International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 5 (September-october 2015), PP. 23-34

A NOVEL PRIVACY PRESERVING MODEL FOR LOCATION BASED SERVERS IN MOBILE CLOUDS

Anjali Kalore[1], Prof.Megha Singh[2]
Dept. of Computer Science and Engineering,
Central India Institute of Technology, Indore (M.P), India
[1]keneanjali@gmail.com

Abstract— — **In today's world most of the applications are based on the location information about users for identifying the point of interest automatically without the explicit query. Mainly the usages are involved with mobility based devices such as cell phones, PDSA's, laptops, GPS based devices, etc. Along with mobility the scalable services using cloud is taking place along with mobile environment. Both the areas are proportional to each other making them famous as a combined choice for user and hence it is considered as mobile cloud area. Here the privacy aims towards making the user's personal information safe. 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 locate server. The existing privacy algorithm will apply more complex query processing with no control over the accuracy and providers authenticity. This work suggests some modifications in the previous privacy handling mechanism for location based services. The system reduces the query processing load with restricted content, usability limits and accuracy for each application. This work also analyses the security and privacy provisions along with performance measurement of the proposed approach. At the analytical level of evaluation, it seems to reduce the overhead and improve the privacy protections in a robust way.**

***Index Terms*— Cloud Computing, Mobile cloud Devices, Location Based Services (LBS), Location Privacy, Trusted Third Party (TTP);**

I. INTRODUCTION

Cloud must have a planned approach to providing the security control to users along with application access and other important factors. The organization leads towards deploying the server, which offers security functionality. Along with the security factors performance factors should also be kept in a min, because if the security control is heavier than the other applications and their usability might get affected. Thus a balance must be mad in between the security approach complexity and the kind of resources they are occupying and how they affect the application response. There are some points which keep in concern always while developing cloud security mechanisms. They are:

- Effective resource management with virtualization support
- Robust service delivery with reliable communications
- Automotive process with reduced fault and performance burdensome and load handling
- Making security just above the value of information
- SOA based security service model

A. Cloud Security Challenges

Technological advancements over the last few decades will lead the social and informational system more secure. It empowers the user's identity belongings and let them more confidential as per the user's needs. Cloud computing is not secure by nature. Security in the Cloud is regularly elusive and less obvious, which definitely makes an incorrect conviction that all is well with the world and anxiety about what is really secured and controlled. The off-premises computing ideal model that accompanies distributed computing has brought about incredible concerns about the security of data, particularly the integrity and confidentiality of data, as cloud service suppliers may have complete control on the computing

infrastructure that underpins the services.

Some of those identified areas where the security elaborations can be made are:

(i) Encapsulated information security standards along with service applicability must be applied over the computing servers

(ii) User and organization defined policies should take a control over the traditional security mechanism used for confidentiality and integrity.

(iii) User's belongings and its personal information must be made secure even against the service providers also.

(iv) Security must be light weight so that additional load cannot be placed on the resources configured.

Since the CSP is the authority that controls the data items stored in the system, the CSP can look into data items stored in cloud storage without the data owner's permission. Thus to make the system more reliable client needs to make some security trusted deals with its data. The actual deployment of cloud computing services is not reliable as they claim because the existing security model doesn't work after migration of services to clouds. This work aims towards making the security more effective by suggesting a novel model which provides security controls over as a service. Mainly the controls include some of the cryptographic algorithms, single sign on (SSO) and digital signature, all under a single service. It serves as a hybrid mechanism which assures the confidentiality of the user's data and privacy in accessing its configured applications. The cryptographic standards serve multiple algorithms simultaneously.

Security Requirements Cloud Computing

The requirements of such mechanism are:

1) **Confidentiality of data:** No one can uncover information about data content from the query and response as well as the cipher texts itself.
2) **Privacy of the data owner**: No one can learn the actual identity of the data owner from the encrypted content.
3) **Integrity and Authenticity of Data**: It provides the correctness of the data which is sent by the user and the originality which is assured by the digital signature to confirm the source identity and its data ownerships.

Technological advancements over the last few decades will lead the social and informational 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 than it previously does. The 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 directed various areas like automation, GPS, nearest entities, etc.

Among other things, LBS let users access relevant and up-to-date information about their surroundings, inform others of their whereabouts, and get instant access to maps and traffic information for their current location. Whether used for fleet tracking or inventory management, for machine-to-machine communications, or for social networking or entertainment, LBS can create a more dynamic user experience that adds value and convenience and changes the way people transact business and organize their activities and free time. But there is a debate towards restricting the information contents passing in an application. If the application is getting more control over the user's information than it may leak 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 regularly transmit their location to a network, they also enable the creation of a precise record of a user's location over time. This can result in the creation of a very accurate and highly personal user profile, which raises questions of how, when and by whom this information can and should be used.

