MOBILE APPLICATION FOR PROVIDING SECURITY TO DATA TRANSMISSION

[1]Prof. P.S. Gaikwad, [2]Pradnya Dalvi, [3]Monal Patel, [4]Charuta Dhalpe, [5]Atul Chaudhari
[1]Professor, Department of Computer Engineering, AISSMS's IOIT
[2,3,4,5]Department of Computer Engineering, AISSMS's IOIT, Pune, India

***Abstract*— Nowadays use of mobile devices has become popular and due to this the frequency of data transmission among the mobile users is increasing. Providing security to the data transmission is important. Security to the data transmission can be provided by encryption of data to be transmitted. These encryption techniques do not consider the location and time of decryption. For such purpose the concept of "Geo-encryption" or "Location-based encryption" has come into existence. Location-based encryption or geo-encryption restricts the location and the time at which the data is to be decrypted. The process of decryption fails if attempted to decrypt the data at some other location and the data is secured. It does not reveal the details about the original data and hence the security is increased.**

***Index Terms*— Encryption, Decryption, Location, Time, GPS.**

I. INTRODUCTION

Nowadays mobile devices have gained importance in our day to day life. Due to this the data communication is increasing and large amount of data is being transferred among these devices. Encryption of data provides security to the data being communicated. Additional layer of security is provided by geo-encryption which is built on the conventional cryptographic algorithms and protocols. The security provided by such location-based encryption is beyond that provided by the conventional cryptographic techniques. The data is encrypted for a specific location and also adds time constraint to it. It supports both fixed and mobile applications. It provides full protection to the data being transmitted.

The process of encryption wherein the decryption of cipher text occurs only at specified location is known as "location-based encryption". The decryption of data fails if it is decrypted at another location and time. The location of the receiver's device which performs decryption is determined by the location sensors such as GPS.

Such location-based encryption techniques can be used to ensure that the decryption of data cannot occur outside a particular area, for example, at the headquarters of government agencies or corporation, at a particular cinema theatre, or an individual's office or home. Time constraint is added to the decryption location. The decryption of data is only possible within the particular time slot. Thus it provides the extra layer of security to the existing cryptographic algorithms.

II. RELATED WORK

A Location-dependent approach known as location-dependent data encryption algorithm (LDEA) was proposed in [1].Firstly the target longitude and latitude coordinates are determined and incorporated with random key for data encryption. The decryption of data occurs only when the target coordinates are matched with the coordinates acquired from the GPS receiver. Its main purpose is to take latitude and longitude coordinates into account for data decryption and thus it restricts the location of data decryption. Tolerance distance (TD) is also considered to increase practicality. Under the restriction of TD decryption is possible. Instead of data encryption standard-GEDTD (DES-GEDTD) to overcome and enhance the performance of geo-encryption algorithm Advanced Encryption Standard Geo-encryption with dynamic tolerance distance (AES-GEDTD) is used [2].

Applications such as location based services managing secure data and digital movies distribution where the major concern is to provide secured access to data is benefited. Such location based encryption system and its uses are proposed in [3].It mainly describes digital cinema distribution application where large media files are encrypted and used at many theatre locations with different geo-lock keys specific to location of theatre. It provides point to multi-point distribution model for delivery through satellite or DVD. A method of encryption where in data can only be decrypted at a specified location is proposed in [4]. It uses Position, Velocity and Time (PVT) mapping function with geo-encryption algorithm. Based on intended receiver's PVT, geo-lock is computed. The session key is then XORed with geo-lock to form a geo-locked session key.

The shortcomings of above two system is overcome by a new concept of geo-encryption and location based encryption is developed [5]. Issues such as confidentiality, authentication, practicability of security and simplicity are met by this new encryption technique based on GPS technology. Geo tags are used encryption of data.

Use of position, time, latitude and longitude coordinates of mobile nodes for encryption and decryption process is described in [6]. To improve the security location based services uses location based encryption methods (LBDEM) such as AES-GEDTD. Some of the applications like patient tele-monitoring system (PTS), Digital cinema distribution and military applications are also described. This paper describes how the conventional cryptographic algorithm such as AES can be extended to use location and time as additional parameters for security.

