PRIVACY PRESERVING LOCATION QUERY SERVICES

Minal P. Patil[1],Lalita R. Shinde[2],Pooja R. Walekar[3],Pratiksha S. Kale[4],Mrs.D.P.Bhamare[5]

[1] *Student, Information Technology, Sanjivani College of Engineering Kopargaon, Maharashtra, India*
[2] *Student, Information Technology, Sanjivani College of Engineering Kopargaon, Maharashtra, India*
[3] *Student, Information Technology, Sanjivani College of Engineering Kopargaon , Maharashtra, India*
[4] *Student, Information Technology, Sanjivani College of Engineering Kopargaon , Maharashtra, India*

ABSTRACT

Location-Based Service (LBS) is getting increasingly popular with the drastic growth of smart phones and changing evolution of social network services (SNS), and it has context-rich functionalities which attract considerable large crowed of users. Some of the LBS provider uses the users location information which offer them ease and useful functions. They also uses the users location to provide needed services at any instance. Therefore, the LBS could highly breach personal privacy as the location itself contains much information about a person. Location reviles much more then the needed information which could not be a prior to maintain the security. Hence, privacy preserving location is still a challenging question now. A privacy preserving location is to be done while achieving the utility from it. Here we tackles this non-trivial dispute by designing and implementing a suite of new fine grained Privacy-preserving Location Query Protocol (PLQP).The fine grained PLQP also helps in customizing and generalizing the security perspective as a user himself want to be as. The protocol allows different levels of location query which gives a convenience to user for hiding or securing its own location from the world. It works on encrypted location information, the location information is hidden from the server itself as it is encrypted so it provides a large security for different users, and it is efficient enough to be applied in mobile platforms. Hence the chosen platform is smart phones as its use is widely increased.

Keyword : - *Location-based service(LBS), social network services (SNS),privacy-preserving location query protocol(PLPQ),K-anonymity, Cloaking region(CR),Attribute-Based encryption(ABE).*

1. Introduction

Location Based Service (LBS) use is increased now a day because of wide area for smart phones is introduced with new and vast specification for GPS and social networking. Many smart phones, equipped with GPS systems and have high computation ability which process holders location information. This availability brought the huge simplicity good of LBS applications in the smart phone ecosystem. A good example is a camera in the smart phone, if person takes a photo with a camera of a smart phone, the location where the snap is taken is embedded in the picture taken automatically, which helps person to remember location. After which the excess growth of social network services (SNS) also associated its growth by construct connections between location information and social network. As a photograph taken by a smart phone (location embedded) is uploaded to the Face book photo album, the system without human intervention shows the location of the picture on the map, and this is shared with the persons friends in the Facebook , unless the privacy setting specifies otherwise. There are many similar applications which exploit both LBS and SNS similarly. They tender several striking functions, but location information contains much more and wide information than hardly the location itself, which could lead to unwanted information escape. The simplest way, which most of applications used now a day is to create group based access control on published locations application, specify security for a members of group who can or cannot see them. Social photograph sharing website like Flicker only allow users to choose all users, friends, family and neighbor to gain the right to use to the locations, and SNS websites as Face book and Google+ in addition support convention groups to specify the accessible user groups. Some mobile applications are of inferior quality. Many mobile applications like Circle, Who's around and Foursquare don't even offer group choices to the one who use it, as an alternative, this

applications only inquire whether the user want to revile his location or not. Apparently, it is very simple to accomplish what users want. Firstly, from user's point of view, it is hard enough to unambiguously settle on a user group and that too in such a way that their locations are visible only to the group created. It is2 more accepted to find a circumstance such that one who satisfies it can or cannot see the location. Secondly prior, binary access control i.e., can or cannot view the location is far beyond an adequate amount to appropriately put together the privacy setting [1].

2. Literature Survey

2.1 Safeguarding location privacy in wireless ad-hoc networks:
There are several all of it achieving privacy-preserving location query. Mobile devices a well-known as know backwards and forwards phones or GPS-enabled cars came up to snuff the retrieve of location based services from approximately anywhere at complete time. Current location-based services are centered from one end to the other the summary to constantly sense a user's location in term to grant and prepare information services based on that location. Way review instructions, a location-based service provider (LSP) that is consistently monitoring a user's location can promptly respond and recalculate a modified set of instructions. As these devices will be permeating our by the day lives they further more maintain privacy risk, an LSP that tracks the activity of a user automatically at for the most part times by all of a valuable degree of spatial and physical precision, is absolutely able to bring about a meticulous user picture that does not unaccompanied include a fastidious his-tory of the users movements but also reveals which quality of information has been accessed to what place and when[2].

