International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Secured Location Sharing Services for Social Networks

Jayaprabha M S[#1], Krupa R[*2], Lavanya K M[#3], Mamatha K[#4], Jagadamba A[#5]
**Asst Professor, #UG in Computer Science and Engineering*
Vemana Institute of Technology,
#1, Mahayogi Vemana Road, 3rd Block, Koramangala, Bangalore - 560034, India

Abstract*- Using Social Networks, such as Four Square, millions of people interacts with their surroundings through their friends and their recommendations. Without an adequate privacy protection, these systems can be easily misused, e.g., to track users or to target them for home invasion. In this paper, we introduce Location X, an alternative that provides significantly improved location privacy without adding errors into the query results or without depending on assumptions about server security. Our key insight is to apply secure user specific, distance preserving coordinate transformations to all the location data shared with the server. The friends of a user share this user's secrets, so they can apply the same transformations. Which allows all the location queries to be evaluated correctly by the server, but our privacy mechanism guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that location X provides privacy even against a powerful adversary model.

Keywords* - Location privacy, Location sharing services, Location based social networking, Spatial-temporal query processing.

I. INTRODUCTION

Location based services are software level information services to identify the location of a person or an object, such as discovering the current location of a friend and notify when a friend is in a certain distance, discovering the nearest restaurants by making use of GPS, it also includes vehicle tracking services, mobile commerce etc. Location based services for social networks today will enable the user to build social relations with the other people, and they can also provide the recommendations to a person or place, e.g, Face book's places, Four Square, Google Plus. Existing systems have mainly taken three approaches to improve the user privacy in geo-social systems: (1) Introducing uncertainty, (2) Introducing error into location data relying on trusted servers, (3) Intermediaries to apply anonymization to user identities and private data relying on heavy weight cryptographic techniques. None of them have proven successful on current application platforms. As users dislike the loss of accuracy in the results, private data can be exposed by software bugs and they are too expensive to arrange on mobile devices and even on the servers in providing queries such as nearest neighbor.

To clarify the need for each component in Location X, design description is started with a basic, simple design. The server supports different types of queries (point, circular range and nearest neighbor queries) on location data. For the server to be able to do this, we need to reveal the location coordinates in plain text. But doing so would allow the malicious server to break a user's location privacy. To resolve this problem, the idea of coordinate transformation is proposed. Each users in the system chooses a set of secrets that they reveal only to their friends. These secrets include a rotation angle θ, a shift angle and a symmetric key. The users exchange their secrets via interactions when friends meet-in person, or via a separate trusted channel, such as email, phone etc. The secret angle and shift angle are used by the users to transform all the location coordinates they share with the servers. Similarly, the secret symmetric key is used to encrypt all the location data they store on the servers. These secrets are known only to their friends, and hence only the friends can retrieve and decrypt the data.

II. RELATED WORK

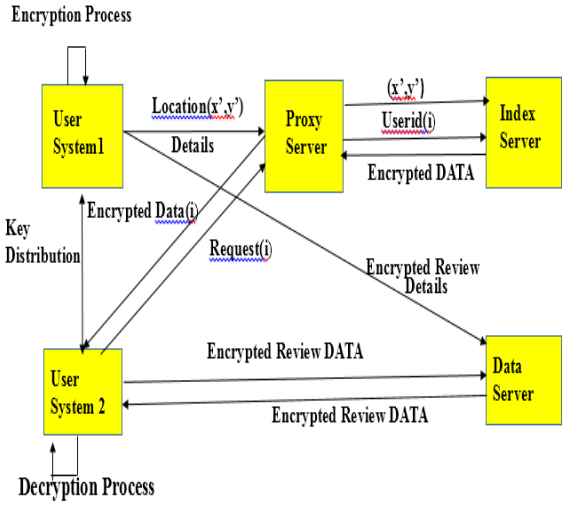
Mobile devices equipped with positioning capabilities (e.g., GPS) can ask location dependent queries to Location Based Services (LBS). To protect privacy, the user location must not be revealed. Existing solutions utilize a trusted anonymizer between the users and the LBS. The user location must not be revealed to protect the privacy. Based on private information retrieval a framework is proposed to support location dependent queries. In this framework there is no need of trusted third party, because privacy is achieved via cryptographic techniques. This approach achieves provides stronger privacy for snapshot of user location [1].

