IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Secure Protocol for Location Based Queries

Pooja M. Navagan[1], Nikita S. Kamble[2], Yogita S. Kayande[3], Prof. M. M. Kokate[4]

Department of I.T., JSPM's Bhivarabai Sawant Institute of Technology & Research, Pune university, India[1,2,3,4]

Abstract: In this paper we present a solution to one of the location-based query problems. This problem is a user wants to query a database of location data, known as Points Of Interest (POI), and does not want to reveal his/her location to the server due to privacy concerns. The owner of the location data, that is, the location server, does not want to simply distribute its data to all users. we propose a novel protocol for location based queries. our protocol is organized in two stages. In first stage user privately determines his/her location within public domain by using oblivious transfer this data contains both Id and associated symmetric key for the block of data in the private domain. In the second stage we are concentrating on the content protection where authorized user can only get the information he wants by using private information retrieval(PIR) method. Hence our protocol thus provides protection for both the user and the server. The user us protected because the server is unable to determine his/her location. Similarly, the servers data is protected since unauthorized user can only decrypt the block of data obtained by PIR with encryption key. The LBS has 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 not have authorization.

Keywords: private query, private information retrieval, oblivious transfer, DES algorithm.

I. INTRODUCTION

A location based service(LBS) is an service provider system which provides information related to regular needs like entertainment, nearest ATM machines, nearest gas station and etc. of the user which is accessible by mobile devices, pocket pc's and operating through mobile network or home pc/laptop in the internet network. A LBS can provide the service of different kind based on the user location. These services provided by a LBS are typically depends on point of interest database. By getting the point of interest from database the user gets the information he wants which now a day's not limited to discovering nearest ATM machines gas station, hospital or police station but also the other information related to location. In recent years there has been lot of use of different GUI devices. Among many difficult areas to the wide usage of such application privacy assurance is a major issue. For example users may feel unsafe to give their locations to the LBS, because it may be possible for location server to learn who is making a certain query by linking these locations with a database of residential phone book since users are usually request a query from home.

A location server(LS) which offers some services, will spend lot of resources to provide point of interest(POI) information to user. Hence, it is expected and needed that the LS would not give any information without authorizing the user and without any fees. Therefore the LBS has to ensure that LS's data is not accessed by any illegal user. During the process of information retrieval users should not be allowed to get any information for which they have not any authorization . It is thus very needy that solutions should be provided which addresses the privacy of the users issuing queries, but also protect the content of LS from getting accessed from unauthorized users.

II. EXISTING SYSTEM

The Location Server (LS), which offers some LBS, spends its resources to compile information about various interesting POIs. Hence, it is expected that the LS would not disclose any information without fees. Therefore the LBS has 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 not have authorization.

Claudio Bettini, X. Sean Wang and SushilJajodia, **"Protecting Privacy Against Location-based Personal Identification"**
This paper presents a preliminary investigation on the privacy issues involved in the use of location-based services. It is argued that even if the user identity is not explicitly released to the service provider, the geo localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals. The paper formally defines a framework to evaluate the risk inrevealinga user identity via location information and presents preliminary ideas about algorithms to prevent this to happen.[3]

Xihui Chen , Jun Pang, **"Measuring Query Privacy in Location-Based Services"**
The popularity of location-based services leads to serious concerns on user privacy. 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

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

reconsideration of the existing privacy metrics, such as K-anonymity. In this paper, we propose new metrics to measure users' query privacy taking into account user profiles. Furthermore, we design spatial generalization algorithms to compute regions satisfying users privacy requirements expressed in these metrics. By experimental results, our metrics and algorithms are shown to be effective and efficient for practical usage.[5]

MihirBellare, Silvio Micali, **"Non-Interactive Oblivious Transfer and Applications"**
We show how to implement oblivious transfer without interaction, through the medium of a public file. As an application we can get non-interactive zero knowledge proofs via the same public file.[7]

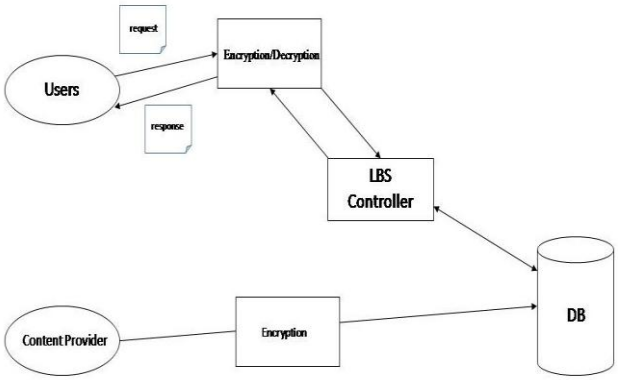
III.PROPOSED METHODOLOGY

In the first stage, the user privately determines his/her location within a public grid, using oblivious transfer. This data contains both the ID and associated symmetric key for the block of data in the private grid. In the second stage, the user executes a communicational efficient PIR, to retrieve the appropriate block in the private grid. This block is decrypted using the symmetric key obtained in the previous stage.