2.2 Rumor riding: Anonymizing Unstructured Peer-to-Peer Systems:
There are two dominant categories of anonymity models for defining the anonymity degree. The models in the first category interpret the anonymity of a certain node as the number of peers that have an equip probable chance of as a result of the given node, which is termed as anonymity set. The second category employs measurements based on information theory, for concrete illustration the mutual idea, to adopt the similarity between two entities, a well-known as the input/output links or suspected participants. The anonymity set used by the first category is extensively adopted due to its capacity of locking up the common features of anonymity. The second ideal focuses on the evidence leakage in anonymous systems. The typical usage of the ideal is to study the anonymity in so called covert channels. We assume the first anonymity ideal and define the Anonymity Degree (AD) as the probability of making an incorrect guess to notice a participant. A higher degree infers that better anonymity has been achieved[3].

2.3 Privacy preserving cloud data access with multi-authorities:
Sahai and Waters approaching a new type of IBE Fuzzy Identity-Based Encryption, which is besides known as Attribute-Based Encryption(ABE). In their field, an identity is viewed as a set of explanative attributes. Different from the IBE, where the decryptor could decrypt the message if his parity is surely the uniform as what specified by the encrypter, this fuzzy IBE enables the decryption if there are identity overlaps exceeding a pre-set threshold mid the one specified by encrypter and the one belongs to decrypter. However, this quite threshold-based schema was depending on for designing preferably general system because the threshold based semantic cannot describe a general condition. More general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-Policy Attribute-Based Encryption (CP-ABE), are eventual by Goyalet al. and Bethencourt etal. respectively to return the aforementioned obstacle of fuzzy IBE. They observe similar, anyhow cipher text and key structures are totally march to a antithetical drummer, and the term of encryption procedure (who can or cannot decrypt the message) is made by different parties[4].

2.4 Can Homomorphic encryption be practical:
In this paper two types of HE has been explained namely Partially Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE). PHE supports continuous number of additions and multiplications, and FHE supports complete additions and multiplications nonetheless it is for all practical purposes less feasible than PHE. Many crypto systems have homomorphic properties: RSA, ElGamal, Benaloh, Paillier, yet only extend additive or multiplicative homomorphism, not both. First program that manage both: Boneh-Goh-Nissim 2005 multiple additions and one multiplication (uses pairings).Fully homomorphic encryption allows doing unpredictable computations on encrypted disclosure without intelligent the confidential key, in distinctive it allows doing an unpredictable number of additions and multiplications. Gentry approaching the alternately fully homomorphic encryption schema in 2009 based on model lattices.The reality is a comparatively homomorphic encryption schema

that can consider low degree polynomials on encrypted data. Cipher texts are noisy and the noise grows slightly everywhere addition and strongly around multiplication. If the SWHE schema can manage its secure decryption course, previously a bootstrapping step can restore cipher texts by homomorphically decrypting by an encrypted confidential key. Only all of it by squashing the decryption circuit. So smoothly quite inefficient[5].

2.5 Functional Encryption: Definitions and Challenges:

The terminology Functional Encryption and its general production, and behind in 2011, Bonehet al. formally bounded it and discussed its challenge. The formal design of practicable encryption is called up by giving unambiguous definitions of the production and its security. Roughly speaking, practicable encryption supports restricted confidential keys that authorize a time signature holder to recognize a persistent field of encrypted message, not with standing recognize nothing else approximately the data. For concrete illustration, if and only if an encrypted course of action the confidential key manage enable the time signature holder to recognize the product of the position on a specific input without study anything else about the program. It is uncovered that defining warranty for practicable encryption is non-trivial. Firstly, it shows that a spontaneous game-based statement is incapable for several functionality. It then detail a spontaneous simulation-based definition and prove that it (provably) cannot be accomplished in the standard model, but cut back be finished in the arbitrary oracle model. It unmask how to manual many actual concepts to our formalization of rational encryption and perform with either interesting unmask problems in this new area. In a sensible encryption program, a decryption key allows a freak to recognize a employment of the encrypted data. Briery, in a practicable encryption position for functionality modeled as a Turing Machine an power holding a master confidential key can bring about a key that enables the computation of the field on encrypted data. More straight, by the decryptor can count one by one F(k; x) from an encryption of x. intuitively, the warranty of the program guarantees that one cannot recognize anything more virtually x, but as we shall manage, locking up this rigorously is appropriately challenging[6].

