Location And Authentication Based Encryption Scheme Application Design For Mobile Device

Nisha Gholap,
ME, Department of Computer Engineering, Pune University.

Prof S. S. Das,
Department of Computer Engineering, K J College, Pune.

Prof Londhe D N,
Department of Computer Engineering, GIT, lavel.

I. Abstract

Beside the use of cell phones for voice communication, we are also able to access internet, conduct money transaction, send important data in form of text or image or video message etc. Also the ease of carrying the device and handling data transfer made it popular among the companies and its employee for their data transfer. Later it was found that our data as well as mobile device were vulnerable to attack and theft. This paper presents encryption scheme application for mobile devices which will help in securing data transfer. It specifically provides security for companies, banks to transfer their data to the branches situated at different locations. It provides authentication by using server which contains employee data-base and does key generation as well as key distribution. Secondly it also provides location based security as it limits recipient to be present at specific location to decrypt the message. It's done using GPS system which will detect recipient location if it matches with the location at server end record, then and only then will the key be provided for decryption to the recipient.

Keywords- *Encryption scheme, authentication, location-based security, key generation, key distribution, GPS system.*

II. Introduction

Today wireless has become a critical business tool and a part of everyday life in most developed countries Use of mobile devices for data storage has increased in last few decades, with it mobile data transfer has also increased to a greater extend. Due to all this many companies and banks restrict their employees to carry data or transfer there important data using mobile devices. Thus study related to security of data has acquired great concern. Security is a very difficult topic. Everyone has a different idea of what "security'' is, and what levels of risk are acceptable. Projects and systems can be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

It is important to build systems and networks in such a way that the user is not constantly reminded of the security system around him along with limitation such as mobile terminals have limited memory, limited computational power, limited screen size and resolution. The characters about mobile networks must be considered carefully also, such as having high cost, limited bandwidth, high latency, low connection stability and low availability.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. In cryptography the term plaintext refers to the actual text, encrypted into cipher text. A cipher is a method for changing the plaintext into cipher text, Encryption is the implementation of the cipher. Decryption is the transforming the cipher text back into the plain text i.e. original text. It enables us to achieve three primary security goals namely:

• Availability: It means that the information is accessible to authorized parties whenever they need it.
• Confidentiality: It ensures that assets are accessed by only authorized parties.

• Integrity: It means assets can be modified only by authorized parties or only in authorized way. Modifications include writing, changing, deleting and creating[1].

This paper presents a scheme which can guide secure data handling. This encryption method has tremendous potential benefits to applications such as location based services. This encryption-scheme application can be used by all those companies, banks who have many branches distributed at different locations not only these but those business which are spread over a wide distance and need security. In this paper we take an example of a company who have branches at 2 locations and a main office where the server is located.

The structure of the paper is organized as follows. Section III introduces the related work about geoencryption. Section IV presents implementation of application. Section V concludes the paper. Section VI provides references.

III. Related study

On study of encryption scheme there were many ideas provided but not all covered every aspect needed, the paper by Rohollah karimi and Qazvin Azad try to apply position and time into encryption and decryption process so that security is provided and presents a modified geo-encryption technique which will restrict decoding a message in the specific location and time period thus the recipient can decrypt message if he stays in specific location and limited time[2]. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext[3] .But it does not provide any authentication to the recipient which is important because many mobile devices are prone to be miss handled by wrong people.

To provide more security the above idea was more enhanced by Hsien-Chou Liao and Yun-Hsiang Chao who presented dynamic location based encryption and decryption technique i.e. receiver can only decrypt the cipher text when the co-ordinate acquired from GPS receiver is matched with the target co-ordinate however, current GPS receive is inaccuracy and inconsistent[4]. The location of a mobile user is difficult to exactly match with the target co-ordinate.

The third paper of self-encryption scheme, describes encryption technique which form key based on bits chosen from the message it-self, thus reducing the size of the message. The key is then used for encrypting the reduced message. Decryption of the message can be carried out only when the user enters his correct PIN, which is stored at server. This scheme is suitable considering authentication as it describes a server which authenticates the user but it do not provide additional security layer considering location[5].

Another paper describes a mobility model for existing geo-encryption techniques that allow mobile nodes to exchange movement parameters, so that a sender is able to geo-encrypt messages to a moving decryption zone that contains a mobile node's estimated location. Paper present method for estimating movement parameters of the node. It helps in optimizing the goals of secure wireless communication[6].