III. PROPOSED SYSTEM

Geo-encryption algorithms enhance the traditional encryption techniques. It uses location and time of decryption as a mean parameter to provide additional security. The decryption process is limited to specific location and time. The algorithm is not a substitute to any of the traditional cryptographic algorithms, but instead adds an additional layer of security. Decryption process fails if any attempt to decrypt the secure data at an unauthorized location is made. The idea of geo-encryption can be implemented as an android app. The data to be sent is encrypted into cipher text by the sender and it is decrypted to plain text by the receiver. Receiver can decrypt the data if he is present at the specified location and specified time.

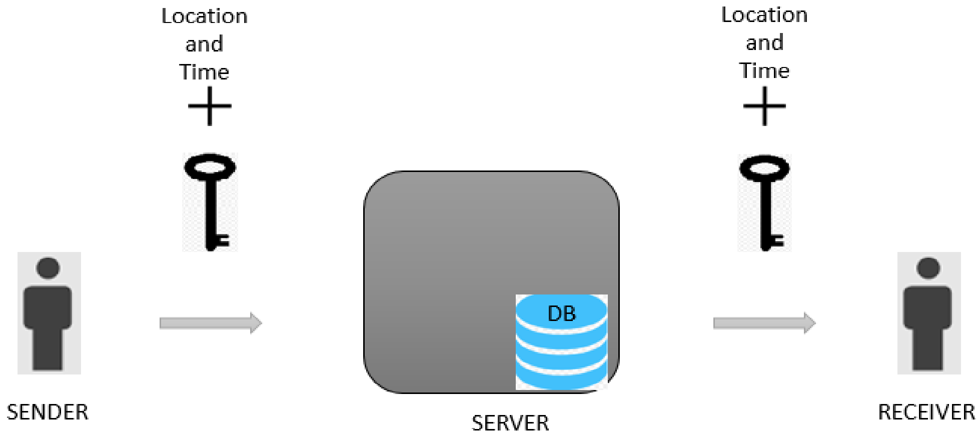
The system makes use of the traditional cryptographic algorithm that is Advance Encryption Standard (AES). AES is symmetric key algorithm with key length of 128, 192 or 256 bits. Hence possible key combinations are 2^{128}, 2^{192} or 2^{256}.It is more secure and powerful than DES algorithm due to long key length.

System Architecture

The Fig.1 shows system architecture. It consists of three components:

- **A.** Sender
- **B.** Receiver
- **C.** Server

Figure 1: System Architecture



- **Sender:** The sender needs to be registered user and after logging in to the system the sender provides the location of the receiver. The location is provided using Google maps. Along with the location the date and time of decryption are also provided. Then the data to be sent is selected and encrypted. The encrypted data is sent to the intended receiver.
- **Receiver:** The receiver also needs to be registered user and after logging in to the system the receiver requests for the data. The location of the receiver is verified by the server and if the user is present at the specified location and time the message gets decrypted else the process of decryption fails.
- **Server:** The server is responsible for sending and receiving of the messages. It also consists of database. It consists of three databases user details, encrypted text message and the uploaded images. The message to be sent is stored at the database and the server keeps the track of the receiver's location. It verifies the location of the receiver and forwards the message to the receiver if he is present at the specified location and time.

IV. SYSTEM IMPLEMENTATION

The components of system are:

- **A.** Login and registration
- **B.** Location retrieval
- **C.** Encryption and Decryption

- **Login and registration:** In this module the user has to register into the application. It consists of simple personal details like user name, password and email. The user logs into the application using user name and password. The registered user details are stored in the database.
- **Location Retrieval:** In this the GPS is used to find the location of the user that is the longitude and latitude coordinates.
- **Encryption and Decryption:** The process of encryption and decryption is done using AES algorithm. The sender provides the location and the time of the receiver and sends the encrypted message. The receiver needs to be present at the specified location and time to decrypt the message. Decryption of message occurs only if the user is present the specified location and time else it fails.

Flow of the system

Figure 2: Sender's side

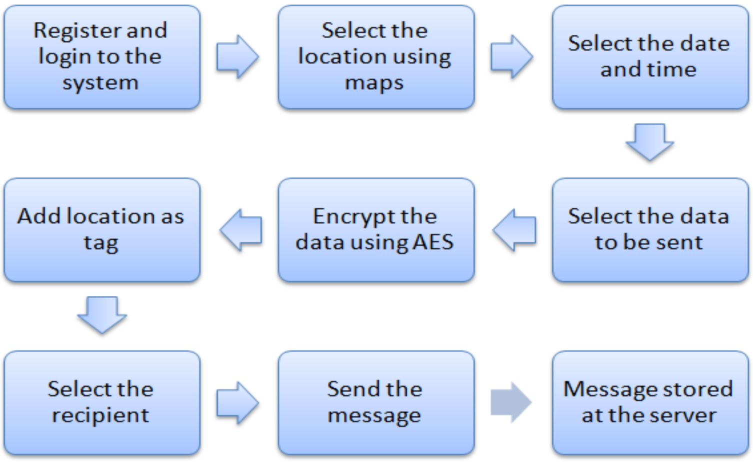

Register and login to the system
Select the location using maps
Select the date and time
Select the data to be sent
Encrypt the data using AES
Add location as tag
Select the recipient
Send the message
Message stored at the server

