International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Security Safe Guarding Location Data Proximity

Shashikumar T R[1], Anitha K L[2]

[1]Department of MCA, Acharya Institute of Technology, Bengaluru, India
[2]Assistant Professor, Department of MCA, Acharya Institute of Technology, Bengaluru, India

---

Abstract - *In Security Safe guarding location data proximity a user can send request to another user for data transaction between sender and receiver. While communicating between the client and the users in the computation scenario there are various problems arises due to security issues. The safe guarding location data can be protected from harmful threats. In this paper we propose a safe guarding location based queries for the data communication problems. When we are sending request to another user for transaction of data the security safe guarding location data proximity provides a solution by implementing the encryption and decryption process for securing the location data through location based services.*

Key Words: Location based service, Navigational aids, cloud database, Encryption, Decryption.

1. INTRODUCTION

In safe guarding location data proximity, location based services (LBS) incorporates data, diversion and utility administration which is available by cell phones, Global Positioning System (GPS) gadgets, stash, and that works through versatile system. In view of the topographical position of their cell phone, LBS can offer numerous administrations to the client. The administrations dependent on a Point of Interest (POI) database which are given by LBS. By recovering the Points of Interest (POIs) from the database server, the client finds solutions to different area based enquires which incorporate yet are not constrained to - finding the closest or nearest location. In later a long time there has been an immense increment in the quantity of questions for data about POI to the area server from cell phones. In some cases user's may feel hesitant about unveiling their location data to the LBS, since it might be workable for an area server to realize who is making a specific question by connecting these areas with the private telephone directory database, as clients are probably going to perform numerous inquiries from home. Location servers spend their assets for gathering data about different intriguing POIs. Thus, it is normal that the LBS will be not revealing any data without expenses. In this manner, the LBS have to ensure that any unauthorized user is not accessing the location servers. The procedure of transmission the user's ought to not be permitted to find any unpaid data. It is in this manner significant that arrangements ought to be encircled to address the security of the clients issuing enquiries, and avoid clients from getting to the substance to which they don't have any approval.

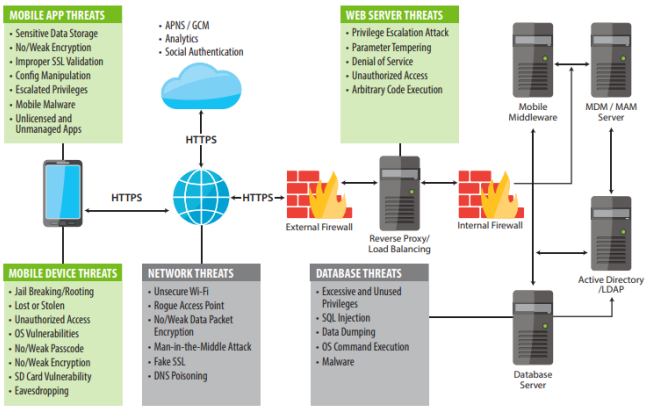

Fig.1 Data secure in Mobile Application

Data security is one of the vital aspects of any organization. Fig.1 shows the threats to data security. In today's digital world, the users are presently relying on multiple devices, such as mobile devices, computers, laptops and other types of tablets to perform significant tasks and to stay connected. Moreover, the users will be having a large amount of personal or business related data on these internet enabled devices wherein the data needs to be kept secured and protected. Proper understanding of the data security threats is a prerequisite to have a secure storage environment. To keep our data safe, it is essential to be aware of the potential threats like mobile app threats, network threats, and database threats and so on.

2. RELATED WORK

If you go through the research records, the first applicable solution to the issue of user location and server address hiding was the Beresford, in which the privacy of user, server is maintained by changing the users address name or location. The characteristic of data being handled and exchanging data in between sender and receiver and instantaneous changing of the user name provides the protection for user's privacy. He also investigates required number of users to satisfy the delinking of property when there are repeated queries over an interval [1].

Another suggested approach to address hiding is the concept of safe guarding location data proximity, which was basically introduced as an efficient technique for hiding and preserving the privacy of user when

releasing sensitive records. This is achieved by using RSA algorithm used for normally ensure that a record could not be tracked, identified and distinguished from other available records. Here the authors provide trusted location based services for the actual location data wherein the location data of a user can't be identified for any other users [2].

An improved trusted approach has also been proposed, which allows the users to set their level of privacy based on value of RSA algorithm. This means if the user feels that the position of data is viable or misused or could be handled maliciously. They have been efforts to make the process naturally by adding the concept of security safe guarding location data proximity services. It is proposed that the users specify a cloaking region that they will protect their privacy [3].

