GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

PRESERVING LOCATION PRIVACY IN GEOSOCIAL APPLICATION

Hemlata Jadhav*1, Nitish Dhotre2, Prof. S.G.Shaikh3

*1,2Department Of Computer Engineering, Sinhagad Institute of Technology, Lonavala

ABSTRACT

This paper introduces a Preserving Location Privacy in geosocial application. The main goal of this paper is to share current location or likely location details and data information of one user to the another user. This paper also discuss about role of security system in location technology which provides a means to link the one user to another user based on positioning technology via wireless connectivity. In this literature survey paper we mainly focused on existing System, drawbacks of existing system. Our key goal is to apply secure, user-specific, distance preserving co-ordinate transformation to all location data shared with the server. We mainly use two servers proxy server and index server for more security of location details. By using these two servers, user one can share his location details to user two. In this proxy server is used to maintain co-ordinate values in encrypted format and index server is used to stores content values of user. This prototype measurement shows privacy protection in very little performance overhead, and it will suitable for nowadays mobile systems.

Keywords— *Location Anonymity, Private Information Retrival(PIR), Query Privacy, Security, Location Based Social Application, Location Transformation,Efficiency.*

I. INTRODUCTION

This is wireless communication system designed for the collection and dissemination of location information that particularly refers to location-based systems. Smartphone application such as android application is quickly becoming dominant platform for today's user application. Within these markets, a new wave of geosocial applications is 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 games. The explosive popularity of mobile social networks such as SCVNGR and FourSquare (3 million new users in1 year) likely show that in the future, social recommendations will be our primary source of information about our surroundings location area.

The wide spread of location-detection devices (e.g., GPS-like devices) enables new applications in which users continuously send their location information to a location based database server. Examples of these applications include store finders, traffic reports, and location-based advertisements. Although location-based applications promise safety and convenience, they threaten the privacy and security of their customers. In order to get a location-based service, a user has to report her private location information to the server. With untrustworthy servers, such model provides several privacy threats. For example, an employer may check on her employee behavior by knowing the places she visits or the personal medical records can be inferred by knowing which clinic a person visits[1].

The increasing number of communication systems (e.g., mobile phones), feature positioning capabilities (e.g., GPS). Users can ask location-dependent queries, such as "find the nearest hospital", which are answered by Location Based Services (LBS) like Google Maps. However, queries may disclose sensitive information about individuals, including health condition, lifestyle habits, political and religious affiliations, or may result in unsolicited advertisement (i.e., spam). Privacy concerns are expected to rise as LBSs become more common[2].

Location based services allow clients to query a service provider (such as Google or Bing Maps) in a ubiquitous manner, in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants, hospitals, etc.). However, similar to web searches or online purchases, location-dependent queries may disclose sensitive information about an individual's health, financial status, political affiliations, etc.[3]

Existing systems have mainly taken three approaches to improving user privacy in geosocial systems: 1) introducing uncertainty or error into location data 2) relying on trusted servers or intermediaries to apply anonymization to user identities and private data and 3) 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 trade-off 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 or 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.

II. PROBLEM STATEMENT

Design and Development of a complete geosocial android application that shares one user location or likely location to another user. This architecture uses two servers, one is the proxy server and another is the index server. Proxy server is used to store co-ordinate values in encrypted format. And index server is used to store content values of user. In this proposed system both user have to register first. And only register user can access their notification. User one shares particular longitude value and latitude value to another user. Due to proxy server these values stores in encrypted format. Hence proxy server stores the coordinate values and index server stores data in content format that means whatever the description of the location. For recovery of this encrypted data the secret key is sent on another user's mail id. Because of this second user can easily get location without any threat and without loss of information.