Fig.2 shows the flow at the sender's side:

- Register and login to the system
- Select location by pinning it on the map
- Select date and time
- Select the data to be sent.
- Encrypt the data using AES algorithm and use location to add geo tag
- Select the recipient and send the message

Figure 3: Receiver's side

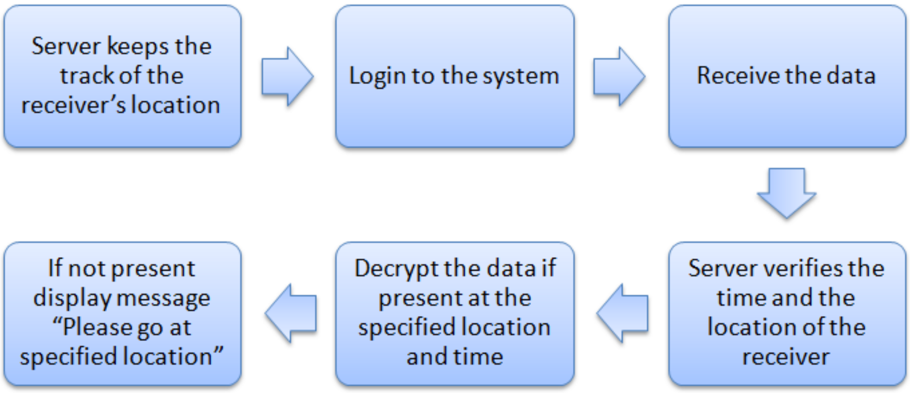

Server keeps the track of the receiver's location
Login to the system
Receive the data
Server verifies the time and the location of the receiver
Decrypt the data if present at the specified location and time
If not present display message "Please go at specified location"

Fig.3 shows the flow at the receiver's side:

- The server keeps the track of the receiver's location
- Login to the system
- Receive the data
- The server verifies the location of the receiver and time
- Decrypt the message if present at the specified location and time
- Display a message 'please go at correct location' if not present at the correct location.

V. CONCLUSION AND FUTURE SCOPE

The security applications can be improved and enhanced by taking location and time into account. The proposed system is used for one-to-one communication. It can also be used for one-to-many communication. The system is able to send only single file at a time so it can be extended to send multiple files at a time. This will give a great elevation to secure the mobile device communication.

VI. ACKNOWLEDGMENT

We would like to express our gratitude to our teachers and friends and all who have helped towards the completion of our system. We are very grateful to our Guide Mrs. P. S. Gaikwad for her guidance through the system. She was very helpful to us, as and when we required her help. We are also very grateful to our other teaching staff for guiding us and all non-teaching staff to help us in various ways in the laboratory.

REFERENCES

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

[2] Pranjala G Kolapwar1, H. P. Ambulgekar, "Use of Advanced Encryption Standard to Enhance the Performance of Geo Protocol in Location Based Network", IJSR, vol. 3, issue 11, pp. 2888-2890, 2014.

[3] L. Scott, D. Denning, "Location Based Encryption and Its Role In Digital Cinema Distribution", Proceedings of ION GPS/GNSS, pp. 288-297, 2003.

[4] L. Scott, D. Denning, "A Location Based Encryption Technique and Some of Its Applications", Proceedings of ION NTM, pp. 734-740, 2003.

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

[6] Pranjala G. Kolapwar, H. P. Ambulgekar, "Location Based Data Encryption Methods and Applications", IEEE Proceedings of GCCT, pp. 104-108, 2015.

[7] Wayne Jansen, Vlad Korolev, "A Location-Based Mechanism for Mobile Device Security", IEEE Computer Society, pp. 99-104, 2009.

[8] Ala Al-Fuqaha, Omar Al-Ibrahim, Joe Baird, "A Mobility Model for GPS-Based Encryption", IEEE Globecom, pp. 1721-1725, 2005.