"Geo-Encryption Lite" - A location based Encryption Application for Android

Smita Chaudhari
Assistant Professor,
Department of Computer Engg.
SPPU, pune, India

Ashish Jha
Student,
Department of Computer Engg.
SPPU, pune, India

Samadhan Yangad
Student,
Department of Computer Engg.
SPPU, pune, India

Ashish Surwase
Student,
Department of Computer Engg.
SPPU, pune, India

ABSTRACT
In today's world mobile communication has become part and parcel of our daily life. It's hard to imagine today life without the service and application that are provided by the mobile device. These services and applications are basically wireless based and there is always need of secure communication or some kind of channel. Encryption is one way of providing secure communication but most of the existing data encryption techniques are location independent. And here comes the concept of "Geo-Encryption" or "Location-Based encryption". It provides an additional layer of security beyond that provided by conventional cryptography. It allows the encryption of data as well as decryption for a specific location(s) or specific area(s) e.g. college campus area or in a particular building. Constraints in time as well as velocity can also be added with respect to the location while encryption. Geo-encryption can be used with both fixed and mobile application and supports wide range of data sharing and distribution policy.

Keywords
Cryptography, Geo-Encryption, Location based encryption, Mobile Communications, Mobile Applications, Android Operating System

1. INTRODUCTION
Mobile phones are considered as a necessity nowadays. It's a powerful form of communication. It represents functionality and style in one small package. Billions of people worldwide are now owners of cell phones. Mobile phones have become a near-ubiquitous tool for information-seeking and communication, thereby increasing the frequency of data transmissions among mobile users. Having such a great popularity in data transmission as well as communication has also called upon the need of data security. Secure exchange of information is possible only through encryption. So, for secure communication the concept of "Geo-Encryption" is introduced which is location dependent. It is an enhancement to traditional encryption that makes use of physical location or time as a mean to produce additional security and security features [9]. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as location. If someone attempts to decrypt the data at some other location, the decryption process fails and reveals no details regarding original plaintext information.

The Geo-Encryption algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. The capability has tremendous potential benefits to applications such as location based services, managing secure data and digital movie distribution where controlling access is the main concern. Location information has many properties good for encryption and authentication [10]. Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system. Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, at a particular theatre, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location.

2. RELATED WORK
The continual search in developing the better encryption strategies has led to the emergence of new encryption techniques inspired by some previous efforts for surveying the characteristics, application and drawbacks of such an area. In this subsection discussion about one of such improved way of encryption and decryption strategy.

The objective of [1] is to make integrate location into the previously established cryptographic algorithm in a way that it does not diminish their security while meeting other objectives. This approach is referred to as "Geo-encryption".

In this method ,the sender encrypts the data according to the expected PVT(position, velocity and time)of the receiver .The PVT block defines where the recipient needs to be seen terms of position ,velocity and time for decryption to be successful. A PVT to Geo-lock mapping function is used to get the Geo- lock key. A bitwise Exclusive-OR is performed between Geo- lock key and randomly generated key to get a Geo-lock session key. This session key is then encrypted using an asymmetric algorithm and is shared with the receiver. For the receiver, an anti-spoof GPS receiver is used to acquire the PVT data. Then, the same PVT to Geo-lock mapping is used to get the Geo-lock key. The key performs Exclusive-OR option with the received Geo-lock key to get the final session key. If the PVT values matches with the PVT values provided by the sender then the final session key would be correct and then the cipher text would be decrypted.

In above method, there is a constraint that the both sender and receiver must own the same PVT-To-Geolock mapping function. This constraint is removed in [6] which focus on the design of Location-dependent Data Encryption Algorithm (LDEA), by skipping such mapping function.

A target latitude/longitude coordinate is determined firstly. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with the target coordinates. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver .The Target coordinate and TD (toleration distance) is provided by the sender to generate the LDEA key, there is randomly key generator which issues a session key, called R-key Which is then Exclusive-ORed with LDEA key to generate the final key for encrypting the plain text. There is no restriction over the use of encryption algorithm DES, AES or Triple DES etc. can be used to encrypt the plaintext by the given final key, TD and R-KEY is transmitted to the receiver via asymmetric encryption algorithm. As soon as the receiver gets the access of TD and R-KEY , the LDEA key can be generated (at the receiver end) by exclusive OR R-KEY with LDEA key. If the acquired coordinates is matched with the target coordinate within the range of TD, the cipher text can be decrypted back to the original plain text, otherwise meaningless and indiscriminate result is displayed. The target coordinate is either determined by the sender or receiver. It must be communicated between the other party/parties via very secure communication.

