# Location Based Services for Sharing Using Trusted Server

[1]Umesh D R, [2]Prakruthi T.N.

[1]Associate Professor, [2]M.Tech, PES College of Engineering, Mandya, India,

[1]umesh.dr.pesce@gmail.com, [2]prakruthikodiyala@gmail.com

**Abstract The main aim of location-sharing is to provide current location information to their designated users. Nowadays, Location Based Service (LBS) has become one of the popular services which are provided by social networks. As LBS activity makes use of the user's identity and current location information, an appropriate path has to be utilized to protect the location privacy. However, as per our knowledge, there is no access to protecting the location sharing with the complete privacy of the location. To consider this issue, we put forward a new cryptographic primitive functional pseudonym for location sharing that make sure privacy of the data. Also, the proposed approach notably reduces the computational overhead of users by delegating part of the computation for location sharing to a server, therefore it is endurable. The primitive can be widely used in many MOSNs to authorize LBS with enhanced privacy and sustainability. As a result, it will contribute to proliferate LBS by eliminating user's privacy concerns.**

***Keywords--- Location based services (LBS), current location, Location sharing, Mobile online social networks (MOSNs), Order-Retrievable Encryption (ORE), one time password (OTP).***

## I. INTRODUCTION

The extensive propagation of pervasive technology as well as of mobile devices relying on them makes available a good amount of highly sensitive location information that can be used for various intentions. Customer-oriented application, social network, and monitoring services can be functionally enhanced with data reporting where people are, how they are traveling, or whether they are close to any specific places. To this end, several commercial and enterprise-oriented location-based services already exist and popular too.

Location-based services are reinforced by modern location technologies that have reached good position and reliability at costs that most people (eg the fare of mobile devices) and companies (eg the fare of integrating location technologies is existing telecommunication infrastructures) can economically afford. As these location-based devices use very compound/complicate and may use the location information for different needs, gathering and managing such information is a cumbersome process out of the different issues that to be addressed on the progressing of such services. Location privacy is becoming highly important nowadays. Location privacy can be defined as the right of an individual to decide how, when, and for which purposes their location information could be released to third parties. The location privacy protection leads to server consequences that make users the target of fraudulent attacks LBSs are using the most important components in MOSNs, which gives information and entrant service based on the geographical position of the mobile device.

LBS has seen explosive growth these years, particularly due to the fast development of mobile technology and cloud computing. In LBS the location of the device represents one of the important contextual information about the device and its user, is utilized to develop innovative and value-added services to the user's context. Several individuals, communication, and enterprise-oriented LBS are available and are popular nowadays.

Various LBS applications have been proposed, such as location-based mobile advertising to mobile device users, LBS can also be applied in E-health systems to allow access to patient records of the hospital by doctors with location-based access technology. There are lot more example of LBS including mobile check-in games like foursquare social networks like Loopt and location-enabled apps such as Google maps. According to the analysis project: the revenue for LBS to grow from 2.8 billion in 2010 to hit 10.3billion by 2015 with an increase in popularity of LBS, the privacy matters on user's locations has been raised Because location tracing capacity of the devices has been improved significantly, user's information such as position and Preference will be leaked and may have risk of improper use.

The basic Objectives of the Present Study are:

- The application is to be share live and present location of the user which is encrypted so that only the intended person can access the data.

 DOI : 10.35291/2454-9150.2020.0365 

- Further, the current location of a user must not be tracked by any unintended entity including the service provider.

So it violates user's privacy and impedes the development of various LBS applications. A recent study showed that pieces of information called from mobile devices can uniquely identify 94% of 1.5 million people in a mobility database. This scenario becomes more serious when it comes to MSN's in which the user's physical location is correlated with their profiles without guarantee of privacy, users may be hesitated to share their location through MOSN's. Hence, how to protect location privacy is one of the challenges in MOSN's.

