IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. VI (Nov – Dec. 2015), PP 52-56
www.iosrjournals.org

Privacy - Preserving Reputation with Content Protecting Location Based Queries

Dr.S.Sujatha[1] (HOD), N.Premalatha[2] (M.Phil scholar)
[1](School of Information Technology & Science,Dr. G. R. Damodaran College of Science,Coimbatore)
[2](School of Information Technology & Science,Dr. G. R. Damodaran College of Science,Coimbatore)

Abstract: *Privacy based Context-aware systems based on location open up new possibilities to users and data servers in terms of acquiring custom services by gathering context information, especially in systems where the high mobility of users increases their usability. Location-based applications utilize the positioning capabilities of a mobile device to determine the current location of a user, and customize query results to include neighbouring points of interests. However, location knowledge is often perceived as personal information. One of the immediate issues hindering the wide acceptance of location-based applications is the lack of appropriate methodologies that offer fine grain privacy controls to a user without vastly affecting the usability of the service. In this paper, novel approach is proposed as a solution to one of the location-based query problems through Privacy preserving based Context Reputation System. The Solution of the System is as Follows, a user wants to query a database of location data, known as Points of Interest (POIs) with respect of protecting their location Information against data leakage. Similarly the owner of the location data, that is, the location server, does not want to simply distribute its data to all users. The location server desires to have some control over its data, since the data is its asset, hence security mechanism named as shared Authority is employed against data sharing also data is reputed based on the reputation mechanism . The solution is efficient and practical in many scenarios. By implementing the solution, it is possible to access the efficiency of the protocol and proposed introducing a security model and analysing the security and reputation of the context of protocol will improve the performance of the system.*

Keywords: *Location Based Service, Information Retrieval, Privacy Preserving*

I. Introduction

Location Based Service is promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling. LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by a LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of location based Services . Users may feel reluctant to disclose their locations to the LBS, because it may be possible for a location server to learn who is making a certain query by linking these locations with a residential phone book database, since users are likely to perform many queries from home. Conventional security approaches mainly focus on the strong authentication to realize that a user and owner can access data based on some security. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the data security . As long as queries are fast enough, considerations such as flexibility (in the types of queries supported), low space consumption, predictable performance, realistic modeling, and robustness (with respect to the cost function) are more important for data accessing in Location based servers. To overcome these limitations, we take a different approach. We propose a unified framework for dealing with POI-related queries based on shared Authority mechanism for Context aware reputation system. Therefore the LBS have to ensure that LS's data is not accessed by any unauthorized user. During the process of transmission the users should not be allowed to discover any information for which they have not paid. It is thus crucial that solutions be devised that address the privacy of the users issuing queries, but also prevent users from accessing content to which they do have authorization and employing of authority for authorizing the content. Authentication: a legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user. Also any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via

an open channel. The rest of paper is organized as follows; section 2 explains the background knowledge regarding the related work. Section 3 explains and formulates the proposed System. The experimental results are discussed in section 4; we conclude the work with future work of the paper at section 5.

II. Related Works

2.1. Private information retrieval suing Mix –Zone Approach

The privacy of the user is maintained by constantly changing the user's name or pseudonym within some mix-zone. It can be shown that, due to the nature of the data being exchanged between the user and the server, the frequent changing of the user's name provides little protection for the user's privacy. They investigated the required number of users to satisfy the unlink ability property when there are repeated queries over an interval. This requires careful control of how many users are contained within the mix-zone, which is difficult to achieve in practice.

2.2. A hybrid technique for private location-based queries with database protection

Mobile devices with global positioning capabilities allow users to retrieve points of interest (POI) in their proximity. To protect user privacy, it is important not to disclose exact user coordinates to un-trusted entities that provide location-based services. Currently, there are two main approaches to protect the location privacy of users: (i) hiding locations inside cloaking regions (CRs) and (ii) encrypting location data using private information retrieval (PIR) protocols. Previous work focused on finding good trade-offs between privacy and performance of user protection techniques, but disregarded the important issue of protecting the POI dataset D. For instance, location cloaking requires large-sized CRs, leading to excessive disclosure of POIs (O(|D|) in the worst case). PIR, on the other hand, reduces this bound to , but at the expense of high processing and communication overhead. In the first step, user locations are generalized to coarse-grained CRs which provide strong privacy. Next, a PIR protocol is applied with respect to the obtained query CR. To protect excessive disclosure of POI locations, we devise a cryptographic protocol that privately evaluates whether a point is enclosed inside a rectangular region. By introducing an algorithm to efficiently support PIR on dynamic POI sub-sets.

2.3. Measuring query privacy in location-based services

The popularity of location-based services leads to serious concerns on user privacy has analysed. A common mechanism to protect users' location and query privacy is spatial generalisation. As more user information becomes available with the fast growth of Internet applications, e.g., social networks, attackers have the ability to construct users' personal profiles. This gives rise to new challenges and reconsideration of the existing privacy metrics, such as *k*-anonymity. In this literature, analyse new metrics to measure users' query privacy taking into account user profiles. Furthermore, gathering details about design spatial generalisation algorithms to compute regions satisfying users' privacy requirements expressed in these metrics.

