International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

LOC X - LOCATION PRIVACY PROTECTION IN GEO SOCIAL APPLICATIONS (MOBILE COMPUTING)

I. DIVYADHARSHINI[1], S. GOMATHI[2], K.HEMALALATHAA[3], Dr.R.JOSPHINELEELA[4]

[1,2,3]STUDENT, DEPT. OF CSE, PANIMALAR ENGINEERING COLLEGE, INDIA [1, 2, 3]

[4]ASSOCIATE PROFESSOR, DEPT. OF. CSE, PANIMALAR ENGINEERING COLLEGE, INDIA

Article Received: 14/03/2015 | Article Revised on:20/03/2015 | Article Accepted on:25/03/2015

ABSTRACT

Using geo social applications, such as Four Square, millions of people interact with their surroundings through their friends and their recommendations from others. Without proper privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce Loc X, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation with others. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms 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 Loc X provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.

Index Terms—Location privacy, security, location-based social applications, location transformation, efficiency

1. INTRODUCTION

With billions in downloads and annual revenue, smart phone applications offered by Apple iTunes and Android are fastly becoming the dominant computing platform for today's user applications. Within these environment, a new wave of *geo social* application are fully exploiting GPS location services to provide a "social" interface to the physical world and the market of today. Examples of popular social applications include social rendezvous, local friend recommendations for dining and shopping, as well as collaborative network services and games and many more. The explosive popularity of mobile social networks such as SCVNGR and Four Square (3 million new users in 1 year) likely indicate in the future, social recommendations will be our primary source of information about our surroundings within this generations . Unfortunately, this new functionality comes with significantly increased risks to personal privacy. Geo-social applications operate on fine-grain, time-stamped location information with less security.

For current services with minimal privacy mechanisms, this data can be used to infer a user's detailed activities, or to track and predict the user's daily movements in everything. In fact, there are numerous real world examples where the unauthorized use of location information has been misused for economic gain, physical stalking, and to gather legal evidence and for more lethal activities. Even more disturbing, it seems that less than a week after Face book turned on their popular "Places" feature for tracking users' locations, such location data was already used by thieves to plan home invasions and other attacks. Clearly, mobile social networks of tomorrow require stronger privacy properties than, the open to all policies available in today's interaction between distances .So this process does not have the visual ability to concrete the point of total security.

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 and the people around them, which reduces their ability to monetize the data and the element of security is drastically reduced. The second approach relies on the trusted proxies or servers in the system to protect user privacy which is mostly single encrypted. This is a risky situation, since private data can be exposed by either software bug and configuration errors at the trusted servers or by malicious administrators. Finally, relying on heavy-weight cryptographic mechanisms that are been practiced in today's process has 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 which are generally complicated. The challenge, then, is to design mechanisms that efficiently protect user privacy without sacrificing the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers. More specifically, we target geo-social applications, and assume that the single encrypted servers (and any intermediaries) can be compromised with less security level. To completely reduce misuse, our goal is to limit accessibility of location information from global visibility to a user's social circle. We identify two main types of queries necessary to support the functionality of these geo-social applications: point queries and nearest-neighbor (KNN) queries. Point queries, query for location data *at* a particular point, whereas KNN queries, query for k nearest data *around* a given location coordinate (or up to a certain radius). Our aim is to support both query types in an efficient manner, suitable for today's mobile devices and other devices. To overcome this challenge, in this paper, we propose *Loc X* (short for location to index mapping), a novel approach for achieving user privacy while maintaining full accuracy in location-based social applications (LBSAs from here onwards) suitable for users. Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data who are ready to share things within them.

2. OVER VIEW OF EXISTING SYSTEM

In this system, It is an ability to prevent the unauthorized entities to access the location data of current and past location of the users or friends .It's defined as the ability to hide the identity of the mobile node by using Pseudonym .So that the real identity of the user can't be traced by the malicious node from the server side. It is an ability to prevent unauthorized entity to relate different sessions of the mobile node during usage.