Hsien-Chou Liao and Yun-Hsiang Chao[2] introduced a location dependent approach called Location Dependent data Encryption Algorithm (LDEA) This protocol is not strong enough because they are using the static location which is latitude/longitude coordinates of mobile node and they are using the static tolerance distance to overcome the inaccuracy and inconsistent of GPS receiver. 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 difficult to attack. However most of them are not strong enough against tampering. If the device is vulnerable to tampering, it may be possible to an advisory to modify it and bypass the location check. To protect against tampering and spoofing, a signal authentication protocol, Timed Efficient Stream Loss-tolerant Authentication (TESLA) [8] is designed .Since then many efforts have been done to complete the above idea and fix its defects. To Overcome these defects, Rohollah karimi and Mohammad Kalantari [4] present a modified Geo protocol and improve its efficiency and applicability. Although it is possible to provide security features such as authentication, integrity and confidentiality. What is secure today may not be secure tomorrow. There will always be malicious users trying to exploit and find new holes in a network. Therefore, there is a need to look into the future so that we are able to face these security issues before they cause damage.

In [5] a location-dependent approach is proposed for mobile information system. This approach can meet the confidentiality, authentication, simplicity, and practicability of security issues. An information system which provides services for mobile clients is called mobile information system. Data encryption techniques are used for ensuring the data transmission security between information server and mobile clients. The mobile client transmits a target latitude/longitude coordinate for data encryption to information server. Then, the server encrypts the message and sends the cipher-text back to the mobile client. The client can only decrypt the cipher-text when the coordinate acquired form GPS receiver matches with the target coordinate. The process of communication is divided into register phase and operation phase. Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information system in the future, a location-dependent data encryption is proposed in this paper. The approach provides a novel function by using the latitude/longitude coordinate as the key of data encryption.

3. PROPOSED SYSTEM

Geo-encryption is an enhancement to traditional encryption that makes use of location or time as a mean to produce additional security and security features. It limits the access (decryption) of information content to specified location & time. The algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. Any attempts to secure information at an unauthorized location will result in a failure of the decryption process. This paper tries to present a modified Geo protocol and improve its efficiency and applicability. The idea of location based encryption can be implemented as an android app. The app is used by two users, the sender and the receiver to transfer data securely between them. The message to be send is encrypted into cipher text by the sender and it is decrypted at the receiver side to get the plain text. Receiver side decrypt the cipher text when he is at the specified location. The components of proposed system are as shown in Fig.1

3.1 Login and Registration

In this module user first register in to the app by giving their simple personal details like username, password, email id etc. and by using the username and password the user login in to the application. In this module database is used to store the registered user details. To create the Database MySQL is used. MySQL is a relational database management system contained in a small C programming library. In contrast to other database management systems, MySQL is not a separate process that is accessed from the client application, but an integral part of it. MySQL is a popular choice as embedded database for local/client storage in application software such as web browsers.