## II. RELATED WORK

In the paper [1], a new location sharing scheme with both location spatiotemporal relation privacy and location privacy has proposed the privacy of users is often invaded essentially because the server has enough knowledge to work out whether a user and its friend are nearby or not. To address this problem, we rather use the service provider merely as an anonymous bulletin board to broadcast the anonym zed location message of a user such that only intended friends of the user of the moment can verify the actual identity of the user. To implement such an application, we proposed a new cryptographic primitive, namely the functional pseudonym, which is designed based on Lagrange polynomial, to merge the public identities, e.g. social network user ID of the user's(temporal) friends into a single value. Then, this value is later added to the anonymized location message to verify the identity of the originator of the anonym zed location sharing, each of the designated friends, whose ID was used to generate the functional pseudonym in the anonym zed location message, uses Lagrange interpolation along with its private information(corresponding to the originator. In this way, we provide location privacy and Spatio-temporal relation privacy at the same time without pre-established secrets among users and without a trusted server.

The paper [2] focuses on unusually large gatherings of people that are in social events. And a methodology is introduced for detecting such social events in massive mobile phone data, based on Bayesian location inference framework. Specifically, a framework for deciding who is attending an event is developed. We have suggested how we will indicate which users are likely to have attended the event, and when and where any events happened. We have demonstrated this method on a few examples, using limited data, namely only positions of the antennas. Still, it remains difficult to validate the method without additional information. However, considering a simple Voronoi method, not using such a probabilistic framework, already seems to provide some indication of whether there's an occasion or not. However, it can easily misinterpret which individuals are attending. Therefore, we might consider the following improvement. We first detect social events employing a simple Voronoi method but use the more refined method suggested here to make a decision in which people participated in the event. So using the Voronoi approach we obtain a coarse-grained view of which events happened, while our method gives a more fine-grained view of who is attending, and could provide a more accurate estimate of the exact location. This would speed up the algorithm, making it more feasible to detect events across the entire country with reasonable accuracy

In this paper [3], a novel solution achieving both location privacy and social network privacy has been introduced. The new construction provides a flexible way for privacy-preserving location sharing for both trusted friends and untrusted strangers, simultaneously supporting range query and user-defined access control. This paper aims at achieving enhanced privacy against the insider attack launched by the service providers in MOSNs, we introduce a replacement architecture with multiple location servers for the primary time and propose a secure solution supporting location sharing among friends and strangers in location-based applications. In our construction, the user's friend set in each friend's query submitted to the location servers is split into multiple subsets by the social network server randomly. Each location server can only get a subset of friends, rather than the entire friends set of the user as the previous work. Also, for the first time, we propose a location-sharing construction that provides check the ability of the searching results efficiently returned from location servers. We also prove that the new construction is secure under the stronger security model with enhanced privacy. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

In this paper [4], a location predicated query solution that utilized for a utility to privately determine his/her location utilizing oblivious transfer on a public grid a confidential intelligence recuperation cooperation that recovers the record with immense transmission capability has been presented. According to an analysis of cognate work on location privacy, in this work, they have implemented the location privacy evaluation model of Distortion-Predicated Metric, which is used to assess the implementation of the K-anonymity solution. The modifications that have done on K-anonymity implementation of where the elimination of personalization and adaptation to the evaluation model of Distortion-Predicated Metric personalization from K-anonymity is eliminated, because the aim is to observe results of K-anonymity protocol when it covers k-many users at a time, hence they made it work in all cases. And also analyzed the performance of our protocol and discerned it to be both computationally and communication ally more efficient than the other subsisting solutions. The

 DOI : 10.35291/2454-9150.2020.0365 

common functionality of many location-based social networking applications is a location-sharing service that allows a group of friends to share their locations. A location sharing service many threaten the privacy of users with a potentially untrusted server.

In this paper [5], a new encryption scheme called Order-Retrievable Encryption (ORE) has been proposed. This ORE scheme enables users to browse their friend's exact locations within a certain distance without revealing any information about their locations to any other users or social networking service providers. This application consists of a database server maintained by a social networking service provider and users. According to the ORE scheme, users send their location information in encrypted form to the database server.

