SoftFence: An Anonymiser and Active Object based TTP Location Privacy Framework

Akshay Gupta[1] and Prof. Rupali Bhartiya[2]
Master of Engineering (C.S.E.) Rajiv Gandhi Proudogiki Vishwavidyalaya, (Collage Name: Shri Vaishnav Institute of Technology & Science), Indore Madhya pradesh, India[1]
Prof. in Shri Vaishnav Institute of Technology & Science, Indore Madhya pradesh, India[2]
akshaygupta896@gmail.com[1], rupalibhartiya@gmail.com[2]

Abstract: *In today's world most of the applications are based on the location information of users for identifying the point of interest automatically without the explicit query. Mainly the usages are involving with mobility based devices such as cell phones, PDSA's, laptops, GPS based devices etc. The device transmits the location information along with the device identity to the location server. Sometimes the application demands more data than it actually needs. There is also a situation where the application uses location information up to certain accuracy. If more accuracy is passed to those applications than there is a chance of security compromises related to confidentiality, integrity and availability. Thus, there must privacy based information handling before passing the values to location server. During the last few years there are various architectural based solutions suggested for serving more privacy in least cost. But after studying the various articles regarding to that techniques, it is found that there are some issues which remains unsolved. Existing privacy algorithm will apply more complex query processing with no control over the accuracy and providers authenticity. Also, the query must hide the user's identity and control the application data requirements. Most of the previous algorithms are based on k-anonymisers and proximity with a defined architecture. There a various direction where the improvements can be applied. This paper introduces a novel SoftFence framework for improving the privacy of location based services. The approach uses the phenomenons of k-Anonymisers, cloaking and active objects for achieving its goals. The system reduces the query processing load with restricted content usability limits and accuracy for each application. More controlling can be served using the active object transfusions. Overall process involves blocking of additional and leveled information belongs to the user's identity and location from malicious activities. This work also analyses the security and privacy provisions along with performance measurement of proposed SoftFence approach. At the analytical level of evaluation, it seems to reduces the overhead and improve the privacy protections in a robust way.*

Keywords: *Mobile Devices, Location Privacy, Trusted Third Party (TTP), K-Anonymisers, Active Object Handling, User Approved Privacy Policies;*

1. Introduction

Technological advancements over the last few decades will lead the social and informative system more secure. It empowers the user's identity belongings and let them more confidential as per the user's needs. The recent systems are mostly using the user's location information for serving better then it previously does. Substantial amount of information is required and protected by such system. In today's application, the location information is proving its effectiveness and reduces the users load towards searching and other activities. It is directing various areas like automation, GPS, nearest entities, etc. After the complete development of the location based services it is found that they require the complete information about their surroundings and let them plot on the maps with accurate traffic information. It could be applied for health care, social network and communication and sharing with dynamic behaviours. But there is a debate towards restricting the information contents passing in an application. If the application is getting more control over the users information than it may leaks the confidential data. Thus, the location based services must have that control over the information. Also the user needs to have some rights over the information passing to that application. Somewhere it raises the issues related to privacy preserving of the user and its confidential information. The location oriented services and applications having support of dependent information transmission with continuous flow of updated information. Such dynamic coverage and transmission of location information provides highly accurate results. For understanding the location based service let us take a brief look over its types. They could be effectively parted into two basic areas: Person Driven and Device Driven.

- **Person Driven LBS:** Such LBS includes all the services which offer all the user a complete measures of their location information. It majorly focuses on fetching the person’s location with certain accuracy measures. Normally, the service users cannot control such functionalities.
- **Device Driven LBS:** They are served as an external application to the existing devices. They don’t need to take the position of the person; instead they acquire the positions of the object on which a person is using that service. Now a day’s most of the devices are having these location added service with ease of operations in there devices.

The above classification is known as level one. In some of the research article a level two classification is also provided. It is based on the type of service offered by the location entities.

- **Push Function:** Such measures provide the complete automation in the location functionality accessibility for the application usages. Here all the application is getting the accurate location information as per there requirements without making any explicit request. They send the information without getting the consent from the user or there device.
- **Pull Function:** Here the applications have to make the explicit request for getting the location information. They usually made a pull call from the networked device for getting the information on its devices. They are normally based on the passed information like where is the ATM close to my location etc.