Techniques have additionally been proposed to identify the location data information, which incorporate way and position of the user. Way of location was displayed by Hoh and Gruteser [4]. The vulnerability to the area information of the user's Position of location data has been proposed as a way to deal with the security for safe guarding privacy. The trusted anonymiser is to identify the users as indicated by a location based services this way making it harder for the LBS to recognize a person [5][6]. Another strategy for consoling the address of user is to utilize position of location and data in safe guarding policy. The essential thought is to found the area of user sending numerous arbitrary false areas to the server, to such an extent that the server can't recognize the real area from the location based services. This causes both handling and correspondence overhead for the client gadget, which less effectiveness furthermore, decrease speed of operation [7]. One of the ongoing framework conceived to accomplish protection of users address, is the idea of safe guarding privacy. The basic idea is to confuse the location of the user by sending many random false locations to the server, such that the server cannot distinguish the actual location from the fake locations. For the most part speaking, LBS plans enable a user to recover information (bit or on the other hand hinder) from a database, without revealing the record of the information to be recovered to the database server [8].

Concentrating on the present situation, while verifying data nowadays most associations are center around verifying just the framework holding the information to be verified. They put them behind firewalls and encoded document stores. When the foundation has been avoided any way for example a firewall break or something as straightforward as an approved client replicating the information off the verified area, the data is there for anybody to see [9]. Using data driven security controls for example, verifies the data itself paying little mind to a system or user. In most associations there is an over helming dependence on expert instinct, experience, industry legend and best practices, in spite of the fact that this may enhance the association, they do not enable administration to make steady for educated choices about security [10]. Therefore associations spend nearly nothing or a lot of time and cash in an endeavor to relieve data security dangers. Structures, for example, the Fair hazard the board system intend to give a stage to understanding, examining and estimating security dangers. They propose to protect these dangers in a way that is effectively comprehended to representatives at each dimension.

3. METHODOLOGY

Whenever a user wants to send a request to a server requesting for the data, then there arises various problems related to data privacy, data protection, user location and data security. The protection of the users are identified with user's location and the data may not be secured and this may lead to abusing one's close to home data. In this manner, to stay away from this, there is a need to secure the subtleties of the user who is sending the request.

An answer for one of the location based enquiry issues is proposed, which is utilized for verifying the user's location that can be acquired from Global Positioning System gadgets which finds the location of the user. We implement the system by providing security to the location data which will be communicated in an encrypted format. A symmetric key encryption will be utilized for communication of the user's data and afterwards the information can be retrieved by using a key once it reaches the location server. The framework will be utilized for back and forth correspondence a trade of data among server and user. Additionally, the idea of ideal seeking dependent on the user's conduct and the past seek methodologies will be included. The idea of positioning will be included as extra element. The paper depicts a framework that comprises of an independent programming which will give a decent interface and will be easy to understand and it will break down the active traffic when we are going to utilize intermediary server and will perceive basic data or your own data in the event that it is gotten to by the intermediary in cloud server or not further and after the acknowledgment it will secure our basic information to be gotten to from the illicit sources. The most significant thing is to have an appropriate web association since this proposed framework totally chips away at sending and getting information from user and server. The general framework stream is appeared.

An epic and probabilistic methodology is connected to tackle the issue of user data security. The protection assurance can be kept up by permitting an intermediary server to go about as a moderate between the users and servers. Here all the mentioned information will be send in encoded structure to the intermediary

server. Subsequently, by doing this the subtleties of the user including their location can be effectively identified. Advanced Encryption Standard (AES) calculation is utilized to get the data in the encoded policy with the goal that some other individual can't see the subtleties, from this time forward proficiency will be given. Symmetric key is utilized utmost importance as a similar key is utilized for both encryption and decryption of the data. Utilization of ideal seeking dependent on past questions and client's conduct of a specific enquiry is finished. This calculation has demonstrated more effective than other encryption strategies.

System encryption (some of the time called organize layer, or system level encryption) is a system security process that applies cryptography administrations at the arrange exchange layer - over the information interface level or the application level. The system exchange layers will be layers 3 and 4 of the Open Systems Interconnection (OSI) reference model. Utilizing the current system administrations and application programming, organize encryption is undetectable to the end users and works autonomously of some other encryption forms utilized. Information is scrambled as it were while in travel, existing as plaintext on the starting furthermore, accepting hosts. System encryption is executed through Internet Protocol Security (IPSec), which means that end users and applications don't need to be altered in any way. Encrypted packets appear to be identical to unencrypted packets and are easily routed through Location Based Services.