## III. PROPOSED SYSTEM

In the existing system there are many issues that interfere with user's privacy there is no appropriate way to protect the location sharing with privacy. So It is important to ensure the privacy of the user and to ensure leaking of data to the third party our application has been developed to tackle these problems by enhancing the privacy concern.

**The issues are**,

• **Anonymity/Pseudonymity** - Privacy by hiding identity. In anonymity, this is done by never providing any information which can be used to identify the user. It is still possible to see an exact location, but it cannot be identified who is at that location. In pseudonymity, an identifier is applied to a location, but it should be impossible for an adversary to map this identity to an actual user. Possible issues: Hiding the identity of the user conflicts with sharing the position with friends.

• **Obscurification** - privacy by not revealing the exact location. There are two basic forms of obscurification: temporal and spatial. In the temporal model, it is possible to see that a user has been at a certain location, but not when. In spatial obscurification, the location of the users is hidden in an area larger than a single point. Possible issues: Adding temporal obscurification makes it impossible to create a crowd-sensing map. Adding spatial obscurification makes it impossible to share a precise location.

•**Policy-Based** - Privacy by allowing/denying subjects permission to the location. Comparable to access control in a file system. Possible issues: Might not be expressive enough. • Protocol - Privacy by a custom communication protocol. Possible issues: Adding privacy to existing LBS requires changing all communication.

• **Cryptographic** - Privacy by cryptography. This can e.g. be done in social network services where users share locations through a server using public-key cryptography. Possible issues: Server still knows which parties are communicating.

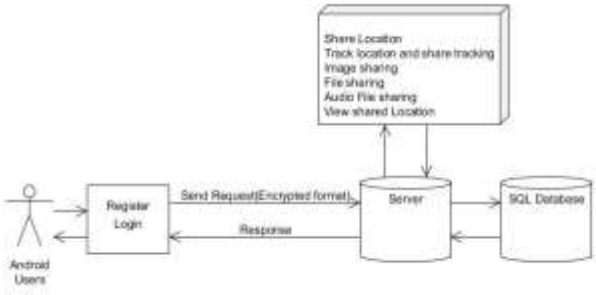


**Fig 3.1 System architecture**

The above fig3.1 shows that the first android user register with its details like name, email id, address, phone number, password, and confirm password. once the user is registered OTP will be generated. Next, the user is login to the main page. Then send the requested to the server share location, track location, image sharing, file sharing audio sharing, a view shared location these all are encrypted and stored in the databases. Then send the response to the user.

The system architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system.

In the proposed application, the problem of user's privacy against insider attack launched by the service providers in files and location sharing functions are addresses. Many kinds of privacy have been considered, including location privacy and data privacy. We have introduced a new architecture with location servers for the first time and proposed a secure solution supporting location sharing among friends and strangers in location-based applications. This application provides an enhanced and secure method for data and location transfer through android mobile. And also provides the security of data. Users can register into the application and a one-time password will be generated which will be received by the user through message and users have to enter this OTP to login and they can upload audio files, pdf, images, live locations and share it to other users. Files will be encrypted while sharing and the receiver can decrypt and view the files easily and efficiently.

Users must disclose their location information to get a location-based service. Users can get more precise services if they disclose more information, however, privacy problems will also get worsen. To satisfy this condition, several schemes were proposed to provide location information in limited circumstances. The proposed application is a cryptographic scheme for location sharing through android phones. Through this application, users can share their live and present location through mobile phones securely.

 DOI : 10.35291/2454-9150.2020.0365 

The proposed application achieves secure location privacy, low computational and communication costs, and efficient data updates. This application provides a reliable approach to sharing and retrieval of information through mobile phones. This application achieves high protection on user's privacy. The storage load has been considerably decreased when compared to existing systems because this system does not users relevant information. In this architecture, we augment a database system with a privacy controller. The privacy processer processes constraints of privacy. The evaluation shows that the proposed scheme has complete privacy through proof of randomness while providing functionality, security, and privacy of pseudonyms. Also, the scheme has sufficient efficiency for resource constrict mobile devices. This application protects the user's identity from unintended parties while each user can send their exact location to the intended friends privately and securely.