III. Existing systems

The existing technology just allows us to get location details using GPS. The privacy-aware query processor system is embedded in- side the location-based database server processing to tune its functionality to deal with anonymous queries and cloaked spatial areas rather than the exact location information. Mobile users register with Casper with a privacy profile that has the form (k, A),where k indicates that the user wants to be k-anonymous, i.e., not distinguishable other k users, while A Min min indicates that the user wants to hide her location information within an area of at least A .Mobile users have the ability to frequently change their privacy profiles to adjust a personal trade-off between the amount of information they reveal about their locations and the quality of service that they obtain from Casper.[1]

Private queries in location based existing system proposed a novel framework to support private location dependent queries, related on the theoretical work on Private Information Retrieval (PIR). This framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. Compared to existing work, our approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. We use our framework to implement approximate and exact algorithms for nearest-neighbor search. We optimize query execution by employing data mining techniques, which identify repeated computing process. This paper was completely dependent on cryptography method for security. Contrary to common belief, the experimental results suggest that PIR approaches incur reasonable overhead and are applicable in practice.[2]

There exist numerous methods that can provide a certain

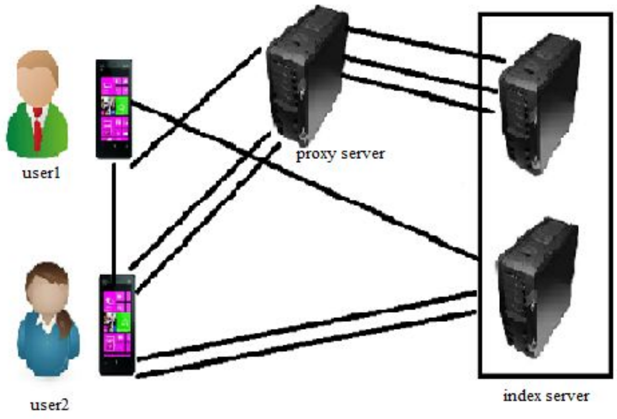
Degree of location privacy, even if they were originally proposed in a different security domain. These solutions can be classified according to three major concepts: (i) location obfuscation, (ii) data transformation, and (iii) private information retrieval (PIR). We argue that currently no methodology can support arbitrary kNN queries providing strong location privacy. More specifically, in location techniques the LBS can restrict the client in a small sub space of the total domain, leading to weak privacy. Schemes based on data transformation are vulnerable to access pattern attacks, which may be correlate the query of outliers, popular locations system.[3]

IV. Threats of existing system

Location-based applications promise safety and convenience, they threats the privacy and security of their customers. In order to get a location-based service, a user has to report her private location information to the server. With untrustworthy servers, such model provides several privacy threats. For example, an employer may check on her employee behaviour by knowing the places she visits or the personal medical records can be inferred by knowing which clinic a person visits. Hence the main threat is privacy and security of information.

V. Proposed system

Preserving privacy location in geosocial application system there is one mobile application in which user can share his location or whatever his likely location to another user. Our existing system one user cn share his location to the another user by using only one server. This system is no up to the mark secure. So now we proposing new architecture a new method like one user can share his details like whatever his location details to another user by using two servers. These are proxy server and index server. Proxy server is used to data maintaining in coordinate values in encrypted format. And index server is used to store actual content values of users. Whatever methodologies we used is two users are registered and two servers are used. Due to use of encrypted format data or whatever longitude or latitude values are encrypted and stores in the proxy server. Because of this encryption method in proxy server data is keep at high security. And this data is send to index server at this stage secret key is forwarded to another users id. Hence another user can get actual content by decryption process. That monitors the location, movement.



.

Figure 1: Architecture Diagram

VI. Application

In this paper we implement LocX in Java. We used AES with 128 bits keys for encryption and decryption. We measured LocX's performance on both desktops and on android mobile phones. The index and data servers were run on the same Dell PowerEdge server. Clients were run on another machine with the same configuration. We used the same code base for both desktop and mobile tests. But we had to modify the code slightly for Android OS to deal with some missing libraries. In addition, we had to make certain optimizations to limit the memory usage to under 16 MBs for LocX process in Android. Here we sketch how to build LBSAs using LocX.