4. EXISTING SYSTEM

Existing frameworks are used to knowledge safe guarding area information security safeguarding inquiry. However some of them are not intended for POI question. In this sort of arrangements at least one outsider's hand-off messages will be reaching among clients and the specialist organization. This methodology shrouds the linkage between client personalities and messages from the specialist. The enquiry territory would be presented to however the client sending the question is tucked away among a lot of clients.

Territory Based Services have seen irritating security breaks starting late. While there has been much late headway by the investigation organize on making insurance redesigning segments for framework, their appraisal has been normally based on the security guarantees, while the theme of whether these instruments can be grasped by helpful applications has gotten limited thought. This framework considers the suitability of Security safe-guarding area nearness shows in the setting of flexible applications.

5. PROPOSED MODEL

Security safe guarding location data proximity is a web based application for communication of data between users and clients through network point of interest. The development of mobile application for data proximity is ability of users to identify own location and users to find their information services in cloud data security. A location based services providing information and utility services which are accessible like mobile devices and Global Positioning System devices, Pocket personnel computers and also using network devices.

In this security safe guarding location data proximity is using cloud for database and purposes of using this is mainly for user's data protection as well as LBS data security. We can store the data they are converted plain text to cipher text in safe guarding data proximity.

6. ANALYSIS SURVEY

In this framework we include a few area based administrations it is an incredible application for portable data administrations. A location based administrations give a few offers give to clients to topographical position of their versatile safe guarding application. The block diagram is shown in Fig.2.

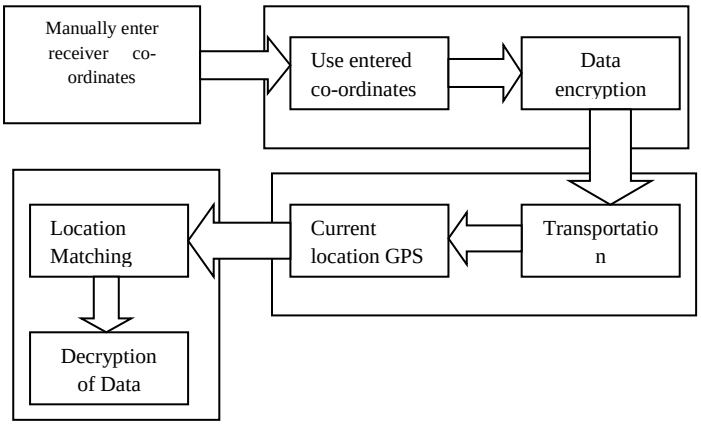

Fig.2 block diagram

6.1 Location Based Services (LBS):

Location based services (LBS) is a killer application in versatile data administrations with the fast advancement in remote correspondence and site situating innovations. Users with area mindful cell phones will scrutinize their surroundings wherever and whenever. In any case, however this present registering world view brings extraordinary accommodation for information get to, the noteworthy of client areas to support providers raises a need of interruption on area security that has hampered the across the board utilization of LBS. In this way, an approach to extract LBS with conservation of data

security has been increasing expanding investigation consideration as of late. Inside the writing, there are a unit mostly 2 classes of ways to deal with safeguard area protection for LBS the essential is through information get to the executives. User's areas region unit sent to the administration providers was normal. It relies upon the administration providers to constrain access to keep area data through guideline based polices. The second is to utilize a dependable middleware running between the users and administration providers. A client will determine for each area based inquiry the security request with a base spatial space needs to find the location. This data would be without a doubt supportive if the telephone's physical area data turns into extra dependable. It may yield a gadget's area to be known once its GPS setting is killed physically.

6.2 ENCRYPTION PROCESS

We can use encryption to protect data from being accessed by unauthorized users. The encryption process is shown in Fig.3. The data encryption system is a block of cipher text which is designed by transaction of data for encryption and decryption process. In encryption process the data blocks consisting 64 bits using 64 bit key. Although the data encryption process input key is used for 64 bits long, the actual data encryption standard is using only for 56 bits length. The least critical in every bit is an equality bit, so that there are dependable an odd number of 1s in each byte. These equality bits are ignored, so just the seven most significant bits of each byte are utilized, bringing about a key length of 56 bits. The algorithm experiences 16 cycles that join squares of plaintext with qualities got from the key. The algorithm changes 64-bit contribution to a progression of ventures into a 64-bit output. Similar steps, with the same key are utilized for decryption. There are numerous assaults and strategies recorded till now those endeavor the shortcomings of , which made in secure the block of cipher text. Regardless of the developing worries about its powerlessness, DES is still generally utilized by financial services and other industries worldwide to protect sensitive on-line applications.

