, 2005).In earlier days people were great sources of unique information but today social networking sites are helping people to obtain any type of information. The aim of "People Net: Engineering a wireless virtual social network" is a wireless social network is used which mimics the way people seek information from other people. The term information refers to only location specific information. The information will be fetched by the users only if both are within the Bluetooth range.

(M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007).The aim of privacy aware location based database server is to allow sharing of anonymous location information among the users. Anonymous location information means unnamed location information. This is possible by using a framework called as CASPER. Casper is implemented as a standalone application.

(P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007).The aim of preventing location based identity inference in anonymous spatial networks is to find the nearest location without revealing the location of the user who is finding the location. To implement this approach two servers are used anonymizer and location based server. The user will first send the request query to the anonymizer but not to the LBS because LBS is not trustworthy, as other users can collaborate with the LBS to find out the location of the user who has issued the request query. The advantage of sending it to the anonymizer is the user ID will be removed from request query and then it will be forwarded to the LBS.

(A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011).Private proximity enables a pair of users to be notified when they are present within the threshold range but location of users will not be revealed. An algorithm called as BerkleyKamp Massey is used to implement this approach.

(Julien Freudiger, Raoul NE, and Jean-Pierre Hubbub," Private sharing of user location over online social networks").Online social networks increasingly allow mobile users to share their location with their friends. Much to the detriment of users' privacy, this also means that social network operators collect users' location. Similarly, third parties can learn users' location from localization and location visualization services. Ideally, third-parties should not be given complete access to users' location. To protect location privacy, we design and implement a platform-independent solution for users to share their location in a private fashion over online social networks. Our solution relies on encryption to enforce access control and uses dummy queries and caching to protect localization and location visualization.

(B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing Magazine, vol. 5, no. 4, pp. 38-46, Oct. 2006).Intelligent transportation systems increasingly depend on probe vehicles to monitor traffic: they can automatically report position, travel time, traffic incidents, and road surface problems to a telematics service provider. This kind of traffic-monitoring system could provide good coverage and timely information on many more roadways than is possible with a fixed infrastructure

such as cameras and loop detectors. This approach also promises significant reductions in infrastructure cost because the system can exploit the sensing, computing, and communications devices already installed in many modern vehicles. This architecture separates data from identities by splitting communication from data analysis. Data suppressiontechniques can help prevent data mining algorithms from reconstructing private information from anonymous database samples.

(A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location- Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004).Privacy of personal location information is becoming an increasingly important issue. We refine a method, called the mix zone, developed to enhance user privacy in location-based services. We improve the mathematical model, examine and minimize computational complexity and develop a method of providing feedback to users. Traditionally, privacy of personal location information has not been a critical issue but, with the development of location tracking systems capable of following user movement twenty-four hours a day and seven days a week, location privacy becomes important: records of everything from the shelves you visit in the library to the clinics you visit in a hospital can represent a very intrusive catalogue of data. Location privacy is an important new issue and several strategies have been suggested to protect personal location information. The first strategy is to restrict access. The Geographic Location/Privacy (Geopriv) Working Groups have outlined an architecture to allow users to control delivery and accuracy of location information through rule-based policies.

5. Results and Discussions

The basic design of LocX which was used in the existing system is not up to the mark secure because the location that is being shared using the basic design is not safe, as there is a possibility that the location information will be leaked or an attacker can attack the system to fetch the shared information. The modified design of LocX will overcome this drawback by maintaining high security while carrying out location sharing and the main modification that is been carried out here is the contents are shared using the modified design of LocX

6. Conclusion

This paper explains the design, prototype implementation, and evaluation of LocX, a system for building location-based social applications (LBS) while preserving user location privacy. LocX provides location privacy for users without injecting uncertainty or errors into the system, and does not rely on any trusted servers or components. LocX uses an approach to provide location privacy while maintaining overall system efficiency, by leveraging the social data-sharing property of the target applications. In LocX, users efficiently convert all the locations shared with the server and encrypt all location data stored on the server using inexpensive keys. Only users with the right keys can query and decrypt a user data. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties. Using evaluation method based on both synthetic and real-world LBS traces, we find that LocX adds little computational and communication overhead to existing systems. Our LocX prototype runs efficiently even on resource constrained mobile phones. Overall, we believe that LocX takes a big step toward making location private.

References

[1] M. Motani, V. Srinivasan, and P.S. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. ACM MobiCom, 2005.
[2] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: A Privacy-Aware Location-Based Database Server," Proc. IEEE 23rd Int'l Conf. Data Eng., 2007.
[3] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.
[4] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," Proc. Network Distributed System Security Conf., 2011.
[5] Julien Freudiger, Raoul NE, and Jean-Pierre Hubbub," Private sharing of user location over online social networks"
[6] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing Magazine, vol. 5, no. 4, pp. 38-46, Oct. 2006. [7] A. Beresford and F. Stajano, "Mix Zones: User Privacy in Location- Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing Comm. Workshop, 2004.