Objective of LBS Designing

In today’s world the devices accessing the location information is getting abruptly increased and shown a exponential growth in the mobile device industry. The device having GPS functionality could be able to use that information for getting the prediction and forecast the next locations for satisfying the needs. The market is fully equipped with such services which give complete access with instant notifications to their personalized contents. They automatically generates the alerts for the user for their desired service types, next locations, upcoming locations and milestones etc for early planning and analysis based on the moving directions. The location enabled service will also help you to be in touch with your friends, family and other persons. Such effective system can be designed by considering the following objectives:

(i) To provide the measured information of location with accuracy up to certain level for detecting the location of their known persons.
(ii) Such location enabled service will forecast the directions for the moving objects or carrier like cars, and other vehicles.
(iii) Detects the point of interest between the two communicating parties for time savings
(iv) Serves the location information based on the proximity analysis for the mobile devices

How LBS Works

While making the LBS various incorporated functionalities is essential like data capture, dynamic data handling, point of information (POI) and collection starting with the digital road maps. Here the generated Map data values are stored in links known as intersection. Each link has start and end points and may also incorporate shape points to model the curvature of the road. Gatekeeper applications use business and pointer information that has been processed into POI databases. Merging the map database with the POI database creates a detailed, digital demonstration of the road network and business services accessible along it. These POI databases contain the kind of detailed information typically found in a phone directory and add value to the map database's geographic content. As is the case with a map database, POI databases collected from multiple vendors can be merged to form a single, comprehensive data set. Each record in an individual POI database is geocoded, or assigned a latitude/longitude coordinate, before being combined with other POI databases. To accommodate changing road features, well-designed Location Engines are designed to work with dynamic data and to use it to supplement and/or override existing map information. The applications depend on LBS engines with dynamic data capabilities because they allow dispatchers to react almost instantaneously to changing conditions. The heart of any LBS system is the Location Engine, which contains the software components that add intelligence to digital map data. The quality of these modules is just as important as data quality for generating accurate results. Software functions such as geocoding, reverse geocoding, and routing are key technologies built into the Location Engine. Proximity search is an important feature by which and location engine is equipped with. Proximity searches use POI database information to find businesses or landmarks near a specified location. Users can search for locations of ATMs, gas stations, restaurants, hotels, or other establishments. The map database, POI database, geocoding, and routing software form the basic components that application developers use to build custom LBS applications.

2. LITERATURE SURVEY

Models Location based service is gaining popularity with the smart mobile devices by which location detection using GPS is effectively planted. They normally raise the queries for location demands for applications which serve relativity of that information. The application is using a certain amount of data for location detection and passes this information to various application or location servers. Sometimes this data can be used for some malicious or attacking activities which lead the degradations or compromises of user's personal information. Thus, location privacy is an area where the improvements are required. Normally, the location engine processes the user's information and generates the outputs based on that query. This information can be further used for tract\king the user and its data. This violates the privacy rules. There is also a condition there the application access your local location information, and for that the amount of data actually used is more than as required. Thus, again there is a probability of losing the users data confidentiality. During the last few years various approaches related to the location based services are developed for improving the user's privacy. The aim is towards improving the current system for making the users data more confidential from the unauthorized accesses. Proceeding towards achieving its aim there are so many paper and articles are studied here. These are:

In the paper [8], Locanym is suggested as a location based service with privacy preserving mechanism. It is based on geolocated capabilities for serving the secure and verified positioning techniques for mobile and embedded environment. Here the techniques keep the factors of performance, precision and accuracy of position. In all the application that access the location information continuously, privacy issues related to \users personal information is always probable. The paper also deals with privacy protection based LBS implementation. The suggested system is having a pseudonym tied to a particular geographical area. More precisely, it aims at deriving, from an accurate and verified positioning. Along with other specific features offered with the tool, it also satisfies the pseudonym properties like Unlinkability, unforgeability, accountability, non-repudiation and sovereignty. At the last the approach is serving all the aims and proving its effectiveness.