B. Types Location Based Service

Analysts and researchers have taken several approaches to classifying LBS applications. A major distinction of services is whether they are person-oriented or device-oriented.

- ***Person-oriented LBS****: It* comprises all of those applications where a service is user-based. Thus, the focus of application use is to position a person or to use the position of a person to enhance a service. Usually, the person located can control the service (e.g., friend finder application).
- **Device-oriented LBS**: These applications are external to the user. Thus, they may also focus on the position of a person, but they do not need to. Instead of only a person, an object (e.g., a car) or a group of people (e.g., a fleet) could also be located. In device-oriented applications, the person or object located is usually not controlling the service (e.g., car tracking for theft recovery).
- In addition to this first classification of services, two types of application design are being distinguished: push and pull service.
- ***Push services*** imply that the user receives information as a result of his or her whereabouts *without having to actively request it*. The information may be sent to the user with prior consent (e.g., a subscription-based terror attack alert system) or without prior consent (e.g., an advertising welcome message sent to the user upon entering a new town).
- ***Pull services,*** in contrast, mean that a user actively uses an application and, in this context, "pulls" information from the network. This information may be located-enhanced (e.g., where to find the nearest cinema).

C. LBS Process

Location-based applications are one of the most anticipated new segments of the mobile cloud industry. These new applications are enabled by GPS-equipped phones. These services are designed to give consumers instant access to personalized, local content. In this case, local content is local to the consumer's immediate location. Some of these applications will couple LBS with notification services, automatically alerting users when they are close to a preselected destination. LBS proponents believe that these services will create new markets and new revenue opportunities for device manufacturers, wireless providers, and application developers. The goal was to provide enhanced LBS solutions for people to stay in touch with their friends and family, to be able to find one another, and to get directions to local shops and restaurants. Thus, there are some objectives for designing the LBS are:

(i) Deliver relevant user information about the location of a friend or family member's mobile cell phone position.
(ii) Calculate driving directions from a mobile cell phone position to an address or point-of-interest (POI).
(iii) Provide for the selection of a business POI meeting place between two mobile cell phone positions.
(iv) Provide for the selection of a business POI in proximity to a mobile phone position.

I. While designing the LBS various integrated functionalities is required like data capture and collection starting with the digital road maps, point of information (POI) and dynamic data handling. Map data are stored in a vector format composed of line segments (links) representing the roads and connecting points representing intersections or other road features. Each link has start and end points and may also incorporate shape points to model the curvature of the road. Concierge applications use business and landmark information that has been compiled into POI databases.

II. Integrating the map database with the POI database creates a detailed, digital representation of the road network and business services available 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 Geo-coded, 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 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 Geo-coding, reverse Geo-coding, and routing are key technologies built into the Location Engine. Proximity search is an important feature of which and location engine is equipped with. Proximity searches use the 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, Geo-coding, and routing software form the basic components that application developers use to build custom LBS applications.

D. BACKGROUND

Location based service is gaining popularity with the smart mobile cloud 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 engines process 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 user's data confidentiality. Solutions proposed for addressing privacy issues in the LBS up until now have not provided complete privacy for all the parties involved in either the client-server model or the peer-to-peer model.

One needs to be careful when designing solutions for these problems since ad-hoc or heuristic solutions may lead to one or more parties unintentionally revealing private data. Hence, one needs solutions that are amenable to rigorous analysis of their security properties, and also which are practical and not too expensive to implement in practice. Another point that may be a matter of concern is that, typically, in applications such as LBS, the software running on the parties' machines (server and users) is assumed to be trusted to perform secure computations. Software can easily be modified and all parties need to be assured that the computations performed on any particular device are trustworthy.

Hence, trust cannot depend on software alone, trusted hardware must also be part of the process of trust establishment. The need to design privacy-preserving solutions for LBS that meet the twin goals of being efficient and feasible to implement while being amenable to formal analysis in a framework that is based on trusted software and hardware was the main motivating factor that led to the development of this dissertation.

Accuracy Requirements

Applications need various types and level of information from the local Geo-location device. There must an accuracy construct between the application requirement and its actual information accessing structure. If the application is accessing more than its requirements, there a chance of information leaks or uncertainty. This leaked information may be used for some malicious act or any unauthorized system drops. Hence, the system

must have a proper control on the parameters of integrity, confidentiality and availability of the information. Let us take a look over the accuracy requirements of various applications as per their types table 1.