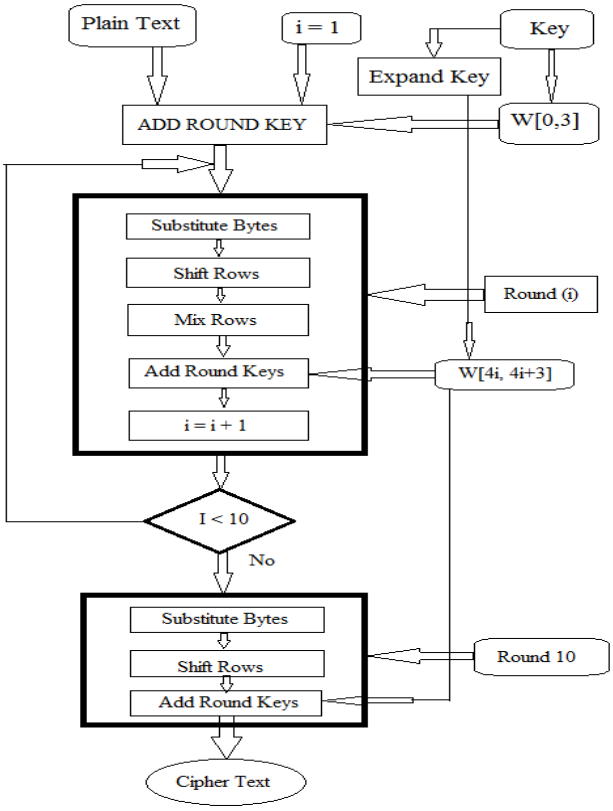

Fig. 3 Encryption process

6.3 IMPLEMENTATION OF ENCRYPTION PROCESS

In security safe guarding location data we are implementing encryption process procedure to follow for hiding the users address and to perform the data transformation.

- The start step when user sends the request to another user.
- This encrypted data are stored in the proxy server or cloud database.
- The proxy server sends the location and data information to the server
- The encrypted data is then decrypted based on server side.
- The server then reply back to required results through the encryption process.
- The data is communicated before first using the encryption process.
- The encrypted data is send back to proxy server.

- Decryption of data or information can perform so that user can receive the data.

We developed the security safe guarding location data proximity by using the tools and technologies like Android, Angular Js, JavaScript, and PHP (Hypertext

Preprocessor). This mobile application is for secure the location data in safe guard policy.