2.6 Identity-Based Encryption from the Weil Pairing:

The warranty of the interpretation relies on the fundamental that no probabilistic polynomial- time algorithms cut back solve the DDH stoppage or DBDH problem mutually non-negligible advantage. This is a principally made theory in distinct cryptographic works. It proposes a fully factual identity-based encryption schema (IBE). The schema has preferred cipher text warranty in the indiscriminate oracle ideal assuming a variant of the computational Diffie- Hellman problem. This program is based on bilinear maps during groups. The Weil pairing on elliptic curves is an concrete illustration of one a map. It gives unambiguous dentitions for retrieve identity based encryption schemes and gives part of applications for one systems[7].

2.7 Cipher text-policy attribute based encryption:

As more confidential disclosure is diffiuse and collected by third-party sites on the Internet, there will be a prefer to encrypt disclosure stored at these sites. One setback of encrypting statement, is that it can be selectively shared abandoned at a coarse-grained directly (i.e., giving another pastime your inaccessible key). Anew crypto system for fine- grained show and tell of encrypted data that is further called as Key-Policy Attribute-Based Encryption (KPABE) is developed. In this crypto system, crypto graphed texts are labeled with sets of attributes and unknown keys are associated with retrieve structures that direct which cipher texts a user is talented to decrypt. It demonstrates the applicability of our interpretation to show and tell of audit-log reference and announcement encryption. This point supports commission of unknown keys which subsumes Hierarchical Identity-Based Encryption (HIBE)[8].

2.8 Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption:

Previous constructions of ABE were only proven to be selectively secure. It achieves full security by adapting the Previous constructions of ABE were detached proven subsequent selectively secure. It achieves realized security by adapting the dual system encryption methodology in a different way introduced by Waters and before leveraged to receive fully recover IBE and HIBE systems. The primary dare in applying dual system encryption to ABE is the richer arrangement of keys and cipher texts. The system is constructed in composite term bilinear groups, to what place the censure is a yield of three primes. It proves the security of our system from three denunciation assumptions. The ABE schema supports unpredictable monotone retrieve formulas. As for ABE, ahead of time constructions of one schemes were unattended proven expected selectively secure. Security is proven under a non-interactive support whose period of time does not await on the location of queries. The schema is comparably practicable to actual selectively retrieve schemes. It further presents a fully recover hierarchical PE schema under

the related assumption. The time signature technique used to receive these results is an elaborate combination of the dual system encryption methodology (adapted to the technique of inside product PE systems) and a new concern on bilinear pairings via the suspicion of dual pairing vector spaces (DPVS) approaching by Okamoto and Takashima[9].

2.9 A peer-to-peer spatial cloaking algorithm for anonymous location-based service:
The spatial cloaked orientation is computed as the part that covers the full group of peers. Two modes of operations are experienced within the coming P2P spatial cloaking algorithm, namely, the on require set and the proactive mode. Experimental results prove that the P2Pspatial cloaking algorithm operated in the on-demand mode has fall apart communication charge and better quality of services than the proactive mode, for all that the on-demand incurs longer response time. Mobile users adopting the P2P spatial cloaking algorithm can preserve their privacy without seeking help from entire centralized third party. Other than the quickly comings of the centralized concern, the trade is by the same token motivated by the hereafter facts:
1. The computation power and storage power of approaching mobile devices have been well at a fast pace.
2. P2P communication technologies, a well known as IEEE 802.11 and Bluetooth, have been generally deployed.
3. Many new applications based on P2P information sharing have urgently taken shape[10].

2.10 Protection of location privacy using dummies for location-based services:
To handle a LBS, the user needs to propel his/her location information onto the job provider, and then the trade provider provides its function based on the user's location. Such location idea is inherently private, over it can reveal the existing information, e.g., to what place the user lives, at which join he/she works, etc. This problem specially becomes genuine when the user continuously uses the LBS for the accumulated location histories makes easier to identify such unknown information[11].

Conclusion from Literature Survey:
From above literature survey we comes to know that there are lots of problems due to location tracking and its too easy for existing tools to track the locations like Friends Search and also in many company ,they uses to track employees location for their purpose but its hard in many situation and create lots of problem. In existing system there are many security systems are available that are based on grouping of people at highest level of security. But its not a feasible solution some systems are provide security based on distance of location founder. So we are introducing the multiple level security for location. Many concepts like grouping of people and based on than specify the condition to it are used on extend level from referred papers.