Application	Accuracy	Application	Accuracy
News	Low	Gaming	Medium
Directions	High	M-Commerce	Medium to High
Traffic Information	Low	Emergency	High
Point of Interest	Medium to High	Sensitive Transportation	High
Yellow Pages	Medium to Low	Child Tracking	Medium to High
Car Navigation	Medium to High	Pet Tracking	Medium to High
Personal Navigation	High	Electronic Toll Collection	Medium to High
Directory Assistance	Medium to High	Public Management System	Medium to High
Car Tracking	Medium to High	Local Advertisement	Medium to High
Asset Tracking	High	Location-Sensitive Billing	Medium to Low

TABLE-I: APPLICATION DATA ACCURACY REQUIREMENTS

The accuracy debate leads to the third area of location use and probably the most ubiquitous one in the future: the commercial use of positioning information. For some time, marketers have been unsure whether lower levels of accuracy as they are obtained would be sufficient to launch compelling consumer and business services. Yet, early service examples show that the accuracy level required depends very much on the service. Even with, location information it can be successfully be integrated by operators into many existing and new applications that enhance current value propositions and usability.

Requirements and Assumptions

The generalized requirements for implementing the cloud location privacy preserving system for data transfer aims towards simplicity and high security. All it needs to practically deal with information and understanding their priority of privacy. The user's information is parted into several fields contain the leveled information. The information which is most priority should be tagged accordingly. When a user demands a data or an application needs user's location information, it finds the nearest neighbours from which the connectivity can be established.

Thus, the user initially constructs the POIs (Nearest Neighbour) by first constructing and sending a query to a known LBS server over the wireless network. The LBS server retrieves the query, performs a search of its POI database, and returns a set of results to the user containing all POIs found in the specified region. Some of the identified information for practically handling such situations is:

- The developed LBS servers need not to detect the exact location of the user. The server relates the closest proximity of the hat region in terms of the general POIs for assuring the sufficient level of privacy to the user's satisfaction.
- The information exchange does not have any third party between the user and server. It reduces the probability of information leaks.
- The implementation must be able to integrate with any of the hardware device with a practically delay tolerant features and other means of data filtering.
- Query processing must be effective which deals with only certain information for

retrieval. It should block any additional information transformation which leads towards privacy degradations.

E. LITERATURE REVIEW

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 user's data more confidential from the unauthorized accesses. Proceeding towards achieving its aim there are so many works and articles are studied here. These are:

In the work [8], Locanym is suggested as a location based service with privacy preserving mechanism. It is based on Geo-located capabilities for serving the secure and verified positioning techniques for cloud 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 work 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 by 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 work [9] presents an iPDA, a system to support privacy-preserving data access in location-based cloud 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 has 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 work [10] covers the same aspect, but specifically for the mobile environment using a global network. Along with another 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 work 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 individual. Here the CliqueCloak algorithm that can handle messages that each have individual spatial and temporal resolution requirements, but also have individual privacy constraints. A measurement relative anonymity of 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 work [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 to work . 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 work [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 use 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 reduce the threshold set intersection on location tags to equality testing using de-duplication technique known as shingling. The work 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 the location tag similarity by private equality testing, a simple and efficient cryptographic primitive. A prototype 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 work gives that much of control to the 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 work [14], proposes a privacy protection solution to allow users' preferences in the fundamental query of k nearest neighbors (kNN) using a HilAnchor approach. Particularly, users are permitted to choose privacy preferences by specifying a 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 the server and receives k nearest neighbor 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 work [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 user's 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 work 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 work , a fine-grained privacy preserving location-based service (LBS) framework, called FINE, for mobile cloud 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 cloud in terms of computation and communication cost.

F. PROBLEM DEFINITION

Location based services aim to provide the accurate location information towards the application requirements. This information exchange must satisfy the user's constraints related to the privacy and confidentiality. 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 user's 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 the application then there is a chance of compromising the privacy of the user and it could be tracked.

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 reduce the probability

of this.

ii. Traditional query and LBS server will make 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 controlled for passing into layered applications restricted to their required content only in some changed forms. This will hide the provider and user's identity.

G. PROPOSED SOLUTION

This work proposed a novel approach for providing the effective privacy handling for location based services in cloud computing. Mainly most of recent applications are accessing the location information for providing the best 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 Geo-locations are used by the devices and software is embedded here for robust security. 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 user's query toward particular information from the application server. The location query contains three fields: node ID, location information and queried information request. Now the local LBS will assure the amount of information required for each application. Here is another module which assures that the location queries must go through some of secure manner. Hence it uses query cryptosystem. Here the user has a 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.

