International Journal of Innovative Research in Engineering
Volume 1, Issue 3 (November-December 2020), PP: 44-47
www.theijire.com

Study of Data Security in Position Centered Services

P RAJA [1], M RAVIKUMAR[2]
[1,2]*Asst.Professor Department of CSE Lakshmi Narayan College of Technology, MP, India*

How to cite this paper: P RAJA [1]. M RAVIKUMAR[2] Study of Data Security in Position Centered Services, IJIRE-V1I3, 44-47.

Abstract: *In this paper, a solution for privacy preservation and data security is presented. Privacy over the internet can be defined as the ability to decide what information one discloses or withholds about a person over the internet, who can access such information and for what reason a person's information may or may not be accessed. The problem is stated as follows: (i) a client needs to inquire a database which contains some authorized and sensitive data and does not want to disclose himself to the server because of privacy concerns the owner of the database i.e the server, does not want to simply give out its data to all users. The server needs to have some control over its information, since the information is its asset. In this paper, a two stage approach is proposed to achieve secure solution for both user and the server. The first step is accomplished using Oblivious Transfer and second step is accomplished using Data Retrieval phase. And, a security model has been devised, which includes encryption and hashing algorithm for providing data security.*

Keywords *- Privacy preservation, data security, and location based services, oblivious transfer, Data Retrieval.*

I. INTRODUCTION

Privacy is one of the critical aspect to look at while browsing over the internet since individuals can be hurt if there are no confinements on public's access and utilization of individual data. If an unauthorized user gets access to sensitive personal information of a person like medical records, court records, psychological tests and interviews, financial records from bank, sites browsed over the Internet and a variety of different sources of information holds numerous close points of interest of a individual's life. If such data of an individual are leaked, it can leave an individual defenseless against a number of misuses. Consider a scenario where, 'A' has a patent database and is not willing to give the entire information present in the database to various groups, but is willing to allow individuals or groups to browse the database via 'World Wide Web' interface. 'B' has a bright idea which 'B' is thinking to patent and so therefore 'B' first carries out a search for correlated patents. But, the concern is about the fact that if 'B' directs an inquiry on 'A's database 'A' might realize what 'B' is keen on and might reveal the idea of 'B'. Therefore the queries of 'B' as to be maintained such that 'A' does not know what 'B' queries are. Therefore in this particular scenario both personal information and the queries of the user have to be protected. Under certain conditions, breach in sensitive personal information is so serious that the individual may be susceptible to blackmail and coercion by those who have admittance to that data. Therefore, privacy preservation is very important while browsing over the Internet.

Data security can be said as protecting data (Ex: database) from corruption and from undesired actions of unauthorized users. Data security is critical when storing the data in the cloud because if the sensitive data in the cloud falls into the wrong hands like hackers, it can cause a serious threat to the user and the company owning the cloud. Ex: If bank account details fall into the hands of a hacker how dangerous can it be. Therefore for providing data security there are many ways like encrypting the data, authorization, authentication, password protection, backup of data and by using hashing algorithms.

A location-based service (LBS) is an application for an IP enabled mobile devices that requires the where about of the location of the mobile device. LBS are query based and it provides information related to the location of the gadget. Ex: Where are the nearest ATM's? Or it can be any paid information about the particular location. Location server provides the LBS to the user. Therefore it is important to secure the privacy of the user while the user is doing online transactions with a location server and the data in the location server must be provided security so that it is not accessed by unauthorized users.

II. LITERATURE SURVEY

Jaydep Sen[1] has proposed a safe and proficient scanning scheme for shared systems that uses Topology modification by building up an overlay of trusted peers. Here selection of neighbors is done based on their trust ratings and content resemblance. Hannes Federrath et al [2] have proposed a devoted DNS Anonymity Service, that ensures privacy preservation of an user. The outline involves two building hinders: a broadcast plan for conveyance of "top list" of DNS hostnames and low latency mixes for inquiring the hostnames left out without being viewed. Pericle Perazzo, Gianluca Dini [3] have proposed a method called UNILO, an obfuscation operator which offers high guarantee on obscurity consistency, even in situations of erroneous location estimation. Muhammad Aqib and Jonathan Cazalas [4] have proposed caching data technique to resolve the privacy problems where in, it reduces the quantity of queries requested to the location server. Jun Shao et al[5] have proposed a technique called FINE which is a fine-grained privacy preserving location-based service (LBS) framework for cell phones. FINE uses data-as-a-service (DaaS) model. Here LBS supplier sends its data to a third party, who in turn evaluates the users LBS queries. The FINE uses cipher text policy unknown attribute based encryption method to achieve location privacy, access control, access policy and confidentiality of the LBS data and get precise LBS query output without concerning any trusted third party.