The paper [9] presents an iPDA, a system to support privacy-preserving data access in location-based mobile services. The iPDA system consists of three main components: a mobility-aware location cloaker that cloaks the user's location with a region and transforms a location based query to a region-based query, a progressive query processor that efficiently evaluates a result superset for the location-based query and, a result refiner that refines the superset to generate the exact query result for the user. The system have a tourist information system named iGuide, as an iPDA application, is prototyped for demonstration. The systems are based on client-server architecture and are equipped with GPS. Users are interested in querying public spatial objects related to their current locations. These objects are maintained by a spatial database on the server. For implementing the solution the system has mobility-aware location cloaking and region-based query processing. The system had adopted a simple yet practical privacy measure, i.e., the spatial area of the cloak region. The quality of location cloaking is measured by entropy. Thus at the evaluation, it also serve best result in near optimal time.

The paper [10] covers the same aspect but specifically for the mobile environment using a global network. Along with other aim the privacy perseveres is also maintained here. Several algorithms to cloak the exact location of individuals have been designed, each of them delivering a certain balance between privacy and usability. This paper presents the results of a small-scale interview performed by the authors, summarizes several methods to cloak location data and explains an algorithm for a privacy-aware location query processor. k-Anonymity To get to such a strict goal, the k- anonymity model is proposed to ensure that any release of information about a single individual can- not be distinguished from the information about at least one other individuals. Here the Clique Cloak algorithm that can handle messages that each have individual spatial and temporal resolution requirements, but also have individual privacy constraints. A measurement relative anonymity for an individual message has been introduced, which equals the ratio between the number of messages that are in the cloaking box and the value of k for this message, e.g. a relative anonymity value of 2 means that the number of messages in the cloaking box is twice the value of k. The location k-anonymity property ensures that the relative anonymity is at least 1 for each message.

The paper [11] deals with a technique for private information retrieval that allows a user to retrieve information from a database server without revealing what is actually being retrieved from the server. Here the retrieval operation in a computationally efficient manner to make it practical for resource-constrained hardware such as smart phones, which have limited processing power, memory, and wireless bandwidth. In particular, the suggested algorithm makes use of a variable-sized cloaking region that increases the location privacy of the user at the cost of additional computation, but maintains the same traffic cost. The approach had implemented a level of privacy for the PIR query. The proposed system does not require the use of a trusted third-party component, and ensures that we find a good compromise between user privacy and computational efficiency. At the evaluation, a proof-of-concept implementation over a commercial-grade database of points of interest is given with the paper. The proposal is to offer users the choice of trading off privacy for better query performance, by specifying the levels of privacy that they want for their queries. On the other hand, such users are equally willing to trade off some levels of performance to gain some levels of privacy support.

Carrying forward the above work the paper [12] suggest a protocol for private proximity testing for allowing two mobile users, communicating through an untrusted third party. The test decides whether they are in close physical proximity without revealing any additional information about their locations. Traditional approaches mainly uses location tags for securing the schemes against the attacks based on the users location information’s. Due to the need to perform privacy-preserving threshold set intersection, their scheme was not very efficient. This work will reduces the threshold set intersection on location tags to equality testing using de-duplication technique known as shingling. The paper proceeds forward by successfully capturing location tags based on the GSM cellular network, which covers a larger area with greater reliability. Moreover, a novel use of de-duplication shingling to test location tag similarity by private equality testing, a simple and efficient cryptographic primitive. A prototypic implementation will prove the quality of the developed system with highly accurate operations.

Even after the various approaches there are certain circumstances on which an individual may not be in control of their private location information. Here the vulnerability towards privacy violations is expected. The paper gives that much of control to user on his private information’s towards making it open by the provider or attacker. The approach aims towards establishing the privacy equilibrium in the form of a prohibitive contract which is established with the intention of preventing a possible privacy violation [13]. Utilizing the utilitarian paradigm approach, it evaluates the overall efficiency of the prohibitive contracts which shows postulates convergence towards an overall balanced system. Determining the intrinsic value of private information is a subjective process and evidently hard. This can be attributed to the fact that privacy and privacy violation is dependent on the individual, the degree of violation, time, circumstance and situation. Private information has a perceived value proportional to the demand for it by others and the amount of anguish it causes the owner should privacy be infringed upon. Information which may be deemed private today may have .less. or even .more. of a privacy implication in the future. This information has the distinct possibility of being relinquished to others without the owner's consent.