2.4. Trusted anonymiser approach

In this system which allows the users to set their level of privacy based on the value of *k* anonymization *[3]*. This means that given the overhead of the anonymiser, a small value of *k* could be used to increase the efficiency. Conversely, a large value of *k* could be chosen to improve the privacy, if the users felt that their position data could be used maliciously. Choosing a value for *k*, however, seems unnatural. There have been efforts to make the process less artificial by adding the concept of feeling-based privacy Instead of specifying a *k*, they propose that the user specifies a cloaking region that they feel will protect their privacy, and the system sets the number of cells for the region based on the popularity of the area. The popularity is computed by using historical footprint database that the server collected.

III. Proposed Model

3.1. Location based service(LBS) protocol model

It is information, entertainment and utility service generally accessible by mobile devices such as, mobile phones, GPS devices, pocket PCs, and operating through a mobile network. LBS can offer many services to the users based on the geographical position of their mobile device. The services provided by LBS are typically based on a point of interest database. By retrieving the Points Of Interest (POIs) from the database server, the user can get answers to various location based queries, which include but are not limited to - discovering the nearest ATM machine, gas station, hospital, or police station. The major important database for LBS

- Point of Interest database
- Phone Book Database
- Historical footprint database

The system model consists of three types of entities; The user does not need to be concerned with the specifics of the communication. The users in our model use some location-based service provided by the location server set of users- record describes a POI, giving GPS coordinates to its location record describes a POI, giving GPS coordinates to its location mobile service provider - The user does not need to be concerned with the specifics of the communication. The users in our model use some location-based service provided by the location server location server - location server *LS* owns a set of POI records

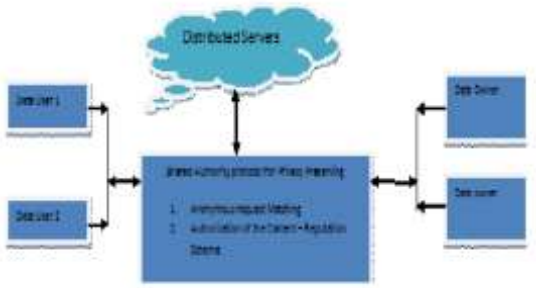


Figure 3.1. Architecture of the Location based Privacy and Reputation System

3.2. Adaptive Oblivious Transfer Protocol

The protocols contain two phases, for the data retrieval operations for initialization and for transfer.

- **Initialization Phase**

The initialization phase is run by the sender (Bob) who owns the N data elements X1, X2, XN. Bob typically computes a commitment to each of the N data elements, with a total overhead of O (N).

- **Transfer phase**

The transfer phase is used to transmit a single data element to Alice. At the beginning of each transfer Alice has an input I, and her output at the end of the phase should be data element XI. An OTN k×1 protocol supports up to k successive transfer phases

Algorithm – Secure data Transmission
Input: Input Query and Data Records based on Location
Process;

Initialization

- Applying the query processing through user Anonymization
- Applying the data encryption using ECC algorithm

Transmission

If query is right user
Transmit the encrypted data with key
Else
Terminate the query

Output: Secure query processing and Secured data contents in server

3.3 Establishing a secured communication against the Data owner at receiver phase

In this design the secured data retrieval is carried out as follows

3.3.1.Data Retrieval and Decryption mechanism

The server then processes the encrypted records through the use of decryption technique to the query records With the knowledge about which cells are contained in the private grid, and the knowledge of the key that encrypts the data in the cell, the user can initiate a private information retrieval protocol with the location server to acquire the encrypted POI data. Assuming the server has initialised the integer *e*, the user *ui* and *LS* can engage in the following private information retrieval protocol using the $IDQ_{i,j}$, obtained from the execution of the previous protocol, as input. The $IDQ_{i,j}$ allows the user to choose the associated prime number power πi, which in turn allows the user to query the server.

Once the database has been initialised, the user can initiate the protocol by issuing the server his/her query. The query consists of finding a suitable group whose order is divisible by one of the prime powers.

Algorithm for Secure Data Retrieval
Input: Query data
Process
Generate the M distinct parameter of the query
For each server record
Apply the decrypt for whole distribution
If query request is accepted
Mine the Suitable record based on the data mining Technique
Else
Report the user without data
Display record for authorized user
End for
Output – Secure data Retrieval

