ISSN:0975-9646

Extension of Preserving Privacy Location in Social Networks

Ravi Konaraddi,
Dept of Computer Science (M.Tech)
MVJCE,Banglore

Abstract-Social network information is now being used in ways for which it may have not been originally intended. For example consider Foursquare Application, so this application works similar to twitter and watsapp but the problem is preserving privacy particularly when we post some review about some hotels or some places to which we had visited recently. So in order to provide some extra security we had designed a mechanism known as Loc X. It works based on query system without relying on an of the trusted proxies and maintains two servers in order to maintain higher security for review posted and hence there by increasing efficiency in maintaining security.

I. INTRODUCTION

Online social networks are now used by hundreds of millions of people and have become a major platform for communication and interaction between users. This has brought a wealth of information to application developers who develop on top of these networks. Social relation and environment. Some of the mobile applications are fully exploiting GPS location services to provide a "social" interface to the physical world. Examples of popular social applications include social rendezvous, local friend recommendations for dining and shopping, as well as collaborative network services and game. The explosive popularity of mobile social networks such as SCVNGR and FourSquare (3 million new users in 1 year) likely indicate that in the future, social recommendations will be our primary source of information about our surroundings.

An example for misusing location information is Facebook. Soon after a week facebook was found to be popular some of the European thiefs used it to track the places of people who were online and then invade there home. And the same problem occued in Foursquare app, **it** is a local search and discovery service mobile app which provides a personalised local search experience for its users. By taking into account the places a user goes, the things they have told the app that they like, and the other users whose advice they trust, Foursquare aims to provide highly personalised recommendations of the best places to go around a user's current location. So instead of maintaining some strong security policy, so that third person may not able to track the user and hence be safe and secure from other externals attacks. So instead of providing these kinds of security they just vanished that feature.

Existing systems have mainly taken three approaches to improving user privacy in geo-social systems: (a) introduc-ing uncertainty or error into location data. Existing systems have mainly taken three approaches to improving user privacy in geo-social systems: (a) introduc-ing uncertainty or error into location data (b) relying on trusted servers or intermediaries to apply anonymization to user identities and private data and (c) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. None of them, however, have proven successful on current application platforms. Techniques using the first approach fall short because they require both users and application providers to introduce uncertainty into their data, which degrades the quality of application results returned to the user. In this approach, there is a fundamental tradeoff between the amount of error introduced into the time or location domain, and the amount of privacy granted to the user. Users dislike the loss of accuracy in results, and application providers have a natural disincentive to hide user data from themselves, which reduces their ability to monetize the data. The second approach relies on the trusted proxies or servers in the system to protect user privacy. This is a risky assumption, since private data can be exposed by either software bugs and configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms to obtain provable privacy guarantees are too expensive to deploy on mobile devices and even on the servers in answering queries such as nearest-neighbor and range queries.

2.SCENARIOS OF SOCIAL NETWOK

2.1 Scenario Consider a very familiar application Facebook.Let us a consider a situation where a person named by ravi was supposed to write his internals, which was known to his parents. Suddenly he changed his mind and decided to watch a movie with his girlfriend in Ionox or PVR.Now by having seated in theatre he checked in into facebook by posting on his wallpost that he is watching movie with so and so in Ionox.Now all his friends could see where and what exactly he is doing.So if his father could see means definetly they will punish him.So in order to avoid such things we demonstrated a new technique which could deny others from viewing those posts.

2.2 Scenario Alice and her friends are also interested in playing location-based games and having fun by exploring the city further. So they setup various tasks for friends to perform, such as running a few miles at the Gym, swimming certain laps, taking pictures at a place, or dining at a restaurant. They setup various points for each task, and give away prizes for the friends with most points. In order for Alice to learn about the tasks available near her, she needs to query an application to find out all tasks from friends near her and the points associated with them.

The scenarios above, while fictitious, are not far from reality. Groupon and LivingSocial are some example compa-nies that are leading the thriving business of local activities. SCVNG offers similar services as location-based games. But none of these services provide any location privacy to users: all the locations visited by the users are known to these services and to its administrators.

Our goal is to build a system that caters to these scenarios and enables users to query for friends' data based on locations, while preserving their location privacy. We want to support: a) *point query* to query for data associated with a particular location, b) *circular range query* to query for data associated With all locations in a certain range (around the user), and c) *nearest-neighbor query* to query for data associated with locations nearest to a given location. Finally, while it is also useful to query for data that belongs to non- friends in certain scenarios, we leave such extensions for future.