3. Problem Statement
We are introducing a ne-grained Privacy-preserving Location Query Protocol (PLQP) which enables queries to get location idea (e.g., Searching a friends echo location, Finding nearest friends) without violating users location privacy. It provides the addition querier based security to the location sharing. Main contributions to the program are three field:

3.1 Fine-Grained Access Control:
This guideline allows users to provide a condition rather of a collection and exert access control over the users who satisfy this condition. This is greater scalable being users can just add a new condition for new privacy setting instead of hand-picking hundreds of users to construct a new group. Also, this is preferably users friendly because users themselves do not definitely know which of their friends should or should not access the idea most of time[1].

3.2 Multi-leveled Access Control:
The protocol also supports semi-functional encryption. That is, the custom enables users to control to what extent (or level) others can recognize his location. The lowest on the threaten no one, and at the cutting edge level corresponds to ones like two peas in a pod location. Levels during them conform to indirect information about on ce location[1].

3.3 Privacy-Preserving Protocol:
In this protocol, individually location information is encrypted and queries are processed upon cipher texts. Therefore, a location publishers friends get nothing for all that the result of the location search, which is under the

location publishers control. In addition, for every location is encrypted, eventually the server who stores location information does not extract anything from the cipher text[1].

5. System Framework

5.1 System architecture

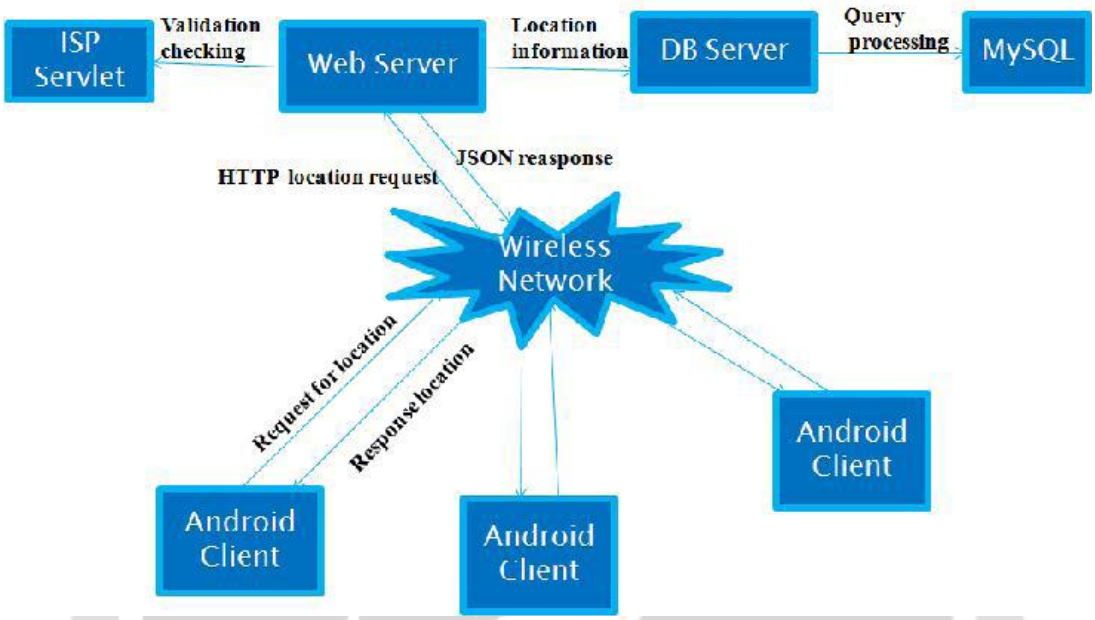

Fig -1: System Architecture

5.1.1 Web Server:
Set of web services are created to handle to requests from the android clients. Interact with database server as per the requirement of client requests.Request to SMS Gateway to send SMS.

5.1.2 Database Server:
Use to store all the data in the proposed system when querier required data it fetch the query and based on that provides to the server.

5.1.3 Android Clients:
Have and application design with user friendly simple GUI Will send requests to web server as login, registration, vote etc Connect with hardware model using Bluetooth Show result back to user Interface between system and user.

5.1.4 ISP Servlet
Used to process validation of requested client. Give feedback to web server about giving the authority of accessing location information to requested client.