## IV. RESULTS

The proposed application has addressed the problem of user's against insider attack launched by the service providers in MOSN's. The location and other data privacy have been considered in this application. The experimental results show that the proposed application provides a secure solution supporting location sharing among friends and strangers in a location-based application. The proposed application achieves secure location privacy, low computational and communication costs, and efficient data updates. This application provides a reliable approach to sharing and retrieval of information through mobile phones. The computation speed of the system is high when compared to traditional systems. An actual computation made by the server is also much faster. These results prove that the proposed scheme is highly efficient, reliable, and secure and is sufficient for mobile usages. Also, the delegable location sharing significantly reduces the computational overhead of users and consequently makes LBSs highly sustainable.

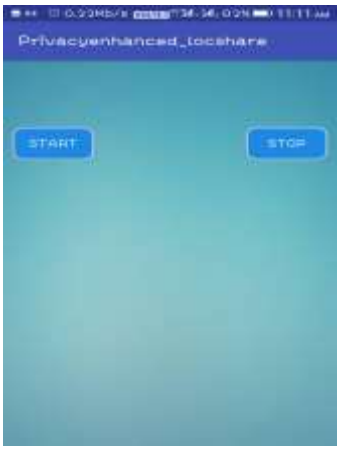


Fig4.1Share live location


Fig4.2 Receiver view in map or track the location

Firstly the user registers by entering some of the details like name, address, email ID, mobile number, password, and confirmation. If anyone of this field is missing then it shows the error message and helps the user to check for eg; If the user misses entering a mobile number, then it shows error and helps by showing mobile number is empty, if the incorrect number is given then it shows the invalid number, then after registration OTP will be generated and those details are stored in the database. Next is log in phase. Here the user enters the application by entering the email ID and password(OTP) which he created while registering. In case if anyone field is wrong then it shows the invalid field and the user cannot enter the application. After entering the homepage there will be options that lead to tracking location, file sharing, and logout.

When you enter user tracking location you enter into a page where there is various options User tracking location sharing. We can access to share live location through which we can share our present location to the person for whom we wish to share by selecting their name and submit it. Then another page will open as shown in Fig4.1, the start and stop button after clicking on start, it will start sharing your location to the receiver whom we have selected, and whenever we wish to withdraw, we can click on the stop button and it will stop sharing our location to the receiver. In the receiver side, the option live location shared for me is clicked then it will show the list of users who sent their live location to the receiver and then the receiver should tap on the user whom they wish as in Fig4.2, which shows details and receiver can track the user in Map.

 DOI : 10.35291/2454-9150.2020.0365 


Fig4.3 Select and share the location


Fig4.4 Receiver view the location

It has three options. Shared location, view shared location, view shared location by me. In share location first, we select the receiver we want to share with and then we should select the location then click on next as shown in Fig4.3, the receiver clicks on a view shared location then the receiver gets details as shown in Fig4.4. Then he can view it in a map by a tap on view in the map. This is about the location services in the application.


Fig 4.5 Select image from gallery


Fig4.6 Receiver view the image

On the home page, there is another option File sharing through which users can share the image, documents, and audio. Image sharing consists of add images, view images, view shared images. by click on add image, we can select the receiver for whom we want to send the images, and select the photos and then upload the image as seen in Fig4.5. The receiver can see the image by entering in view image as in Fig4.6.


Fig4.7 Upload the file


Fig4.8 Receiver view the file

File sharing consists of add file, view file, view shared file by click on add file we can select the receiver to whom we want to send the file, and select the file then send to the receiver as seen in Fig4.7. The receiver can see the file by entering in view file as in Fig4.8.