Our protocol thus provides protection for both the user and the server. The user is protected because the server is unable to determine his/her location. Similarly, the server's data is protected since a malicious user can only decrypt the block of data obtained by PIR with the encryption key acquired in the previous stage.

In other words, users cannot gain any more data than what they have paid for. We also provide results from a working prototype showing the efficiency of our approach.

System Architecture

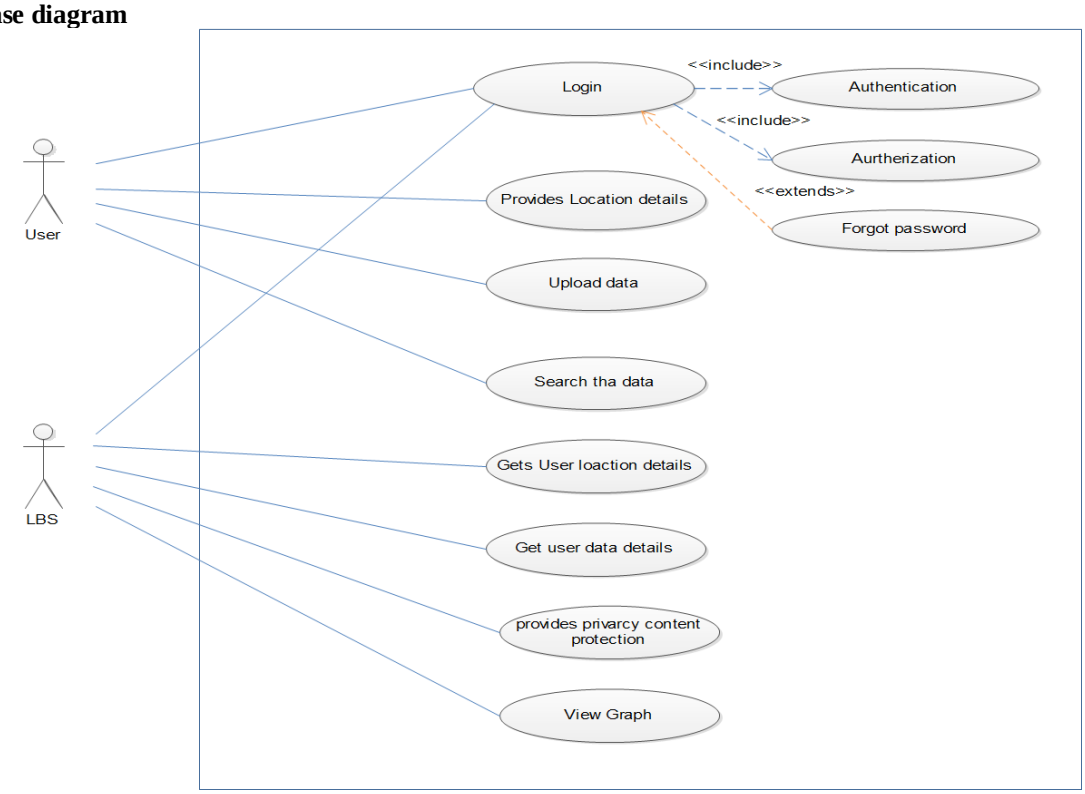


DES Algorithm

The Data Encryption Standard (DES) is a secret key encryption. A variant called Triple-DES (TDES or 3DES) uses a longer key and is more secure, but has never become popular. Triple Data Encryption Algorithm block cipher. It is so named because if applies the Data Encryption Standard(DES) cipher algorithm three times to each data block. It increases the key size of DES to protect against brute force attack without requiring a completely new block cipher algorithm. The original DES cipher key size of 56 bits was generally sufficient when that algorithm was designed but (brute force attack)so TDES provides increasing key size to protect without need of new algorithm.