We demonstrate the usage of our APIs by building three applications. In today's systems that provide these services, the data are entrusted to the server in plain text, which performing the computations in the application logic. But since we do not trust the server in LocX, the application logic that computes on the plain-text location data is moved to the client. Location-based reminders. This application users place

Reminders for friends at specific locations (e.g., reminder to buy milk near a grocery store), and when the friends are at that location, an alert is generated on their device. To build this application in our model, a user bundles all the details about the reminder, such as the reminder text and time, encrypts the whole bundle and generates a corresponding I2D. Then, the user transforms the reminder location based on the friend's secret and generates a corresponding L2I. These pieces are stored on the servers with a putL2I and a putI2D calls. Each user periodically runs a neighbourhood query for data from her friends. First the user takes her current location, transforms it according to her secret, runs a neighbourhood query, and fetches the L2Is and I2Ds, if any, using the getL2I and getI2D calls. Then, the device decrypts and reminds the user as appropriate. We measured the communication costs between clients and servers, the client processing time, the query completion time, and the server processing time.

VII. Graphical scenario

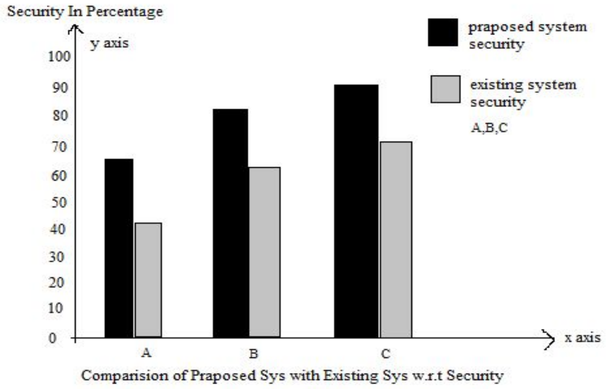


Figure 2: Graphical Representation

Above diagram represents graphical scenario of security. Which shows comparision of security factor among proposed system and three existing systems(A,B,C). A refers the security contents of A privacy aware location based data based server. B refers the security contents of private queries in location based services. C refers the security contents of nearest neighbour search with strong location privacy.

ACKNOLEDGEMENT

We express our thanks to all those who have provided us valuable guidance towards the completion of this project as part of the syllabus of bachelor’s course. We express our sincere gratitude towards co-operative department who has provided us with valuable assistance and requirements for the system development.

We hereby take this opportunity to record our sincere thanks and heartily gratitude to our Project guide, Prof S.G.Shaikh for his useful guidance, making available to us his intimate knowledge and experience in making Automotive Telematics as project.

We are also thankful to our project co-ordinator Prof. R.S Shishupal for their constant enlightenment and motivation which has been highly instrumental in making our project.

The acknowledgment will be incomplete if we do not record our sense of gratitude to our HOD of the Computer department, Prof. S.D.Babar and Principal Dr. R.S.Gaikwad who gave us necessary guidance, encouragement by providing us all the facilities to work on this project.

REFERNCES

1. *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.*
2. *G. Ghinita, P. kalnis, A. Khoshgozaran, C. Shahabi, and K.-l. Tan,”Private Queries In Location-Based Services: Anonymizers Are Not Necessary” Proc.ACM SIGMOD Int’l Conf. Management Data 2008.*
3. *S. Papadopoulos, S. Bakiras, and D. Papadias,“Nearest Neibhour Search With Strong Location Privacy ,” proc VLDB Endowment, vol. 3, nos ½, pp 619-629, sept 2010.*
4. *A. Khoshgozaran and C. Shahabi, “Bliend Evaluation Of Nearest*
5. *Neighbor Queries Using Space Transformation To Preseve Location Privacy ,”Proc. 10th Int’l Conf. Advances Spatial Temporal Database 2007.*
6. *G.Ghinita,P.Kalnis, and S.Skiadopoulos,”Private:Anonymous Location- Based Queries in Distributed Mobile System ,”Proc.16th Int’l Conf. World Wide Web .2007.*