Thomas Ristenpart et al [6] have proposed a system called Adeona. It provides good surety of location confidentiality and it has the capability to proficiently find missing devices. Adeona uses OpenDHT as the third party service. Shahriyar Amini et al [7] have proposed a system named as Cache. This system provides location privacy for some classes of location-based applications and helpful location enhanced contents are taken in prior. Applications can get the contents if required from the local cache on the cell phone. This methodology permits the user to utilize the location enhanced content while simply revealing to third-party content providers what geographic range she is in instead of her precise area. Femi Olumofin et al [8] have proposed an entry privacy method and a framework for questioning huge databases. This strategy investigates offline data classification, restraint based query transformations and privacy saving questions to record structures much smaller than the databases. This technique empowers the querying of a large database by statically determining or dynamically describing database portions on keys, possibly with high diversity in their collection of values, thereby minimizing data leakage about the potential data items of interest to users. Marco Gruteser and Dirk Grunwald[9] have introduced a middleware design and algorithms that can be utilized by a federal location broker service. The adaptive algorithms changes the decision of location information along spatial or temporal magnitude so that it meets the exact anonymity limitations based on the individuals who could be using location services inside a particular region. Krishna P. N. Puttaswamy and Ben Y. Zhao[10] have told about Location Based Social Applications (LBSAs). LBSAs have adapted to a methodology where in untrusted third party servers are simply treated has encoded data stores and functionality of the application will be moved to the client's gadget. The area coordinates are encoded, when sharing and can be decoded only by the client to whom the data is proposed. M. Bellare and S. Micali [11] have proposed a client and fair protocol for safe two-party communication in the Optimistic model. Here a partially trusted third party is used but however it's not going to be involved in standard computation of protocol. Third party is necessary just if there exists any interruption in communication or if one of the two parties denies or gets out of hand. This protocol guarantees that regardless of the possibility that one party terminates the protocol at any of the time, the computation is still reasonable for the other party to communicate via asynchronous network.

Chi-yin chow et al [12] have proposed a framework called Casper has been introduced in which a user can obtain LBS without him needing to disclose his private location information. Casper involves two main components- Location anonymiser (trusted third party) and privacy aware query processor. Location anonymiser withholds the precise region information of the client into a cloaked region. The privacy aware query processor is in the location server which tunes the functionality according to cloaked region rather than specific point information. B. Hoh and M. Gruteser[13] have proposed an algorithm called perturbation algorithm. When two users path meet, improbability to the location data of the user is added. This will make it difficult to track a user just using location data.

III. SYSTEM IMPLEMENTATION

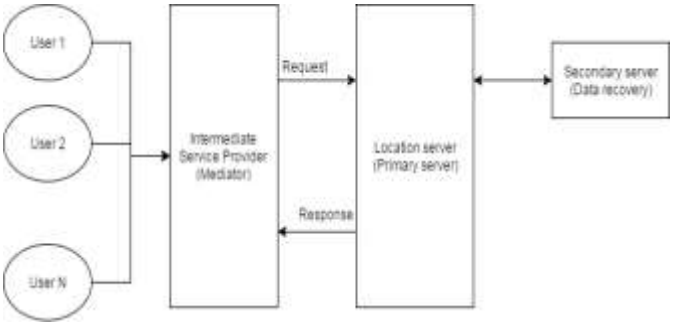

Fig : System Architecture

The implementation of this paper is as follows: There are four components. They are as follows: 1) End Users log in via PC or a mobile 2) Intermediate Service Provider (Trusted third party) 3) A location server.
4) Secondary server

An end user first has to register himself with the Intermediate Service Provider (ISP) so that he can have the benefits of the ISP. After registration, the end user will be given the login credentials which he has to use at the time of login. The ISP's main aim is to protect the individual's privacy and to protect the data of the server that is it gets only the data which the user asks for and none of the other data is revealed to the user.

Location Data upload

The location based data will be uploaded into the location server by the Admin of location server. While uploading the data, it is going to be encrypted and then saved in the location servers. For each data, a Message Authentication Code (MAC) will be generated using SHA-1 algorithm. Then a secret key is going to be generated for the data using RSA algorithm. So therefore, Secret key, MAC and the encrypted data will be stored in the Primary server and the Secondary server. In secondary server, data is stored for data recovery in case if an attacker changes or deletes the data in the primary server. In the server, each block of data will be encrypted using a different secret key.

Location Data Retrieval by End user

After the end user has registered himself with the ISP, the user can access the location server via World Wide Web without their personal details or location details being revealed. When the end user wants to retrieve some information from the server he sends his query regarding the information which he wants to the ISP. ISP then retrieves the information in two stages. They are oblivious transfer phase and Data Retrieval phase (DRP). In the first phase, Oblivious transfer phase the ISP gets the secret key and the cell ID of the queried information from the server and gives the end user, the secret key and the cell ID is not disclosed to the end user. In DRP phase, end user is asked to enter the secret key obtained and then the data will be retrieved by the ISP and provided to the end user. At the time of data retrieval in the servers, the MACs of the data stored in primary server and the secondary server are compared. If both the MACs are same then the data in the server is safe and data will be sent from the primary server to the ISP. And if the MACs are not same then the data in the primary server might be corrupted. So therefore, data from the secondary server will be sent to the ISP and data to the primary server will be recovered. The end user can decrypt the received data only if he has the right secret key.