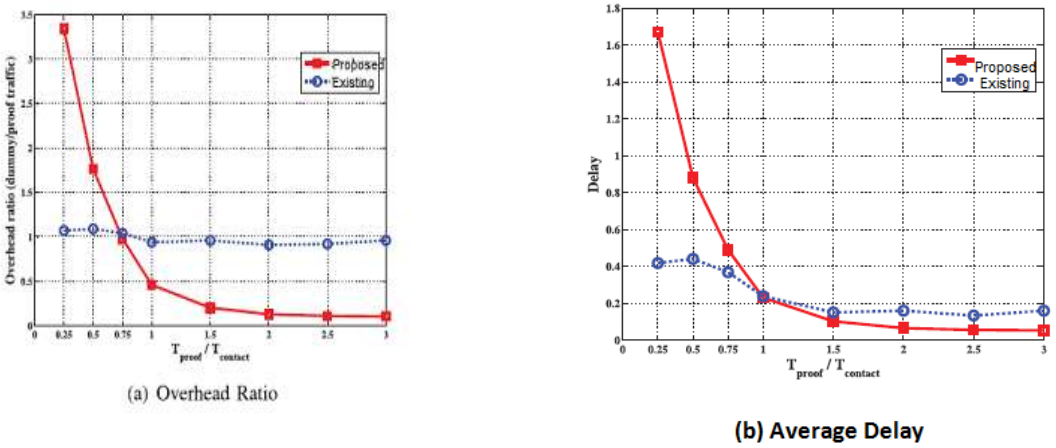
3.4. Privacy preserving Reputation technique

Misleading data can be controlled by the Privacy based reputation Mechanism. Data integrity is identifying the tampered data fields against the data user and data owner. This is achieved with respect to the authorization principle through shared authority. Storage integrity auditing mechanism, which introduces authorization rule coded data to enhance secure and dependable storage services. The scheme allows users to audit the location storage with lightweight communication overloads and computation cost, and the auditing result ensures strong location storage correctness and fast data error localization User revocation is achieved by a revocation list without updating the secret keys of the remaining users

IV. Experimental Results

In this section, detailed analysis about the proposed using simulating the location server and location user in the Android Platform using kitkat OS .

The most expensive operation in protocol is the modular exponentiation, through focus on minimising the number of times it is required. The System assumes that some components can be precompiled, and hence only consider the computations needed at runtime. Furthermore, to reduce the number of exponentiations required by the PIR protocol to the number of multiplications that is required in terms of the overhead and delay.



(a) Overhead Ratio

(b) Average Delay

Figure 5.2. Performance of the Private information retrieval in terms of overhead at fig 5.2.a and Average delay at fig 5.2.b

The figure 5.2. Explains the overhead and delay of the proposed (ECC encryption)and existing system(RSA encryption)of the location based Service in the data preserving at the server side and location preserving at the client side against the information retrieval and privacy management . These techniques performance is computed and evaluated against the factor mentioned above.

The proposed system has presented a solution with results in table 5.1. Offering context aware and privacy aware recommendations that take into account context information, and users' locations, privacy, and behaviour patterns.

Technique	Throughput	Elapsed time	Long point Message	Short Point Message
Privacy preserving based k anonymity	100	9ms	600	250
Privacy preserving based on the ECC scheme	90	10ms	700	300

Table 5.1. Performance Analysis of the filtering Techniques against various contexts

The proposed System protects users' information and locations by allowing users to decide the granularity at which they want to share their information, to whom, and where; and the time during which they want to reveal information.

V. Conclusion

Location based query solution that employs two protocol that enables a user to determine and acquire location data in a private manner.The first step is for a user to privately determine his/her location using oblivious transfer on a public grid.The second step involves a private information retrieval interaction that retrives the record with high communication efficiency.The proposed work analysed the performance of the protocol and found it to be both computationally and communicationally more efficient than the existing system.This work has been implemented a software prototype using a desktop machine and a mobile device.The software prototype demonstrates that the protocol is within practical limits.

Future work can involve testing approach on many different mobile devices by considering the degree of scalability ration in case of private information retrieval method.

References

[1] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in Proc. 2nd VDLB Int. Conf. SDM, W. Jonker and M. Petkovic, Eds., Trondheim, Norway, 2005, pp. 185–199, LNCS 3674.

[2]. M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," Trans. Data Privacy, vol. 3, no. 2, pp. 123–148, 2010

[3]. G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644

[4]. G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica, vol. 15, no. 14, pp. 1–28, 2010

[5]. G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in Proc. ACM SIGMOD, Vancouver, BC, Canada, 2008, pp. 121–132.

[6]. G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in Proc. 18th SIGSPATIAL Int. Conf. GIS, 2010, pp. 3–12.

[7]. P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowl. Data Eng., vol. 19, no. 12, pp. 1719–1733, Dec. 2007.

[8]. J. Krumm, "A survey of computational location privacy," Pers. Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, Aug. 2009.

[9]. L. Marconi, R. Pietro, B. Crispo, and M. Conti, "Time warp: How time affects privacy in LBSs," in Proc. ICICS, Barcelona, Spain, 2010, pp. 325–339.

[10]. T. Xu and Y. Cai, "Feeling-based location privacy protection for location-based services," in Proc. 16th ACM CCS, Chicago, IL, USA, 2009, pp. 348–357.

[11]. B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011, pp. 494–505.

[12] L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing with Anonymous ID Assignment," IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.

[13] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191.