© 2014- 17, IRJCS- All Rights Reserved

Location based service called friend locator notifies a user if the user is geographically close to any of the user's friends. This kind of services is getting increasingly popular due to the penetration of GPS in mobile phones. The main idea is to develop an efficient communication solution by detecting the proximity between a user and user's friends, users have flexible choices to their proximity detection distances. Here they are developing a client server solution for proximity detection by using grid based mapping of locations [2]. Emergent practices around 'microblogging', changing and sharing status within a social group. Results from 'Connecto' which is a phone based status and location sharing application that allows a group of friends to 'tag' areas and have individual's locations shared automatically on a mobile phone. Through sharing status and location the system supported each group's ongoing repartee a site for social exchange, enjoyment and friendship [3].

III. SYSTEM ARCHITECTURE

The main idea of our secured location sharing services for social networks is that a user or a group initiator registers with the system to create a user group. Each group will have unique crypto key and that key is distributed and stored in all the users in that group. There will be one timer program that timer program will automatically pick the user location (GPS Coordinator) which will be encrypted using the group key and send to proxy server. The proxy server receives the data and stores it in the index server to avoid the data from the hackers. When user2 from the same group is requesting for the user1 location to the proxy server, proxy server has to verify the requesting user2 belongs to user1 group or not. If user2 is from the group of user1 it has to fetch the encrypted location detail from the index server and end it to the user2 device. In user2 device the data will be decrypted using group key and shows the user1 location on Google map.



IV. PROBLEM DEFINITION

The general functionality of many location based social networking applications is a location sharing service that allows users to discover the current location of their friends and notify the users when a friend is in the vicinity or within a certain distance. With a potentially untrusted server, such a location sharing service may threaten the privacy of users.

V. ADVANCE ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is a symmetric block cipher, it implemented in software and hardware throughout the world to encrypt the sensitive information. AES encryption compares three block ciphers AES-128, AES-192 and AES-256. Each cipher will encrypt and decrypt data in blocks of 128 bits. This done by using cryptographic keys. In symmetric key ciphers both the sender and receiver use the same key for encrypting and decrypting the information. So both the sender and receivers should know and use the same key. All the key lengths are considered in a specified way to protect classified information. More sensitive information will require 192 or 256 bit key lengths. To create a cipher text it considers a round which consists of several processing step such as substitution, transposition and mixing of input plaintext. There are 10 rounds foe 128 bit keys, 12 rounds for 192 bit keys and 14 rounds for 256 bit keys. The AES has proven reliable and provides the most efficient cipher text which is difficult to break.

© 2014- 17, IRJCS- All Rights Reserved

VI. CONCLUSION

Introducing a Location X which includes both latitude and longitude coordinates. It is an alternative that provides significantly improved location privacy. All the data information that is shared by user is double encrypted by using AES algorithm and stored in the index server. By using both proxy server and index server the data will be double encrypted and if any hacker tries to hack proxy server, he can't get the decrypted data as all the data is stored in the index server. Proxy server acts as an intermediate between the user and index server that stores the data, the proxy server will check whether the user belongs to the specified group and provides data if he belongs. The encryption takes place at the user side. So any attacks for the data flow betweenthe user and the proxy server data can't be leaked.

REFERENCES

[1]. Roman Schlegel, Chi-Yin Chow, Qiong Huang, and Duncan S. Wong, "Privacy preserving location sharing services for social networks", 2016
[2]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: Anonymizers are not necessary," in Proceedings of the ACM International Conference on Management of Data, 2008.
[3]. L. Barkhuus, B. Brown, M. Bell, S. Sherwood, M. Hall, and M. Chalmers, "From awareness to repartee: Sharing location within social groups," in *Proceedings of the ACM Conference on Human Factors in Computing Systems*, 2008.
[4]. L. Siksnys, J. R. Thomsen, S. Saltenis, M. L. Yiu, and O. Andersen, "A location privacy aware friend locator," in *Proceedings of the International Symposium on Spatial and Temporal Databases*, 2009

© 2014- 17, IRJCS- All Rights Reserved