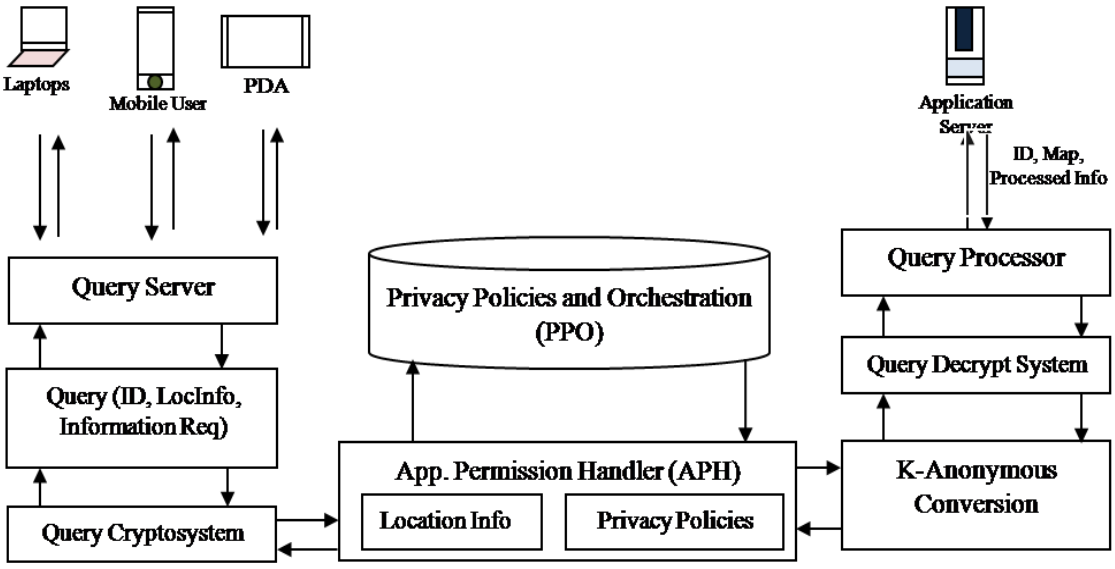

Figure 1: Novel Privacy Preserving Model for Location Based Servers (LBS) in Mobile Clouds

Now, after the information, their policies and application is matched up by the application permission handler (APH) module. This module works as an intermediation between the provider and the 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 behaviors 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 a major solution of traditional approaches issues. Once the information is converted to the active object, k-Anonymiser hides the location ID for the user. Privacy Policies and Orchestration (PPO) module adds an additional policies which could be scalable as per the requirements. It also stores the decision of the various location queries along with applications, their privileges and user group.

Here the Anonymiser assumes that the 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 the LBS server engine of

the provider's 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. 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 cloud and cloud computing.

H. APPLICATION OF APPROACH

LBS have facilitated the development of several types of services and applications:

- **Navigation and Travel –** Applications in this category allow a user to perform a search based in part on location, *i.e.*, to find the nearest hotel, ATM, bus stop, or particular restaurant.31
- **Tracking and Geo-Social Networking –** Using applications in this category, users can share their location with friends, family, or strangers via online social networks. Included in this category are applications that recommend restaurants or other places of interest based on where a user's network of "friends" has checked-in.
- **Gaming and Entertainment –** These applications allow users to play games on their wireless devices with friends and family, persons in their local network, or anyone online. Some location-based games track phone movement and create real-life scavenger hunts.
- **Retail and Real Estate** – Retail applications enable consumers to find the nearest store, provide in-store maps, check real-time inventory data, or shop from their phone, while real estate applications show houses for sale or rent or in foreclosure in a given area.
- **Advertising** – Location-based advertising allows users to receive ads relevant to their current location or based on patterns of frequently visited locations. The ads generally appear within other applications or in web browser windows.
- **News and Weather** – These applications provide users with weather and news targeted to their specific location. Some applications provide connection to local radio or TV providers for video or audio streaming, including access to police scanners.
- **Device Management** – LBS management applications allow users to track and

control their wireless devices from other sources (like a home computer) or to control other devices from their wireless devices. This may include tracking, locking, or erasing a lost phone, or locating, unlocking, and starting a vehicle.

- **Public Safety** – Some LBS applications, principally serve public safety functions. Like an application that has been developed enables students to alert campus security to an incident, provide its location, and stream live audio and video directly to the dispatcher.

II. 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 exchange between both is guided by the k-anonymity property offered by the trusted third party controller. The Primary objective with that is to manage a clear isolation between the users locate information and application. An application using the device or user's 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] YihChun Hu and Helen J. Wang, "A Framework for Location Privacy in Wireless Networks", in ACM SIGCOMM Asia Workshop, Beijing, China, doi: 1595930302/05/0004, 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