2.1 Drawbacks of the Existing System:

Sharing our location where there is no privacy about location or content because it is stored in a single server where anyone can see the message, this is not that much secure and not up to the mark. In this project we bring double security for the data which is shared between two users that cannot be hacked.

3. PROPOSEDAPPROACH

To address these challenges, in this paper, we propose *Loc X* (short for location to index mapping), a novel approach to achieve user privacy while maintaining full accuracy in location-based social applications (LBSAs from here onwards).

Our insight is that many services do not need to resolve distance-based queries between arbitrary pairs of users, but only between friends interested in each other's locations and data and happy with sharing their details and reviews. Thus, we can

partition location data based on users' social groups, and then perform *transformations* on the location coordinates before storing them on servers. A user knows the transformation keys of all their friends, allowing them to transform their query into the virtual coordinate system that their friends use. Our coordinate transformations preserve distance; perform both point and queries correctly on the transformed data. However, the transformation is *secure*, where the transformed values cannot be easily associated with real world locations without a *secret*, which is only available to the members of the social group. Finally, transformations are efficient, in that they incur minimal overhead on the LBSAs. This makes the applications built on Loc X lightweight and suitable for running on today's mobile devices and easily accessible by the users with more secured environment.

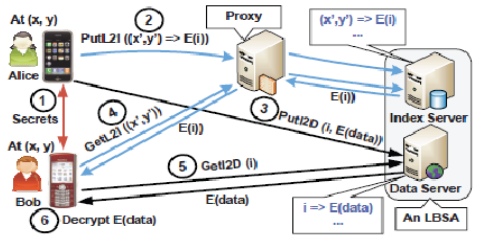
3.1 MERITS

There is double security in sharing the location, the data which are transferred is encrypted and then transferred and stored in the index server as a key and the data are stored in the data server. The key is sent in the mail so that, only the concerned person can only view the location. Without reading he key from the mail the review cannot be viewed.

4. ALGORITHM AND DESIGN

AES (advanced encryption standards) is based on the cipher encryption and decryption. Here we use 128 bit with 10 round and there are certain other stages involved in this shift row, sub bytes, mix columns, add round keys. The block size of AES is 4 and we use bitwise OR operation. The AES specification refers to this as the Key Expansion routine. Generating, in essence, multiple keys from an initial key instead of using a single key greatly increases the diffusion of bits. Although not overwhelmingly difficult, understanding Key Expansion is one of the trickier parts of the AES algorithm.

4.1System architecture:



5. IMPLEMENTATION DETAILS

LOCX Module: Loc X builds on top of the basic design, and introduces two new mechanisms to overcome its limitations. First, in Loc X, we split the mapping between the location and its data into two pairs: a mapping from the transformed location to an encrypted index (called **L2I**), and a mapping from the index to the encrypted location data (called **I2D**). This splitting helps in making our system efficient and easy to understand for us. Second, users store and retrieve the L2Is via un trusted proxies. This redirection of data via proxies, together with splitting, significantly improves privacy in Loc X. For efficiency, I2Ds are not provided, yet privacy is preserved (as explained later).

Proxy L2Is for location privacy: Users store their L2Is on the index server via proxies. These proxies can be any of the following: Planet Lab nodes, corporate NATs and email servers in a user's work places, a user's home and office desktops or laptops, or Tor [34] nodes. We only need a one-hop indirection between the user and the index server during processing. These diverse types of proxies provide tremendous flexibility in proxy L2Is, thus a user can store her L2Is via different proxies without restricting themselves to a single proxy. Furthermore, compromising these proxies by an attacker does not break users' location privacy, as (a) the proxies also only see transformed location coordinates and hence do not learn the users' real locations, and (b) due to the noise added toL2Is (described later). To simplify the description, for now, we assume that the proxies are non-malicious and do not collude with the index server during the process. But we will later describe our solution in detail to even defend against colluding, malicious proxies. With this high-level overview, we now describe our solution to store and query data on the servers in detail for all users. We also explain the challenges we faced during the study, and the tradeoffs we made in making our solution secure and efficient than the prevailing systems.