Design

Use case diagram



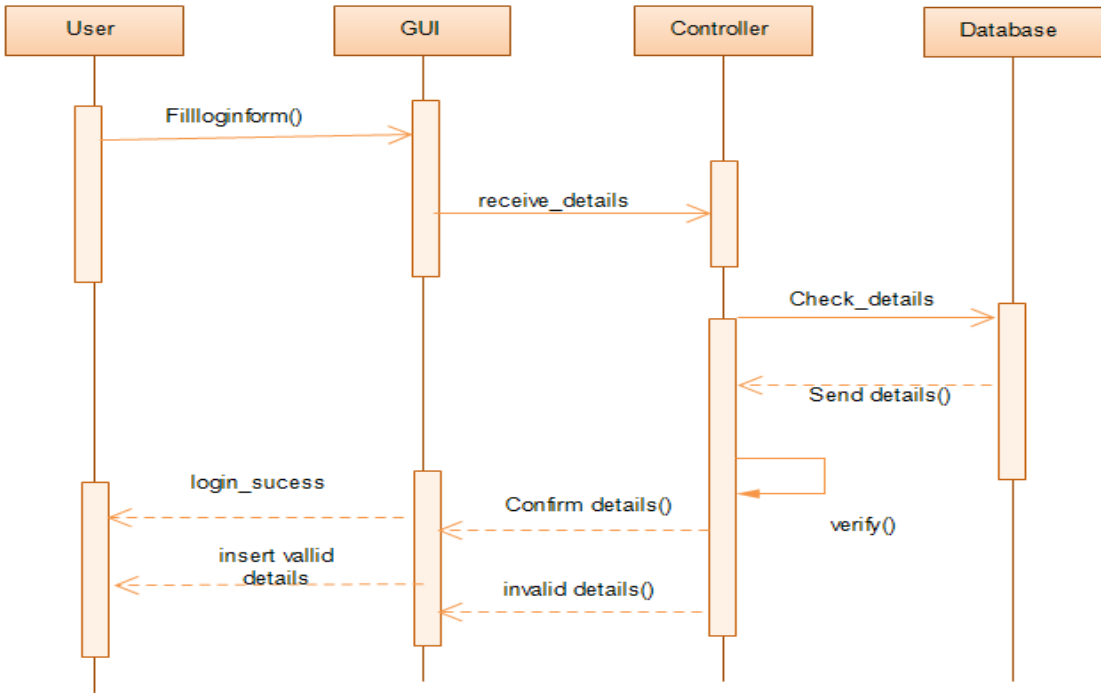
DOI 10.17148/IJARCCE.2016.53139

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Sequence diagram



IV.CONCLUSION AND FUTURE WORK

A location server (LS) which offers some services, will spend lot of resources to provide point of interest(POI) information to user. Hence, it is expected and needed that the LS would not give any information without authorizing the user and without any fees. Therefore the LBS has to ensure that LS's data is not accessed by any illegal user. During the process of information retrieval users should not be allowed to get any information for which they have not any autherization.It is thus very needy that solutions should be provided which addresses the privacy of the users issuing queries, but also protect the content of LS from getting accessed from unauthorized users.

Future Scope:- We implement our solution on a mobile device to assess the efficiency of our protocol. Future work will involve testing the protocol on many different mobile devices. The mobile result we provide may be different than other mobile devices and software environments.

REFERENCES

[1] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacy preserving and content-protecting location based queries," in *Proc. ICDE*, Washington, DC, USA, 2012.
[2] B. Palanisamy and L. Liu, "MobiMix: Protecting location privacy with mix-zones over road networks," in Proc. ICDE, Hannover, Germany, 2011.
[3] Claudio Bettina, X. Sean Wang and SushilJajodia, "Protecting Privacy Against Location-based Personal Identification".
[4] M. Damiani, E. Bertino, and C. Silvestri, "The PROBE framework for the personalized cloaking of private locations," *Trans. Data Privacy*, 2010.
[5] Xihui Chen,Jun Pang ,"Measuring Query Privacy in Location-Based Services".
[6] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," GeoInformatica,vol. 15, 2010.
[7] MihirBellare, Silvio Micali, "Non-Interactive Oblivious Transfer and Applications".
[8] Maria Luisa Damiani, Elisa Bertino, Claudio Silvestri, "The PROBE Framework for the Personalized Cloaking of Private Locations".