Security to Mobile banking using Location based Encryption

[1]Apurva Deshpande, [2]Manisha Jagtap, [3]Supriya Kadam, [4]Ashwini Chechare, [5]Pallavi Dhade

Department of Computer Engineering, Savitribai Phule Pune University, Pune-India

***Abstract*— We are developing banking application using Location Based Encryption. As compare to current banking application which are location-independent, we are developing banking application which is location dependent. It means in Cryptography Cipher-text can only be decrypted at a specified location i.e. location-dependent approach. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. This is important in real time application ,example in military base application ,cinema theater. But our system is flexible enough to provide access to customer to his/her account from any location. Our system also provide solution to physical attack using virtualization ,in which customer is allowed to perform fake transaction for his/her physical security purpose.**

***Keywords*- accurate GPS ,Cryptography, Geo-Encryption, Location Based, Security.**

I. Introduction

We are developing banking application using **Location Based Encryption.** As compare to current banking application which are location-independent, we are developing banking application which is location dependent. It means in Cryptography Cipher-text can only be decrypted at a specified location i.e. location-dependent approach. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. This is important in real time application, example in military base application, cinema theater. But our system is flexible enough to provide access to customer to his/her account from any location. Our system also provide solution to physical attack using virtualization ,in which customer is allowed to perform fake transaction for his/her physical security purpose.

Security has always been an integral part of human life. People have been looking for physical and financial security. With the advancement of human knowledge and getting into the new era the need of information security were added to human security concerns. Data is encrypted only when person is having private key can decrypt it. In cryptography **“identity”** component is important ,we can specify name, address, id as identity, but we can also give place (i.e. Physical presence at a particular location) as identity. This place can be used in encryption.

We trust physical security more. Those are inside (part of) particular geographical area are approved for data decryption otherwise not allowed. Another use of “Location Based Cryptography” is access control.(ex-accessing printer in a room but cannot access outside of room.)

II.Block Diagram

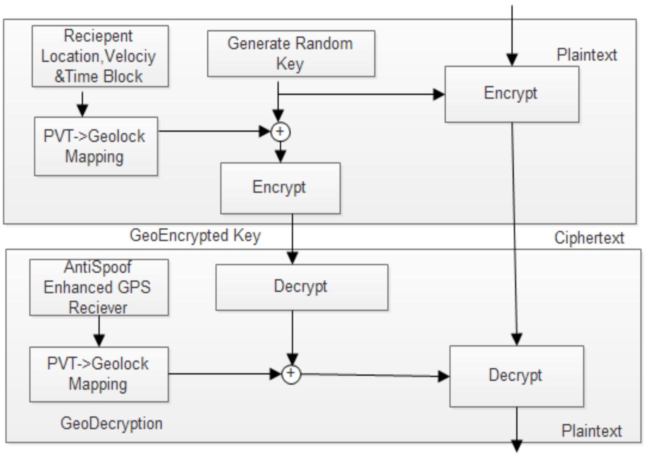


Figure 1.Loaction Based Encrption Scheme

Fig.1 Basic Model Geo-encryption-decryption Process

Figure 1 shows the block diagram of the system. Geo-Encryption used to encode files related to films in the manufacturer studios and send them to the cinema theaters through a wide network like the Internet. The sent files could be downloaded in all the areas which were covered. But they could be decrypted only on the location of the considered cinema theater at a specific time. The geographical information of the cinema theater must be matched with the information used in the sender's file. As we know, using symmetric encryption (private key) in terms of computational and implementation is very fast. Asymmetric encryption (public key) method uses both the public and private keys and its security is very high. On the other hand due to the difficulty in computing its performing rate is low. Therefore in the “Geo-Encryption” algorithm a combination of symmetric and asymmetric encryption is used .The public key algorithm is used to secure and distribute session keys and the symmetric encryption algorithm is used to encrypt the information . The sender uses the session key (which is random) and a symmetric algorithm like “AES”to encrypt the desired data. Then using location information,time and speed of receiver (PVT) and a mapping table makes a certain code named “Geolock”. Last the session key is encrypted by the certain code (Geolock) and by using an algorithm such as “RSA” the results are encrypted and sent.

The receiver using their PVT information obtained via positioning tools (Anti-spoof GPS) and the mapping table, calculates the Geolock +and then:

Geolock + encrypted key = Session key.

III.LDEA PROCESS

The purpose of LDEA is mainly to include latitude/longitude coordinate in the data encryption to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver.