3.RELATED WORK

3.1 Privacy in general location based services

There are mainly three categories of proposals on providing location privacy in general LBSs that do not specifically target social applications.First is spatial and temporal cloaking,wherein approximate location and time is sent to the server instead of the exact values.The intuition here is that this prevents accurate identication of the locations of the users or hides the user among K other users and thus improves privacy. This approach however hurts the accuracy and timeliness of the responses and most importantly, there are several simple attacks on these mechanism that can still break user privacy. Pseudonyms and silent times are other mechanisms to achieve cloaking, where in device identifiers are changed frequently, and data is not transmitted for long periods at regular intervals. This, however, severely hurts func-tionality and disconnects users. The key difference between these approaches and our work is that they rely on trusted intermediaries, or trusted servers, and reveal approximate real-world location to the servers in plain-text. In LocX, we do not trust any intermediaries or servers. On the positive side, these approaches are more general and, hence, can apply to many location-based services, while LocX focuses mainly on the emerging geo-social applications.

The second category is location transformation, which uses transformed location coordinates to preserve user location privacy. One subtle issue in processing nearest-neighbor queries with this approach is to accurately find all the real neighbors.Blind evaluation using Hilbert Curves, unfortunately, can only find approximate neighbors. In order to find real neighbors, previous work either keeps the proximity of trans-formed locations to actual locations and incrementally pro-cesses nearest-neighbor queries or requires trusted third parties to perform location transformation between clients and LBSA servers. In contrast, LocX does not trust any third party and the transformed locations are not related to actual locations. However, our system is still able to determine the actual neighbors, and is resistant against attacks based on monitoring continuous queries.

The third category of work relies on Private Information Retrieval (PIR)to provide strong location privacy. Its per-formance, although improved by using special hardwares, is still much worse than all the other approaches, thus it is unclear at present if this approach can be applied in real LBSs.

3.2 Anonymous communication systems.

These systems, including Tor, provide anonymity to users approach seems to provide privacy as the server only sees location data but not the identity of the user behind that data.However, recent research has revealed that hiding the identity of the users alone is not sufficient to protect location privacy. Even if Tor is used, it is possible for an attacker with access to the location data to violate our privacy and unlinkability requirements. For example, using anonymized GPS traces collected by the servers, it has been shown that users' home and office locations, and even user identity can be derived. LocX defends against such attacks and meets all our requirements.

Systems on untrusted servers.

In the context of databases, recent systems proposed running database queries on encrypted data (stored on untrusted servers), using heavy-weight homomorphic or asymmetric encryption schemes. These approaches are suitable for spatial data outsourcing or data mining scenarios where the data is static and is owned by limited number of users. But they are less suitable for LBSAs, where the data is dynamic and personal, and thus cannot be encrypted under a single secret key.

In the context of location and social applications, Persona and Adeona also relied on encrypting all data stored on untrusted servers to protect user privacy. Persona focused on privacy in online social networks, and Adeona focused on privacy in device tracking systems where there is no data sharing among users. Applying Persona's mechanisms to LBSAs directly would encrypt all location coordinates, making LBSAs unable to process nearest-neighbor queries. But if location is not encrypted, attacks using anonymized GPS traces, mentioned above, can succeed, making Persona insufficient to protect location privacy. Similarly, Adeona is useful for a user to retrieve her own data, but not the data from her friends. Our contributions complement these systems. Some techniques in these papers can help LocX as well, e.g. Persona's approach to partition data shared with friends into fine-grained groups, and Adeona's hardware-assisted approaches to speed up crypto processing. from the server, and most importantly, there are several simple attacks on these mechanisms that can still break user privacy.

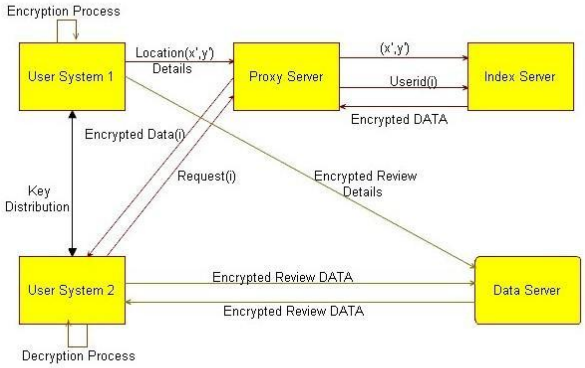
Pseudonyms and silent times are other mechanisms to achieve cloaking, where in device identifiers are changed frequently, and data is not transmitted for long periods at regular intervals. This, however, severely hurts func-tionality and disconnects users. The key difference between these approaches and our work is that they rely on trusted intermediaries, or trusted servers, and reveal approximate real-world location to the servers in plain-text. In LocX, we do not trust any intermediaries or servers. On the positive

side, these approaches are more general and, hence, can apply to many location-based services, while LocX focuses mainly on the emerging geo-social applications.