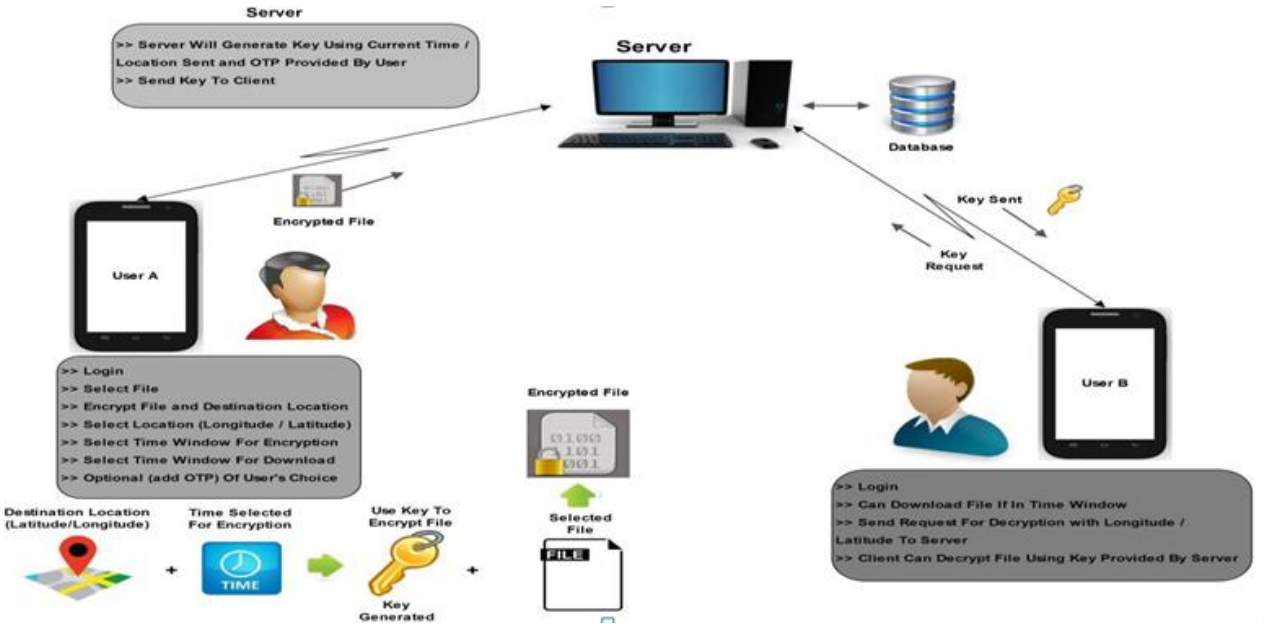

Fig 1: Architecture Diagram

3.2 Location Retrieval

In this module the latitude and longitude of the user is getting from the device by using either GPS or by using PROVIDER (Location manager is the class used to get the location in android). In android by using these steps the user location is located.

1. Start application.
2. Sometimes later, start listening for updates from desired location providers.
3. Maintain a "current best estimate" of location by filtering out new, but less accurate fixes.
4. Stop listening for location updates.
5. Take advantage of the last best location estimate.

Two providers are used in android to get the user location, GPS provider & NETWORK provider. GPS provider determines the location using satellites. Depending on conditions, this provider may take a while to return a location fix. The GPS provider will only work correctly and more efficiently in places where we can see the sky. It requires either of one permission, ACCESS_COARSE_LOCATION or ACCESS_FINE_ LOCATION. By using this latitude and longitude can be obtained, geo coordinates of the user's location. This geo-coordinate can be converted in to location by using geo-coding. Geo- coding is the conversion of geo-coordinates in to the place name.

3.3 File Upload and Encryption

In this module, file is picked by clicking on button "Pick File". Then the sender selects the recipient name from the drop down list .The sender generates a random key that has to be communicated to receiver in order to decrypt the message. After clicking the "Generate key "button a pop-up menu appears that asks user to select time, date and location for decryption. The "Upload to Server" button uploads the file on server in encrypted format. AES encryption is used for encryption purpose. The encryption process uses a set of specially derived keys called combined keys. Combined Key is made up of AES key and Location & Time Parameter Key. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array is called the state array. After successful upload of file on server a toast gets displayed enumerating "success".

3.4 File Download and Decryption

After login, user checks if there is any file to download by clicking "To download list". It displays list of files to download. The user selects the file name and download the file on his/her drive. Though the file is downloaded it is still in encrypted format. The user is asked to supply the random key as given by the sender and if user is present at the intended location and the time is intended for decryption then and only then the file will be decrypted else not. The decrypted file is saved in his/her drive in Decrypt Folder.

4. IMPLEMENTATION

This app is implemented using Android Operating system. Android provides access to a wide range of useful libraries and tools that can be used to build rich applications. For example, Android enables developers to obtain the location of the device, and allows devices to communicate with one another enabling rich peer–to–peer social applications. To get the location parameters, GPS system is used. It is a radio navigation system that allows land, sea, and airborne users to determine their exact location, velocity, and time 24 hours a day, in all weather conditions, anywhere in the world.

User first registers in the app by giving their simple personal details like user id, password, name, address, email etc. All the details entered get checked with the database entries. If match found then user gets allowed to use the app and "Upload Form "gets displayed else login failed. In the "Upload Form" as shown in Fig.2 (a) file is picked by clicking on button "Pick File". Then the sender selects the recipient name from the drop down list .The sender generates random key that has to be communicated to receiver in order to decrypt the message. After clicking the "Generate key "button a pop-up menu appears that asks user to select time, date and

location for decryption. Fig.2 (b) shows a Pop-up Alert Dialog Box which consists of Time-Picker, Date-Picker, Calendar and List consisting of locations. Using this sender defines the location, time and date parameter to decrypt the message.