The paper [14], proposes a privacy protection solution to allow users' preferences in the fundamental query of k nearest neighbours (kNN) using a HilAnchor approach. Particularly, users are permitted to choose privacy preferences by specifying minimum inferred region. Via Hilbert curve based transformation, the additional workload from users' preferences is alleviated. Furthermore, this transformation reduces time-expensive region queries in 2-D space to range the ones in 1-D space. Therefore, the time efficiency, as well as communication efficiency, is greatly improved due to clustering properties of Hilbert curve. HilAnchor processes a kNN query in two rounds, a user sends a false point p0 of point p, called an anchor of point p, to server and receives k nearest neighbour answers, denoted as kNN (p0), in terms of p0. In the second round, the client sends back RCA created from the returned answers. The server returns all POIs located inside the RCA. Finally, the actual result is pinpointed at the client side. During these two rounds, RCA needs to meet two-fold requirements. First, the region of RCA must cover the targeted POIs. Second, it promises users' preferences to MIR. The difficulty of RCA creation stems from the latter requirement; it is possible for adversaries to shrink the inferred region within a big RCA, invalidating its privacy protection. This observation contradicts usual institutions of enlarging RCA in a brute-force way, and lets alone the increasing cost with large RCA. There- fore, the realization of HilAnchor framework becomes difficult when it aims to allow for user-specified MIR.

The paper [15] focuses same intentions towards mobile cloud computing (MCC) environment. Despite providing various benefits, MCC is still in its early stages in providing trust guarantees to a user. Location-Based Services (LBS), on the other hand, are those services which operate on a users location to provide him/her services such as finding nearby restaurants, hospitals, bus terminal and ATMs, to name a few. While a user's location is mandatory for LBS to work, it imposes serious threats to the user's privacy. This paper proposes a privacy preserving cloud-based computing architecture for using location-based services. On one hand, the suggested architecture provides a secure mechanism for using LBS services anonymously while on the other hand it utilizes untrusted but fast and reliable cloud services for its implementation in an efficient and effective manner. Moreover, it provides various attack scenarios and show that how our architecture preserves the privacy of the user and is difficult to compromise.

In this paper, a fine-grained privacy preserving location-based service (LBS) framework, called FINE, for mobile devices is given [16]. It adopts the data-as-a-service (DaaS) model, where the LBS provider publishes its data to a third party (e.g., cloud server) who executes users' LBS queries. The proposed FINE framework employs a ciphertext-policy anonymous attribute-based encryption technique to achieve fine-grained access control, location privacy, confidentiality of the LBS data and its access policy, and accurate LBS query result while without involving any trusted third party. Moreover, the proposed FINE framework also integrates the transformation key and proxy encryption to migrate most of computation-intensive tasks from the LBS provider and users to the cloud server. This property keeps mobile devices away from massive resource-consuming operations. Extensive analysis shows that our proposed FINE framework is secure and highly efficient for mobile devices in terms of computation and communication cost. After studying all the related articles for location based services it is found that there are some more breaches which remains to be solves. These issues will affect the future development of LBS with the cloud and mobile environment. Thus, a robust and scalable privacy preserving mechanism is required satisfies the constraints of mobile clouds.

