Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Privacy for Location Based Services

[1]Chaitanya S A, [1]Samarth P Shenoy, [1]Supritha R Maiya, [1]Suryanidhi D, [2]Dr.Mohan H S

Abstract

Location-based services (LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks. Existing privacy-preserving techniques for LBS have several limitations, such as requiring a fully-trusted third party, offering limited privacy guarantees and incurring high communication overhead. In this paper, we propose location privacy using a semi trusted third party system, in which the location is sent via the semi trusted third party server to the service provider to hide the identity of the user.

Index Terms—Location based Service, Mid Server (MS), and Service Provider (SP).

Introduction

Location based services are software level services that provides real time, and relevant data to the querying user. LBS include services to identify location of a person or object, such as discovering the nearest banking cash machine (ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

These are vital information and thus, by tracking requirements of a person it is possible to build a profile which can reveal information about user's work or their lifestyle and so on. Therefore a number of approaches have been recently proposed for preserving the user's location. Fully-trusted third party (TTP) is one of the most popular privacy-preserving techniques which requires a TTP to be placed between the user and the service provider to hide the user's location information from the service provider. This method has several drawbacks which are (i)All the users have to continuously report their current location to the third party even if they do not request any service (ii)Since the third party knows the exact location of the user, the attacker easily can misuse this. Private information retrieval (PIR) or oblivious transfer (OT) is another technique proposed. Although PIR or OT techniques do not require a third party, they incur a much higher communication overhead between the user and the service provider, requiring the transmission of much more information than what was initially permitted by the user.

In this paper, we propose that we use a semi trusted third party mid server, through which we send the location to the service provider. Two main things that we have to safeguard are user's identity and user's location. The location is encrypted, using AES encryption algorithm, before it is sent to the service provider, via mid server. The user's identity is hidden by the use of the mid server. Thus, we are protecting both the user's identity and the user's location. This is valid as long as the mid server and service provider do not collude.

RELATED WORK

(1) Location-based services (LBS) are context aware systems that facilitate users in terms of providing services such as finding places, routes, ATMs etc. Using the location-context, the service provider can determine the living style, personal details and also, can track an individual. This violates the privacy of the user. Hence, the location-context must be protected from the service provider.[6] Cloaking is an often used technique to protect the location. This can be achieved by focusing on graph-based clique cloak algorithm that aims to find out the maximum clique to form the cloaked region within the maximum area provided by the user. In this approach, the probability of finding the exact user is decreased for the malicious LBS providers and the number of users getting cloaked is increased compared to the other clique cloak algorithms.

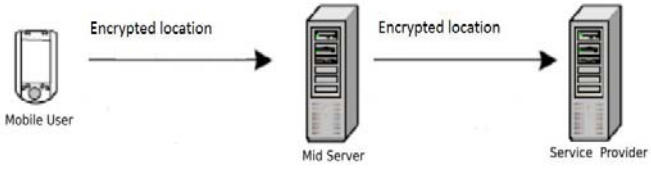
A distributed approach [4]. This approach assumes that there are multiple servers, each deployed by a different organization. A user's location is known to only one of the servers (e.g., to her cell-phone provider), so there is no single entity that knows everybody's location. With the help of cryptography, the servers and a user jointly determine whether the k-anonymity property holds for the user's area, without the servers learning any additional information, not even whether the property holds. A user learns whether the k-anonymity property is satisfied and no other information. The evaluation of this sample implementation shows that distributed k-anonymity protocol is sufficiently fast to be practical. Moreover, this protocol integrates well with existing infrastructures for location-based services.

(3)A scalable architecture [3] for protecting the location privacy from various privacy threats resulting from uncontrolled usage of LBSs. This architecture includes the development of a personalized location anonymization model. A unique characteristic of our location privacy architecture is the use of a flexible privacy personalization framework to support location k-anonymity for a wide range of mobile clients. The prototype that we develop is designed to be run by the anonymity server on a trusted platform and performs location anonymization on LBS request messages of mobile clients such as identity removal and spatio-temporal cloaking of the location information.

(4)Robust spatial cloaking technique [2] is used for snapshot and location-based queries that clearly distinguish between location privacy and query privacy. By such distinction, we achieve two main goals: (i) supporting private location-based services to those customers with public locations, and (ii) performing spatial cloaking on-demand basis only (i.e., when issuing queries) rather than exhaustively cloaking every single location update. Experimental results show that the robust spatial cloaking algorithm is scalable and efficient while providing anonymity for large numbers of continuous queries without hiding users' locations.

(5) Development of DUMMY-Q [5], a user-centric technique for query privacy protection which operates solely on the user side and does not require any trusted third party. The key idea is to confuse the adversary by issuing multiple counterfeit queries with varying service attributes but the same (real) location, henceforth referred to as dummy queries, along with each real query issued by the user.