Storing L2I on the index server: Firstly consider the process of storing L2I on the index server. This transformation preserves the distances between points1, so circular range and nearest neighbor queries for a friend's location data can be processed in the same way on transformed coordinates as on real-world coordinates using the map. Then the user

generates a random index using their random number generator and encrypts it with their symmetric key to obtain at the transformed coordinate on the index server via a proxy. The L2I is small in size and is application independent in high levels, as it always contains the coordinates and an encrypted random index throughout the process. Thus the overhead due to proxy is very small and the process will be more secured.

Storing I2Ds on the data server: The users can directly storeI2Ds (location data) on the data server. This is both secure and efficient than the existing process

1) This is secure because the data server only sees the index or the key stored by the user and the corresponding encrypted block of data. In the worst case, the data server can link all the different indices to the same user device, and then link these indices to the retrieving user's device. But this only reveals that one user is interested in another user's data, but not any information about the location of the users, or the content of the I2Ds, or the real-world sites to which the data in the encrypted blob corresponds to with complete security.

2) The content of I2Dis application dependent. For example, a location-based video or photo sharing service might share multiple MBs of data at each location. Since this data is not provided in this, Loc X still maintains the efficiency of today's systems.

CONCULSION

Loc X provides location privacy for users without inserting uncertainty or errors into the system, and does not rely on any trusted servers or components with least security levels. Loc X takes a novel approach to provide location privacy while maintaining overall system efficiency, by leveraging the social data-sharing property of the target applications. In Loc X, users efficiently *transform* all their locations shared with the server and encrypt all location data and information stored on the server using inexpensive symmetric keys. Only friends with the right keys can query and decrypt a user's data in any situation. We introduce several mechanisms to achieve both privacy and efficiency in this process, and analyze their privacy properties to a great extent. Using evaluation based on both synthetic and real-world LBSA traces, we find that Loc X adds little computational and communication overhead to existing systems in many ways. Our Loc X prototype runs efficiently even on resource constrained mobile phones with needed requirements. Overall, we believe that Loc X takes a big step towards making location privacy practical for a large class of emerging geo-social applications along with data security.

FUTURE ENHANCEMENT

For our future work, we intend to improve privacy location and also implement some advance features into Loc X like *Location-based reminders*: users place reminders for friends at specific locations (for *e.g.* reminder to buy milk near a grocery store), and when the friends are at that location or environment, an alert is generated on their device, *Location-based recommendations.* This application aims to recommend nearby sites (restaurants, shopping malls, etc.) to users based on the reviews given to these sites by their friends for knowing about that particular place.

REFERENCES

[1]. M. MOTANI, V. SRINIVASAN, and P.S. NUGGEHALLI, "People Net: Engineering a Wireless Virtual Social Network," Proc. ACM MOBI Com, 2005.

[2]. M. Hendrickson, "The State of Location-Based Social Networking on the I Phone," http://techcrunch.com/2008/09/28/the-state-oflocation- Based-social-networking-on- the- I phone, 2008.

[3]. P. Mohan, V.N. PADMANABHAN, and R. RAMJEE, "NERISELL: Rich Monitoring of Road and Traffic Conditions Using Mobile Smart phones," Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008.

[4]. G.Ananthanarayanan, V.N.Padmanabhan, L. Ravindranath, and C.A. THEKKATH, "Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading ,"Proc. Fifth Int'l Conf. Mobile Systems, Applications Services, 2007.

[5]. [5] M. SIEGLER, "Food spotting is a Location-Based Game that Will Make Your Mouth Water," http://techcrunch.com/2010/03/04/Foodspotting,2013