3. Problem Definition

Location based services aims to provide the accurate location information towards the application requirements. This information exchanges must satisfies the users constraints related to the privacy and confidentiality. Such controls can be established using some rules and regulations for guiding the information. Also there must be control on the amount of information passed means the structure of the data should be fixed for each application and authorized by the user. Some of the application violates this information disclosure rules and maliciously use this in some other way. Thus there must be security constraints which continuously monitor the above process. Also the end user must be known about the disclosure of their location information along with other content and its usages. It should be in a notice form which can be easily displayed on the users device screen and easy to read. There must be provider user agreement with the restricted content policy with the accuracy dependencies. Means the application must also assure the kind of accuracy required for achieving their goals. If more accurate information is passed to application then there is a chance of compromising the privacy of user and it could be tracked. For serving the aim of privacy controlled LBS designing, there are various architecture implemented. This work mainly deals with the trusted third party architecture and founds the problem associated with it's for further improvements. Some of their shortcomings are:

i. The traditional K-Anonymity can compromise the query handler identity like TTP. For effective control the identity of even this handler must be made secure. Thus, some object based transmission will reduces the probability of this.

ii. Traditional query and LBS server will made the delays in the transmission due to over protectiveness. It causes drops in systems performances. Some lightweight form of above process will resolve the issue.

iii. Level information must be control for passing into layered applications restricted to their required content only in some changed forms. This will hide the provider and users identity.

4. Proposed Solution

This work proposed a novel SoftFence approach for providing the effective privacy handling for location based services. Mainly most of recent application is accessing the location information for providing the better services to the user. This application aims towards using the user's location information for proving the relative index for their current location. The work aims towards making the applications local data access towards user in a more secure manner. Thus, the geolocations is used by the devices and software is embedded here for robust security and hence it is named as SoftFence. The approach is solving the information passing solution for a specific application and must assure the limit as required by applications. Means no of the application could access any of the information without the user permissions. Any location based service uses only two major entities, user and provider. The process starts with the users query toward particular information from the application server.

The location query contains three fields: node ID, location information and queried information request. This query is passed to the local location engine. Now the local LBS will assure the amount of information required for each application. Here the user have an complete control over the information because before applying the values to the application each polices have to be approved by user which in turn behaves as a agreements between the provider and user.

Now after the information, their policies and application is matched up, this is forwarded to the trusted third party verifier modules. This module works as an intermediation between the provider and user. The first entity is this module is the active object creation. Here the information is further transfused to some object based form with fixed information and temporary behaviours which is destroyed after the particular use of the application is over. It does not hold the temporary data thus, malicious usages of this information is also prevented. This stops the location tracking and pattern formation as major solution of traditional approaches issues. Once the information is converted to active object, k-Anonymiser hides the location ID for the user.

Here the Anonymiser assumes that communications are anonymous, i.e. LBS providers do not require an ID to answer queries. It assures the identification abstraction in a layered means for applications. A very universal way to hide the real location of the users from the LBS provider is by using the k-anonymity property which guides the information disclosure properties. Fundamentally it replaces the original information with the cloaking regional codes or information with a certain amount of user's locations. After that, the Anonymiser forwards the request to LBS server engine of providers end. This replies to the query with the content relativity measurement. Now, the requested query is replied instead of other is verified by the verifier and mapper functionality.

The cloaking process requests the broadcaster's neighbours which satisfies the k-anonymity property, with a defined diversity and granularity of the information. Here also actual location ID is replaced by some anonymous information belonging to a particular group. Thus in this way a complete privacy perservness is maintained by the proposed framework. Analytical evaluation of the proposed approach will prove its effectiveness over its competitors. Future implemented code will shows the less complex, and light weighted solutions with a clear supports to mobile and cloud computing.

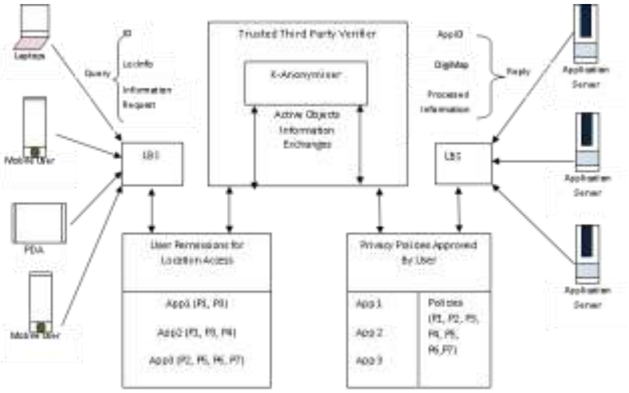

Fig. 1 SoftFence: A Secure Location Privacy Framework

5. Conclusion

Location based service is a dynamic location information managing system which cloud be further improved in terms of its privacy handling. This service contains the transition of users requested query and information to the providers. This location information exchanges between both is guided by the k-anonymity property offered by trusted third party controller. Primary objective with that is to manage a clear isolation between the users location information and application. An application using the device or users location information should only use limited content as required for achieving the privacy and confidentiality constraints.