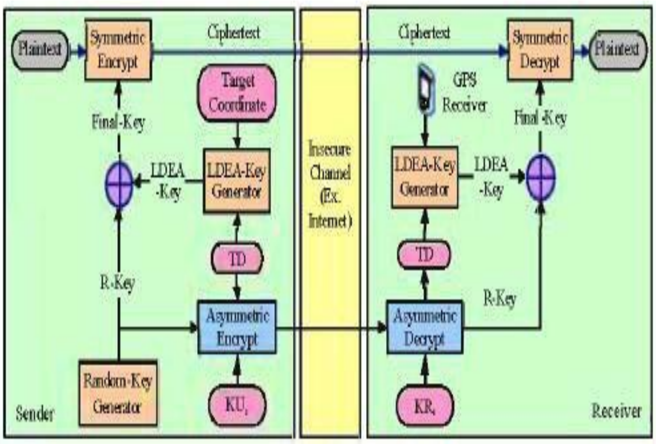


Fig 2: LDEA process

the mobile clients transmits a target latitude/longitude coordinate and an LDEA key is obtained for data encryption to information server. The client can only decrypt the ciphertext when the coordinate acquired from GPS receiver matches with the target coordinate. They makes the use of random key (R-key) an addition to the LDEA key to improve security. LDEA protocol makes the use of static location. It is difficult for a receiver to decrypt the cipher text at the same location which is exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as a key for data encryption. So, a protocol which makes the use of dynamic location of mobile node and dynamic tolerance distance which makes it very strong to attack. In this protocol, the mobile receiver with GPS service, register a set of coordinates and velocity during movement and estimate the next position. This new coordinate is applied in the secret key with dynamic tolerance distance (DTD). DTD is designed to overcome the inaccuracy and inconsistent problem of GPS receiver and to increase its practicality. These parameters and the type of movement makes this protocol more secure than the static encryption which depends only on a position of mobile nodes and static TD. However most of them are not strong enough to tampering. By tampering, deals with both physical attacks on the hardware and attacks on the implementation such as spoofing. If the device is vulnerable to tampering, it may be possible to for an adversary to modify and bypass the location check . If there is an unauthorized tamper access, or attacker sent a faked message, the system assumes a tampering is being attempted and ignores the message and process will be failed. Thus the messages really sent from the sender will distinct from the fake messages and then only these messages will be decode. To protect against tampering and spoofing, a signal authentication protocol.

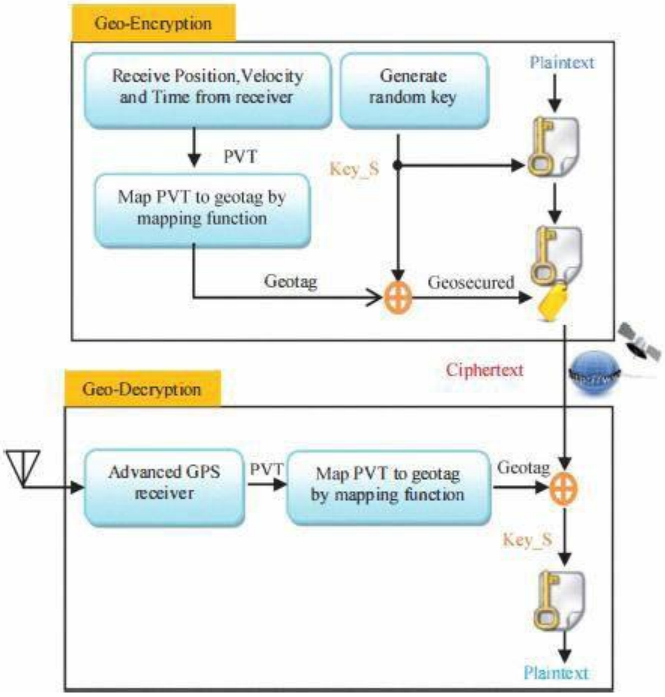
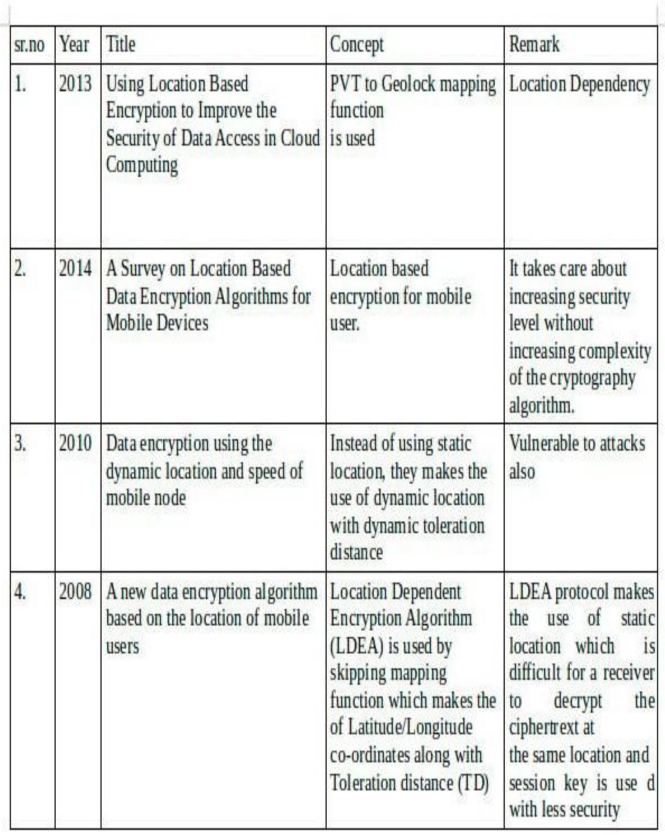