 DOI : 10.35291/2454-9150.2020.0365 


Fig 4.9 Upload the audio


Fig 4.10 Receiver view the audio

Audio sharing consist of add audio, view audio, view shared audio by click on add audio we can select the receiver to whom we want to send the audio and select the audio and then send the audio as seen in Fig4.9.. The receiver can hear the audio by entering in view audio as in Fig4.10.

## V. CONCLUSION

This paper introduces the new application location privacy the third party cannot access the data. We have addressed the problem of user's privacy against insider attack launched by service providers in MOSNs. Information regarding physical locations of users is rapidly becoming easily available for processing by online and mobile location-based services. Combined with novel application opportunities, however, threats to personal privacy are gaining special prominence, as witnessed by recent security incidents targeting the privacy of individuals. The project's main techniques are aimed at protecting location privacy. Techniques for location privacy protection and privacy enhanced location-based access control is proposed.

## REFERENCES

[1] J. son, D. Kim, R. Tashakkori, A. O. Tokuta, and H. Oh, ”A new mobile online social network based location sharing with enhanced privacy protection”, in ICCCN 2016 Conference Proceedings. IEEE, August 2016.

[2] Vincent Traag, Arnaud Browet, Francesco Calabrese, Frederic Morlot “Social event detection in massive mobile phone data using probabilistic location inference” September 2011.hal-00627122.

[3] J.Li, H.yan, Z. Liu, X. Chen, X. Huang, and D. S. wong “Location –Sharing system with enhanced privacy in mobile online social networks”, IEEE System Journal,vol.11, no.2,pp.439-448,June 2017.

[4] R. Schlegel, C-Y Chow, Q. Huang, and D. S. Wong, “Privacy-Preserving location sharing services for social networks”, IEEE Transaction on Services Computing,vol.10, no. 5, pp.811-825,September/October 2017.

[5]Minxin Du, Qian Wang, Meiqi He, and Jian Weng “Privacy-preserving Indexing and Query processing for secure dynamic cloud storage”, IEEE 2018.

[6]H. T. Dinh, C. Lee, D. Niyato, and P. Wang ”A survey of mobile cloud computing: architecture, applications and approaches” Wireless Communication and Mobile Computing,vol.13, no.18, pp.1587-1611, December 2013.

[7]D. Quercia, N.Lathia, F. Calabrese, G. D. Lorenzo, and J. Crowcroft “Recommending social events from mobile phone location data” in IEEE ICDM10 Conference Proceedings, IEEE , December 2010, pp.971-976.

[8]C .R.Vicente, D.Freni, C. Bettini, and C. S. Jensen,” Location-related privacy in geo-social networks” IEEE Internet Computing, vol.15, no.3, pp.20-27, February 2011.

[9]W. Wei, F. Xu, and Q. Li, ”Mobishare: Flexible privacy-preserving location sharing in mobile online social networks”, in IEEE INFOCOM12 Conference Proceedings, IEEE Computer and Communication Society March 2012, pp.2616-2620.

[10]L. Backhaus and A .K. Dey,” Location-based services for mobile telephony: A study of users privacy concerns”, in Proc.INTERACT.2003,vol.3,pp. 702-712.

[11]Z. Lin, J.Li, X. Chen, J. Li, and C. Jia,” New privacy-preserving location sharing system for mobile online social networks”, in Proc.3PGCIC, 2013, pp.214-218.

[12]K. P. N. Puttaswamy and B. Y. Zhao, ”Preserving Privacy in location-based mobile social applications ”in proc. Hot mobile.2010.pp 1-6.

[13]Huaxin Li,Haojin Zhu , Senior Member, IEEE, Suguo Du, Xiaohui Liang, Member,IEEE, and Xuemin(Sherman)Shen,Fellow, IEEE “ Privacy leakage of location sharing in mobile social networks:Attacks and Defense”.

[14]Gang Sun,Yuxia Xie,Dan Liao,Hongfang Yu,Victor Chang “User-Defined privacy location-sharing system in mobile online social networks”.

 DOI : 10.35291/2454-9150.2020.0365 