Fig. 4 Login page

Fig. 5 Registration page

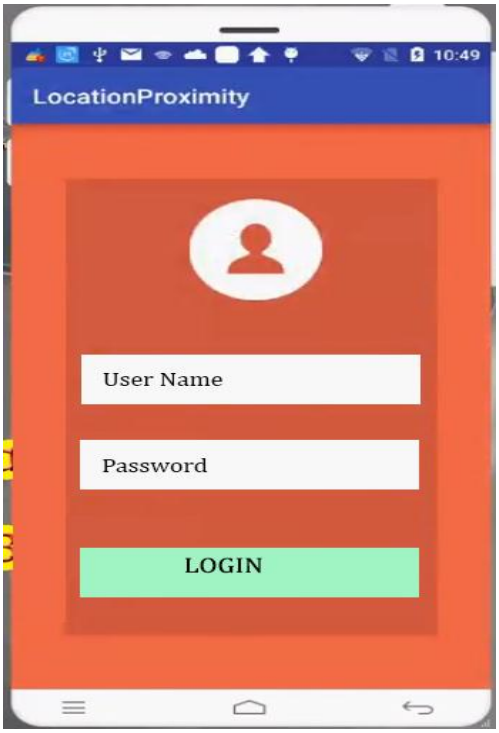

Fig. 6 Login-Details

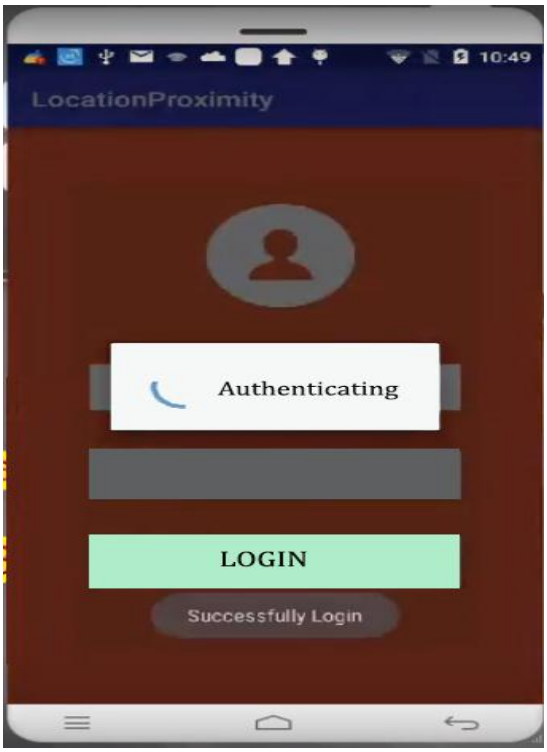

Fig. 7 Login Authentication

Fig. 8 Secret-key

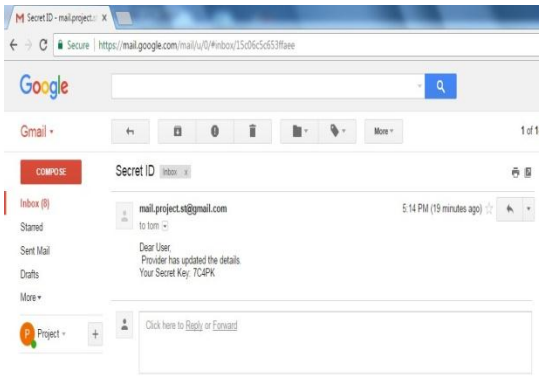

Fig. 9 Secret-key via mail

6.4 DECRYPTION PROCESS

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data manually or unencrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption secret code or key is not available may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

7. ALGORITHM

RSA [Rivest-shamir-adleman] algorithm in cryptography [11]: RSA algorithm is asymmetric cryptography algorithm. Asymmetric is actually it means that it works two different keys are used one is private key and public key. As the name indicates public key is used to everyone and private key is used to private.

RSA algorithm for key generation

- Input: none
- Computation:
  - Select two prime integer's p, q
  - Compute integers n = p ×q
  v = (p-1) ×(q-1)
  - Select small odd integer k such that
  Gcd (k, v) = 1
  - Compute integer d such that
  (d×k)%v= 1

RSA algorithm for encryption

- Input: integers k, n, M
  - M is integer representation of
  Plain text message
- Computation:
  - Let C be integer representation of
  Cipher text C = (Mk) %n
  -Cipher text or encrypted message

RSA algorithm for decryption

- Input: integers d, n, C
  - C is integer representation of cipher
  Text message
- Computation:
  - Let D be integer representation of
  Decrypted cipher text D = (Cod) %n
  - Decrypted message

8. CONCLUSIONS

The outcomes detailed in this paper conclude that the security frameworks appointed on cloud framework are more efficient than working them on single processor framework. For both local and cloud condition, encryption process is the more time consuming than decryption process. But it is seen that Accelerate Ratio is acquired in encryption for low input document sizes furthermore, the Speed-Up Ratio falls forcefully as the info record measure is expanded. Data encryption in algorithm consumes least encryption time in RSA algorithm has less memory use while encryption time contrast is exceptionally minor if there should be an occurrence of encryption and decryption process in algorithm. In safe guarding policy, it tends to be seen that higher key size prompts clear change

in the safe guarding data and location. Computation time for encryption and decryption in various position data demonstrates that RSA algorithm is executed in lesser time consumption in security safe guarding policy.

REFERENCES

[1] Behrouz A Frozen, "Data Communications and Networking", McGraw-Hill, 4th Edition.

[2] S.B. Gosavi, Dr.SV.Gumaste, "Location based Queries for Content protecting and Privacy preserving," International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, July 2015

[3] L. Sweeney, "k-Anonymity: A model for protecting privacy,"Int.J.Uncertain.Fuzziness Knowledge. Based Syst., vol. 10, no. 5, pp. 557–570, Oct. 2002.

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

[5] S. Mascetti and C. Bettina, "A comparison of spatial generalization algorithms for lbs privacy preservation," in Proc. Int. Mobile Data Manage., Mannheim, Germany, 2007, pp. 258–262.

[6] B. Hoh and M. Gutsier, "Protecting location privacy through path confusion," in Proc. 1st Int. Conf. Secure Comm., 2005, pp. 194–205.

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

[8] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in Proc. 3rd Int. Conf. Pervasive Compute., H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468.

[9] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers

12. BIOGRAPHIES

Shashikumar TR is a student in the Department of Master of Computer Application from Acharya Institute of Technology Bangalore, India. His area of interest Data security in cloud database and Networking's.

Anitha K L is an assistant professor Dept of MCA in Acharya Institute of Technology Bangalore, India Her research interests include cloud computing security, networking and distributed computing, cloud data storage.