Fig 3:Geo encryption model

Instead of using PVT geo-lock mapping table in fig[1], we are using LDEA algorithm to provide mobility . As we providing this application for mobile users. Use of mapping table is for static location our model is on mobility hence we are using LDEA algorithm. Attackers cannot simulate signals or use any mean to spoof the GPS receiver because they don't have the key used to generate authenticated messages. Therefore, if there is an unauthorized tamper access, or attacker sent a faked message, the system assumes a tampering is being attempted and ignores the message and process will be failed. Thus the messages really sent from the sender will distinct from the fake messages and then only these messages will be decode. In this paper, they designed a framework to safeguard users location information as well as the check in record by considering demands in LBSNs. LBSN is is location based social network system in which users expose their location when they check in at a venue or search a place. There are so many encryption methods which converts the information before sending on communication link. Each of these encryption methods has their own merits and demerits. A smooth comparison of various encryption algorithms and their techniques for secured data communication in multi node Named-Based-Encryption which provides great security level with lesser time complexity . This technique is the combination of stream ciphering and symmetric ciphering. This proposed encryption algorithm work's by user defined dynamic key and ASCII value of the secrete key. Dynamic

IV.LITERATURE SURVEY



sr.no	Year	Title	Concept	Remark
1.	2013	Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing	PVT to Geolock mapping function is used	Location Dependency
2.	2014	A Survey on Location Based Data Encryption Algorithms for Mobile Devices	Location based encryption for mobile user.	It takes care about increasing security level without increasing complexity of the cryptography algorithm.
3.	2010	Data encryption using the dynamic location and speed of mobile node	Instead of using static location, they makes the use of dynamic location with dynamic toleration distance	Vulnerable to attacks also
4.	2008	A new data encryption algorithm based on the location of mobile users	Location Dependent Encryption Algorithm (LDEA) is used by skipping mapping function which makes the of Latitude/Longitude co-ordinates along with Toleration distance (TD)	LDEA protocol makes the use of static location which is difficult for a receiver to decrypt the ciphertext at the same location and session key is use d with less security

V.RELATED WORK

Meer soheil [1] developed the idea of geoencryption in which PVT-to-Geolock mapping function is used as a primary mechanism to ensure that the data can be decrypted successfully. It is troublesome for sender and receiver to own the same mapping function before the data transmission if they communicate occasionally.

Hsien-Chou Liao and Yun-Hsiang Chao[2] They design theLDEA by skipping the mapping function. The purpose of LDEA is mainly to include latitude/longitude coordinate in the data encryption to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver.

LDEA protocol makes the use of static location.It is difficult for a receiver to decrypt the cipher text at the same location which is exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as a key for data encryption.

Hatem Hamad and Souhir Elkourd [3] ,proposed a protocol which makes the use of dynamic location of mobile node and dynamic tolerance distance which makes it very strong to attack. In this protocol, the mobile receiver with GPS service, register a set of coordinates and velocity during movement and estimate the next position. This new coordinate is applied in the secret key with dynamic tolerance distance (DTD). DTD is designed to overcome the inaccuracy and inconsistent problem of GPS receiver and to increase its practicality. These parameters and the type of movement makes this protocol more secure than the static encryption which depends only on a position of mobile nodes and static TD.