SYSTEM ARCHITECTURE



The above figure shows the system architecture of our proposed system. This has three main parts, namely, Mobile User, Mid Server, and Service Provider.

3.1 MOBILE USER

Here the user enters the location in terms of latitude and longitude coordinates. There is a client server communication module in the mobile to transmit the user's location, this also checks if the coordinates are within the strategic sector premises.

3.2 MID SERVER

The mid server acts like a mediator and forwards the information from user to the intended service provider. The information is sent through mid-server in order to hide the details about the user.

3.3 SERVICE PROVIDER

The encrypted or unencrypted location is received here. The value of the encrypted location is displayed on the console. Similarly the location which is unencrypted is also displayed on the console.

IMPLEMENTATION METHODOLOGY

Encryption can be of two forms namely, symmetric or asymmetric. Symmetric encryption deals with a single key that is used for both the encryption of the data entered by the user, i.e. plaintext and decryption of the cipher text obtained.

Asymmetric encryption also known as public key encryption uses two keys, known as the private and public keys. The public keys are distributed among various users whereas the private keys are known only to the owner(s). Our goal here is to establish the Advanced Encryption Standard (AES), a popular symmetric key algorithm with the data provided by the user.

4.1 AES

The AES encryption algorithm is a subset of the Rjindael cipher, which comes with different key and block sizes. The AES algorithm is a globally accepted

encryption algorithm which hasn't yet been broken into. It has a block size of 128 bits and differing key lengths which can either be 128, 192 or 256 bits. We are implementing the 128 bit variant which provides sufficient security to the data.

4.2 CLIENT SERVER COMMUNICATION

We use the concept of http servlets. A servlet is a module that can be integrated into a server application to respond to client requests. Although a servlet need not use a specific protocol, we will use the HTTP protocol for communication at the client side. A URL Variable is initialised and a stream for input is opened. Secret key is generated for the process of encryption. The input location is taken after the generation of the key. An output stream is created and the data is written to the stream for further transmission. At the server side a stream is created for input and the data is read from the same and is displayed to the console.

4.3 WORKING

The location which is entered by the user is checked. If it is within the strategic sector premises (restricted or semi restricted areas), the location will get encrypted and is forwarded to the mid server. If the coordinates are not in sector premises, then the location is directly sent to service provider.

We use a client server module to transmit the location from the user to the MS and MS to SP.

There is also an additional feature or option that puts the mobile phone into Aeroplane mode when the user enters into the semi restricted area. Also, the camera gets disabled in order to avoid the user from photographing restricted information. Switching to the Aeroplane mode suspends the radio frequency transmission thereby disabling telephony, Wi-Fi, Data which is an advantage in the strategic sector, which means that the user cannot have a means of communication in the vicinity of strategic sectors.

FUTURE WORK

Further enhancements include introducing a dynamic grid for the system i.e. the location area will be divided into equal sized grid cells based on the dynamic grid structure mentioned by the user. From this, the user can send their encrypted query and the encrypted location to the service provider via the mid server. We can also include a decryption module in the SP side, where the SP decrypts the query and location. SP renders the service to the user's query by giving the point of interests. These Points of Interests (POIs) are sent back to MS where it is stored, which it later sends back the subset of POIs in the vicinity of the user. Then the user decrypts these POI's and computes their query answer. Since the user is mobile and keeps moving the user might require the information about the

POI's located in other grid cells that have not been previously requested to the MS. Since the MS already has stored information about the entire grid it need not consult the SP for the service. MS sends the required encrypted POI's back to the user.

CONCLUSION

Location based services have long been in use and the general user has reaped benefits. However, over time users begin to rely heavily on these trusted third parties to fulfil their requests. The presence of semi trusted party will provide the user the services he requests. These services are provided under the assumption that the MS and the SP do not collude. This client-server communication model achieves a certain level of privacy through the use of the MS and the SP. This paper illustrates a system in which the user can successfully obtain relevant information by making use of these features.

ACKNOWLEDGEMENT

We thank Dr.Mohan H.S, Professor & Head, Department of Information Science and Engineering, SJB Institute of Technology for his guidance. We would also like to thank Mr Rakesh A for his valuable support during the course of the paper work.

References

[1]. User-Defined Privacy Grid System for Continuous Location-Based Services Roman Schlegel, Member, IEEE, Chi-Yin Chow, Member, IEEE, Qiong Huang, Member, IEEE, and Duncan S. Wong, Member, IEEE

[2]. B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.

[3]. C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.

[4].T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in ACM GIS, 2007.

[5]. G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," in IEEE PerCom, 2009.

[6]. Shanthi and S.R. Balasundaram P "A graph-based cloak algorithm to preserve location privacy in location-based services" 2015(NIT Trichy)