References

[1] Marco Gruteser and Dirk Grunwald , "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", in Proceedings of MobiSys International Conference on Mobile Systems, San Francisco, CA, USA, May, 2003

[2] Emmanouil Magkos, "Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey", in Ionian University, Department of Informatics, Corfu, Greece

[3] Chi-Yin Chow Mohamed F. Mokbel, "Privacy in Location-based Services: A System Architecture Perspective", Department of Computer Science and Engineering, University of Minnesota

[4] Yih-Chun Hu and Helen J. Wang, "A Framework for Location Privacy in Wireless Networks", in ACM SIGCOMM Asia Workshop, Beijing, China, doi: 1-59593-0302/05/0004, April 2005

[5] Panos Kalnis, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias, "Preventing Location-Based Identity

Inference in Anonymous Spatial Queries", in IEEE Transaction on Knowledge and Data Engineering, ISSN:1041-4347, doi: 10.1109/TKDE.2007.190662, 2007

[6] Nayot Poolsappasit and Indrakshi Ray, "Towards a Scalable Model for Location Privacy", in ACM SPRINGL, Irvine,CA, USA, doi: 1-60558-324-2/08/11, 2008

[7] Ali Khoshgozaran and Cyrus Shahabi, "Private Information Retrieval Techniques for Enabling Location Privacy in Location-Based Services?", in University of Southern California Department of Computer Science Information Laboratory (InfoLab), Los Angeles, CA

[8] Sebastien Gambs, Marc-Olivier Killijian, Matthieu Roy and Moussa Traore, "Locanyms: Towards Privacy-Preserving Location-Based Services ", in LAAS, CNRS and ANR French national program for Security and Informatics.

[9] Jing Du,Jianliang Xui, Xueyan Tang and Haibo Hu, "iPDA: Supporting Privacy-Preserving Location-Based Mobile Services", in Hong Kong SAR, China

[10] Mark van Cuijk and Barry Weymes, "Location Privacy", Dec 2010

[11] Femi Olumofin, Piotr K. Tysowski, Ian Goldberg and Urs Hengartner, "Achieving Efficient Query Privacy for Location Based Services", in PETS and LNCS Journal of Energy & Commerce, 2010

[12] Zi Lin, Denis Foo Kune and Nicholas Hopper, "Efficient Private Proximity Testing with GSM Location Sketches", in ACM, 2010

[13] N.J Croft_and M.S Olivier, "Location Privacy: Privacy, Efficiency and Recourse through a Prohibitive Contract", in Transaction on Data Privacy, 2011

[14] Wei-Wei Ni, Jin-Wang Zheng and Zhi-Hong Chong, "HilAnchor: Location Privacy Protection in the Presence of Users' Preferences", in Journal of Computer Science and Technology, Volume 27, Issue:2, doi: 10.1007/s11390-012-1231-2, March 2012

[15] Fizza Abbas, Rasheed Hussain, Junggab Son and Heekuck Oh, "Privacy Preserving Cloud-based Computing Platform (PPCCP) for using Location Based Services", in IEEE/ACM 6th International Conference on Utility and Cloud Computing, doi: 10.1109/UCC.2013.26, 2013

[16] Jun Shao, Rongxing Lu and Xiaodong Lin, "FINE: A Fine-Grained Privacy-Preserving Location-based Service Framework for Mobile Devices", in IEEE Infocomm Conference on Communication, 2014

[17] Mahdi Zamani and Mahnush Movahedi, "Secure Location Sharing", in ACM, doi: /10.1145/2634274.2634281, 2014