4.SYSTEM DESIGN

4.1Common Terms Used

Co-ordinate Transform:Transforming the current location(x,y) to encrypted location(x^1 ,Y^1) using Advanced Encryption Standard(AES).



Design of Locx mechanism

Proxy Server:

1.The proxy server acting as broker between user application system and indexing server.
2.The system user application can't directly communicate with indexing server or data server.
3.The system user application will communicate with proxy server application for every request.
4.The proxy server will check for every transaction, this request valid request or not from valid user.
5.The proxy server system will maintain all data's are secure manner i.e. all data will be in encrypted format only without knowing secret key user or hacker can't able to view the data's.
6.The proxy server will communicate indexing server based on query requesting, after getting data reference only can able to communicate with data server.
7.Without knowing the secret key user cant view the user details or server data details.
8.Its giving the security in both way latitude and longitude will be encrypted, data will be encrypted and also it won't be stored directly, that data's stored into some other server.

Index Server

1.The indexing server will have encrypted data about the data stored information after getting indexing information only, can able to get the original data from the data server.
2.The proxy server is without getting the reference from the indexing server cant get clear data based on the user requesting query.

Data Server

1.The data server is having only encrypted data's.
2.This data's all are indirectly related with indexed data if user trying to get the review detail about particular organization, the proxy server will get the organization detail from the indexing server, based on the data the proxy server will get review detail from the Data Server.

5.IMPLEMENTATION

The main thing that we need to show is, server should support all kinds of queries such as point queries,nearest neighbour query and Circular range query.In basic design,in order to show this features location coordinates must be revealed in plain text but by doing so it could break security system

In this system we are using Advanced Encryption Standard(AES) Cipher Block Algorithm for encryption and Decryption. And a Random Generator Function for generating Index at user Side

So we have designed new mechanism known as LocX which could solve all issues.In this system we had introduced two new servers.They are

1. Index Server.
2. Data server

Index server is used to store encrypted location and index Mathematically it is given as

L2I=[(x',y'), E(i)]

Where L2I indicates location to an encrypted index i.e it stores an encrypted index at location (x',y')

Data Server is used to store encrypted location data at index i It is given as

I2D=[i, E(data(x,y))]

Steps for implementation.

1.User Systems needs to share some keys such as Shit s,rotational angle β and symmetric key by email or cellphones. 2.UserSytem 1 generates L2I and I2D servers with respect to some hotel or school.

Transform or Encrypt location (x,y) and send it some untrusted or Trusted proxy and from there to Index Server.
3.Generate a random Index I,using Random Generator function and encrypt the location data and store it in Data Server.
4.UserSystem-2 fetches L2I from key shared by UserSystem 1 i.e it decrypts and obtains location.
5.UserSystem-2 after obtains index i by decrypting it using AES(CBC) algorithm.
6.Finally after getting Index I,UserSystem-2 decrypts the data and views it.

6.CONCULSION

LocX design mechanisms efficiently protects user privacy without sacrificing the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers. More specifically servers (and any intermediaries) can be compromised and, therefore, are untrusted.It also enables users to query for friends' data based on locations, while preserving their location privacy and supports a) *point query* to query for data associated with a particular location, b) *circular range query* to query for data associated with all locations in a certain range (around the user), and c) *nearest-neighbor query* to query for data associated with locations nearest to a given location.

REFERENCES

[1] M.Motani, V.Srinivasan, and Nuggehalli, "Peoplenet engineering a wireless virtual social network," 2008

[2] Dailynews, "How cellphone helped cops nail Key murder suspect secret pings that gave bouncer away" march 2007

[3] K.P.N Puttaswamy,R Bhagwan, and V.N Padmanabhan,"Anonygator:Anonymity and Integrity Preserving Data Aggregation ," in Proc.of Middleware,2010

[4] B.Schilit,J.Hong and M.Gruteser,"Wireless location privacy protection " Computer vol 36,2003

[5] "Police:Thieves robbed homes based on facebook,social media sites,"September 2010

[6] T.Jiang,H J Wang,and Y-C Hu,"Preserving location privacy in wireless lans" in proc. Of MobiSys 2007.