5.2 Mathematical Definetion:
We use the concept of secret sharing for all the computation and comparison In cryptography, secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. It gives tight control and removes single point vulnerability. Individual key share holder cannot change/access the data Goal is to divide some data D (e.g., the safe combination) into n pieces D1,D2.Dn in such a way that:
1. Knowledge of any k or more D pieces makes D easily computable.
2. Knowledge of any k -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely). This scheme is called (k, n) threshold scheme. If k=n then all participants are required together to reconstruct the secret

5.2.1 Shamir Secret Algorithm:

Shamir intended a nation key encryption scheme in which the public key can be an arbitrary string. In such a scheme there are four algorithms:

1. setup generates global program parameters and a master-key
2. extract uses the master-key to generate the private key corresponding to an arbitrary public key string
3. encrypt encrypts messages via the public key ID
4. decrypt messages for the exact private key[3].

Setup: PK, MK. The project algorithm takes no one as input other than the implicit security parameter. It outputs the public parameter PK and a master key MK. The master key supplement the issuer and is laid away secret.

Encrypt (PK, M, T): ET (M). The encryption algorithm takes as input the public key PK, a message M, and an access tree T. It will encrypt the message M and returns a cipher text CT a wellknown that only a user with key useful the access tree T can decrypt it.

Key Generate (PK, MK, S): SK. The Key Generation algorithm takes as input the public key PK, the master key MK and a set of attributes S. It outputs a private key SK which contains the attributes in S.

Decrypt(PK, SK, ET (M)) : M. The decryption algorithm takes as input the public parameter PK, a private key SK whose attribute set is S, and a cipher text CT which contains an access tree T . It outputs the original message M if the set S satisfies the access tree T [7].

6. CONCLUSIONS

The proposed a fine-grained Privacy-preserving Location Query Protocol (PLQP), which successfully solves the privacy problems in active LBS applications. It also provides various location based queries. This PLQP uses our new distance computing and comparison protocols to put into practice semi-functional encryption. This semi-functional encryption supports multi leveled access control, and it use CP-ABE as supplementary encryption scheme which make access control be highly fine-grained. During the whole protocol, if not proposed by the location publisher, the location information is kept secret to anyone else using any system to search location. Experiments are conducted to show the performance of protocol is appropriate in a real mobile network. Using this fine-grained Privacy-preserving Location Query Protocol (PLQP) the Location can be hide from undesired persons, any unwanted organizations and existing system. By implementing this project we can provide security in various fields like army, navy, detective agencies and also for common people. As any user can set their own privacy profiles according their own needs it is feasible to use this system. User can themselves change their privacy any time according to conditions. It provides querier safety and accuracy than the existing system.

7. REFERENCES

[1]. Xiang-Yang Li and Taeho Jung, Search me if you can: Privacy preserving location query service, IEEE TRANSACTIONS MOBILE COMPUTING YEAR 2013.

[2]. T. Hashem and L. Kulik, Safeguarding location privacy in wireless ad-hoc networks,
Ubicomp 2007: Ubiquitous Computing, pp. 372390, 2007.

[3]. Y. Liu, J. Han, and J. Wang, Rumor riding: anonymizing unstructured peer-to-peer systems, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 3, pp. 464475, 2011.

[4]. T. Jung, X. Li, Z. Wan, and M. Wan, Privacy preserving cloud data access with multi authorities, in IEEE INFOCOM, 2013.

[5]. K. Lauter, M. Naehrig, and V. Vaikuntanathan, Can homomorphic encryption be practical, Preprint, 2011.

[6]. D. Boneh, A. Sahai, and B. Waters, Functional encryption: Definitions and challenges, Theory of Cryptography, pp. 253273, 2011.

[7]. D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, in Advances in Cryptology EURYPTO 2001, pp. 213229.

[8]. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, in IEEE Symposium on Security and Privacy, 2007.

[9]. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, Advances in Cryptology EUROCRYPT 2010, pp. 6291, 2010.pp. 321334.

[10]. C. Chow, M. Mokbel, and X. Liu, A peer-to-peer spatial cloaking algorithm for anonymous location-based service, in Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, 2006, pp. 171178. 37
[11]. H. Kido, Y. Yanagisawa, and T. Satoh, Protection of location privacy using dummies for location-based services, in 21st International Conference on Data Engineering Workshops, 2005, pp. 12481248.