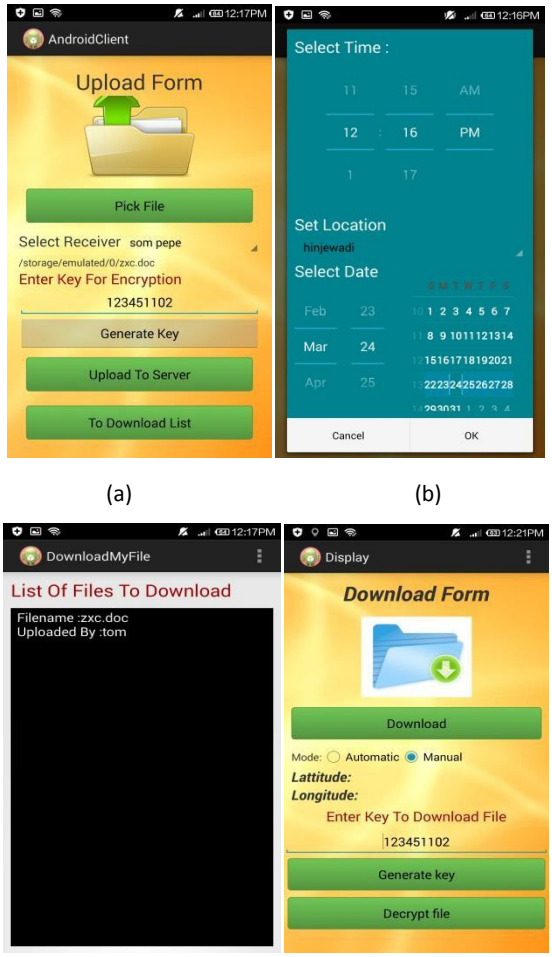

Fig. 2 Snapshots of Geo-Encryption App

Fig.2 (c) shows the list of files ready to be downloaded by the receiver. It shows various files in a list view detailing the filename and the sender name. For downloading, the receiver has to click on the filename. The receiver can download the file by simply clicking the Download button. However the downloaded file will still be in encrypted form. In Fig.2 (d) receiver enters the key as given by sender and if the receiver is present at the intended location of decryption then and then only file will decrypt otherwise not.

5. APPLICATIONS

Traditional Encryption Systems cannot restrict the location of mobile clients for decryption. Thus to enhance the security feature and to meet the needs of the advancement in security system in nearby future, a modified system is proposed in this paper. Geo-Encryption provides strong protection against location spoofing, location secrecy and mobility. It can be used to employ in banking applications where data such as account details need to be secure and details should be open at only bank location. Also confidential data sharing between business firms can be accomplished.

It has also application in military where the location to which one wants to decrypt, may be the location of a submarine or concealed military forces, or the location of a target where a weapon will activate following decryption. Even if the application itself does not require location secrecy, keeping the decrypt location secret can help protect against spoofing. Adding further, if military forces move through a region, message sent to their communication devices could be enciphered to their current location. If devices fall to enemy hands, they will be useless as the forces will have moved on and it can be only deciphered at that location only. Furthermore, if decryption is restricted to a brief period of time, the enemy would be unable to decrypt any previously intercepted message even at the current location, as the time would no longer be current. Another application could be in digital film distributions [7]. "*Today, the film studios spend over $1 billion each year to duplicate, distribute, rejuvenate, redistribute and ultimately destroy the thousands of film reels required to bring the close to 500 films released each year to audiences across the U.S.*" Geoencryption would provide a very efficient and cost effective digital cinema distribution model, but piracy is a major concern.

6. CONCLUSION

Location based encryption enhances security by integrating position and time into encryption and decryption processes. The described geo-encryption approach builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific location(s) or for specific area(s), e.g. a corporation's campus area. Constraints in time as well as location can also be enforced. Geo-encryption can be used with both fixed and mobile applications and supports a wide range of data sharing and distribution policies.

In summary, geo-encryption offers the possibility of enhanced security through location constraints. It may be particularly attractive for defence applications and applications that would be undermined by compromises on a grand scale, such as in the movie industry. This preliminary analysis is intended to stimulate further research on location-based methods, including a deeper analysis of security issues. There seems to be quite a great potential in providing security at many levels in Geo-Encryption. Velocity can be added in integration with location and time as an additional parameter while encryption and decryption.

7. REFERENCES

[1] Logan Scott, Dorothy Denning, "A Location Based Encryption Techniques and some its Application", ION NTM, pp. 734-740, 2003..

[2] Hsien-Chou Liao and Yun-Hsiang Chao," A New Data Encryption Algorithm Based on the Location of Mobile Users", Information Technology Journal 7(1), pp. 63-69, 2008.

[3] Hatem Hamad and Souhir Elkourd, "Data encryption using the dynamic location and speed of mobile node", Journal Media and communication studies, pp. 67-75, 2010

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

[5] H. Liao, P.Lee, Y.Chao, C.Chen, "A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security", In The 9th International Conference on Advanced Communicate Technology, pp. 625-626, Feb. 2007.

[6] H. C. Liao, Y H. Chao, and C. Y Hsu, "A Novel Approach for Data Encryption Depending on User Location," The Tenth Pacific Asia Conference on Information Systems (PACIS 2006), July 2006.

[7] L. Scott, D. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003.

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

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

[10] S U Nimbhorkar, Smruti P Patil, "A Survey on Location Based Authentication Protocols for Mobile Devices", IJCSN, pp. 44-48, 2013.