VI.PROPOSED SYSTEM

Users (individuals or companies) are concerned about the access to the information by unauthorized users. Now suppose that data is some critical and confidential information from a bank, or a company and etc. Certainly the necessity of access control in the cloud computing is more than ever and is a very important part of data security in cloud.

In our method we use the user's location and geographical position and we will add a security layer to the existing security measures. Our solution is more appropriate for banks, big companies, institutions and examples like this. The only thing we need is an Anti-Spoof and accurate GPS that companies can afford to buy. Also implementing the Geo-Encryption algorithm on the cloud and the user's computer (which is connected to the GPS) is required. We can label the data. Label contains name of the company or a person who works in the company (for example the company's boss). These labels are placed in an index table that refer to the user's geographic location and the time frame considered to access data, in a database. These labels and values of the database can be added manually or automatically. For example, suppose that a bank stores some information in the cloud and only the accountant can have access to it. The new generation “Anti-Spoof” GPS is very accurate and can give us the latitude, longitude and altitude accurately. As a result we can limit the data access to the room located on a particular floor of a building and a specified time frame.

We are providing solution to physical attack. There might be situation in which victim will be suffering from forceful attack . In that situation victim should enter an extra key along with password. There will be successful login but virtual .And the forceful attack will be indentified at server side.

VII.SOCIAL CAUSE

Banking application is always helpful for normal user. In which security is provided using location as identity. It also provide solution to physical attack using, virtualization,which allows user to perform fake transaction.

VIII.CONCLUSION

Hence we are implementing new security level to existing security measures, using location based encryption. We also provide solution to physical attack. One of the most challenging issues in cloud computing is data access control. Because of the benefits of the cloud computing more people and more companies turn to this technology every day. Like almost every proposed procedure, there are challenges as well as the advantages present in this technology. In this paper, cloud security and its challenges are briefly discussed. Location based encryption and “Geo-Encryption” algorithm were also reviewed. Finally a new security level was added to the existing security measures using location-based encryption. This method can be used in several places such as banks, big companies, institutions and have the desired performance.

This mobile banking application will allow users to move/migrate to another location n still they can access their account. Location is a major constraint which is used in encryption and decryption process. It also makes use of Anti-spoof GPS to measure accurate location using latitude and longitude.

IX.FUTURE SCOPE

The person performing transaction should be stable at various different locations .But in future we can provide application in which person will be travelling.

X. ACKNOWLEDGMENT

We would like to thank our project guide Prof. Pallavi Dhade for her enormous co-operation and guidance. We have no words to express our gratitude for a person who whole heartedly supported the project and gave freely of her valuable time while making this project. The technical guidance provided by her was more than useful and made the project successful. We would also like to thank our Department of Computer Engineering, Pimpri Chinchwad College of Engineering.

XI. REFERENCES

[1] Meer soheil ,"Using location based Encryption to improve the security of data access in cloud computing",2013

[2] Hsien-Chou Liao and Yun-Hsiang Chao,"A new data encryption algorithm based on the location of mobile users",2008

[3] Hatem Hamad and Souhir Elkourd* ,"Data encryption using the dynamic location and speed of mobile node",2010

[4] Manisha S Manindraker,"A Survey on Location Based Data Fig. 3 Solution to physical attack Encryption Algorithms for Mobile Devices",2014

[5]]. Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson,"Geoencryption using Loran".

[6] A. Perrig, R. Canetti, J.D. Tygar, D. Song, "The TESLA Broadcast Authentication Protocol", 2002, pp. 2-13

[7]]. Di Qiu, Sherman Lo, Per Enge, Dan Boneh and Ben Peterson, " Geoencryption system security-Loran as a case study".

[8] Ayesha Khan, "Geolocation Based RSA encryption Techniques", ISSN, 2013, pp. 17-20.

[9] Rohollah karimi and Mohammad kalantari, "Enhancing security and confidentiality in location based data encryption algiritms", IEEE Conference, pp. 30-35, 2011.

[10] V Rajeswari, V Murali and A.V.S. Anil, "A naval approach to identify Geo-Encryption with GPS and Diffrent Parameteers (Location and Time)", IJCSIT, pp. 4917-4919, 2012.