Data Recovery

Consider a scenario, where in the data in the location server is attacked and the contents are modified. The attacker has modified the contents of the primary server. When the end user asks for the data which is attacked and modified then the following steps take place:

(i) The MACs of the data from the primary server and the secondary server will be compared. Since data in the primary server is attacked MAC of the two data will not be same.
(ii) So, therefore in this situation data from the secondary server will be sent to the user.
(iii) Then regarding the attack admin is going to be notified. And then he recovers the data into primary server from the secondary server.

Intermediate Service Provider

Intermediate Service Provider is the mediator between the user and location server. Here two phases namely oblivious transfer and data retrieval phase undergo. The phases work as follows:

2.4.1 Oblivious Transfer Phase

Oblivious Transfer is a protocol where in two parties are involved. At first the sender has a few information and toward the end of the communication the other party, the recipient finds out about this information in a way where in the sender (server) won't realize what information the recipient learnt. In this implementation, oblivious transfer is used to get one and only one record from the database. In this paper, "K out of N oblivious transfer protocol" is used where in we can retrieve K information from a set of N data available in the database.

This protocol contains two phases. They are as follows:

2.4 ,1.1 Initialization Phase

The initialization phase is controlled by the server who possesses the N information components X_1, X_2….. X_N. Server typically generates an assurance to each of the N data components.

Transfer phase

The transfer phase is utilized to transmit a solitary information component to recipient. At the start of each transfer phase recipient has an input I and output at the end of the phase is the data element X_I. "K out of N oblivious transfer protocol" supports up to k successive transfer phases.

IV. ALGORITHM

Input: Request for key of Data Record based on Location

Output: Obtained Secret key and Cell-ID

Initialization phase

- Applying the query processing through ISP
- Applying the data encryption using AES algorithm

Transfer phase

If query from authorized user

Transmit the key and cell-ID

Else

Terminate the query

4.1 Data Retrieval Phase

With the knowledge of the cell ID and the secret key that encodes the information in the cell the user can start a data retrieval protocol with the location server to obtain the encoded point of interest data.

Therefore, request is sent to the server regarding the retrieval of the data from the cell-ID specified. In response, the server sends the information in the cell to the ISP, which will be then sent to the end user. The end user will be sent an encrypted data which can be decoded using the secret key acquired in the previous phase.

V. CONCLUSION

In this paper, a solution for privacy preservation and data security for the location based services is presented. The user can get the data from the server without revealing his identity to the server and server's data is also secured since only the requested data is sent to the user and none of the other data are revealed. Even if a user gets hold of the data which he is not authorized he won't be able to decrypt it since it requires a secret key. Here an ISP is used to secure the information of an end user. Data security to server data is provided by AES, SHA-1 and Secret key generated for each file.

REFERENCES

[1] Jaydip Sen, "A Secure and User Privacy-Preserving Searching Protocol for Peer-to-Peer Networks" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 1, April 2012.

[2] Karl-Peter Fuchs, Hannes Federrath,, Christopher Piosecny, Dominik Herrmann, "Privacy-Preserving DNS: Analysis of Broadcast, Range Queries and Mix-based Protection Methods" Volume 6879 of the series Lecture Notes in Computer Science pp 665-683.

[3] Gianluca Dini and Pericle Perazzo, "A uniformity-based approach to location privacy" 0140-3664 2015 Published by Elsevier B.V.

[4] Jonathan Cazalas and Muhammad Aqib, "Trusted Base Stations-Based Privacy Preserving Technique in Location-Based Services" Computer and Information Science; Vol. 8, No. 4; 2015 ISSN 1913-8989 E-ISSN 1913-8997 Published by Canadian Center of Science and Education

[5] Xiaodong Lin, Rongxing Lu and Jun Shao, "FINE: A Fine-Grained Privacy-Preserving Location-based Service Framework for Mobile Devices" IEEE INFOCOM 2014 - IEEE Conference on Computer Communications.

[6] Tadayoshi Kohno, Arvind Krishnamurthy, Gabriel Maganis and Thomas Ristenpart, "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs" Proceeding SS'08 Proceedings of the 17th conference on Security symposium Pages 275-290 USENIX Association Berkeley, CA, USA ©2008.

[7] Eran Toch, Jason Hong, Janne Lindqvist, Jialiu Lin and Shahriyar Amini, "Caché: Caching Location-Enhanced Content to Improve User Privacy" Proceeding MobiSys '11 Proceedings of the 9th international conference on Mobile systems, applications, and services Pages 197-210 ACM New York, NY, USA ©2011.

[8] Ian Goldberg and Femi Olumofin, "Preserving Access Privacy Over Large Databases" ACM New York, NY, USA©2011.

[9] Dirk Grunwald and Marco Gruteser, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking" Proceeding MobiSys '03 Proceedings of the 1st international conference on Mobile systems, applications and services Pages 31-42 ACM New York, NY, USA ©2003.