While the another paper propose a new method of message security by using the coordinates in GPS service, where it can specify the path of movement by taking some coordinates during travel of mobile node MN and estimate the following situation of MN in a constant time interval. This new estimated coordinate is applied in our secret key. Dynamic Toleration Distance (DTD) is also designed in our key to increase its practicality. The security analysis shows that the probability to break this key is almost impossible due to the security of coordinates and DTD, and adjusting the length of the Random key. Experimental study shows that the ciphertext can only be decrypted under the restriction of DTD[7].

IV. Implementation

This paper present encryption scheme application which can prove beneficial for banks, companies whose branches are spread over a wide distance and need security assurance for data sharing.

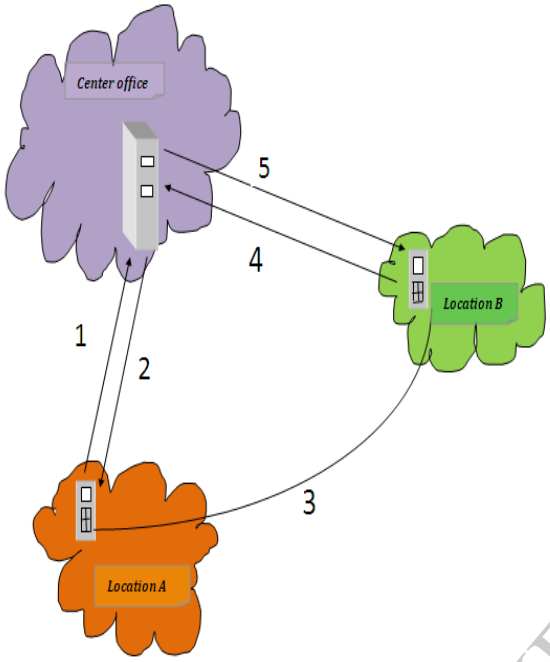

Fig 1.1 Block Diagram (numbers indicate steps)

Above fig 1.1 shows a block diagram in which we consider a company who has a center office with a server (violet color), it has one branch at location A (orange color), other branch is at location B (green color). If an employee at location A wants to transfer any important data to employee at location B he has to just enter recipients phone number then following sequence of steps are executed by the application

1. Senders Application approaches the server to check whether the recipient is an authorized employee.

2. Server authenticates the recipient and forms a key from recipient's office location and his unique random number (generated by the server at a time). Server then transfers this key to the sender's application.

3. Sender then types in his message (important data) and encrypt it with the key from server. Later he sends it to the recipient at location B

4. After recipient receives this message he first needs to enter his password which will be transferred to the server along with his present location for authenticating himself.

5. Server will check password against his name, phone number and his present location if he is a legitimate user and is at same location present at server record (his office location) then server will send him the key formed from his own office location and unique random number.

Recipient then receives this key and decrypts his message. Here two things are considered to be very crucial firstly recipient should be authenticated employee whose data should be present at server end. Secondly whenever recipient wants to decrypt his message he should be at the location which is present at server record (consider his own office location in table 1.1).

Employee Name	Employee's phone number	Employee's password	Employee's Location ID
Om Menon	8333432100	M489	Pune
Shiv Prasad	9878543102	S231	Mumbai
Devyani Swami	7655321001	D532	Goa

Table 1.1 shows Authentication table at server

Employee Phone number	Employee's message Id	key
8333432100	431	RE2390API1

Table 1.2 shows key table at server

Key Generation

When sender request for the key, recipient is authenticated and his record is entered in table 1.2. key is formed at server end by a random number which is generated at server end using any operation combination or function and location Id from table 1.1.

This key is entered in table 1.2. Message id is transferred to sender application, this id is appended to message thus whenever recipient request for key the phone number, message id and location are check by the server and then key is provided to the recipient once the message is decrypted the record in table 1.2 is deleted.

Encryption Algorithm

An Algorithm is considered computationally secure if it cannot be broken with standard resources, either current or future. The following list outlines the strengths and weakness of symmetric key algorithm.

1.1. Strengths of symmetric key Algorithms

- Much faster than asymmetric systems
- Hard to break if using a large key size

1.2. Weakness of symmetric key Algorithms

- Key distribution requires a secure mechanism to deliver keys properly [1].

AES stands for Advanced Encryption Standard and is actually an algorithm that was originally called Rijndael, after its inventors Rijmen &Daemen. The encryption standard of the US National Institute of Standards and Technology (NIST), and the US government reportedly approves AES with 192 or 256-bit keys for encrypting

top secret documents.AES has key size as 128,192,256 and the speed of algorithm depends on key size.128 bits key AES is stronger enough to even secure credit card numbers. AES is symmetric encryption algorithm which is less time consuming and good for small device application. The problem is the weakness of linearity existing in the S-box and key schedule [1]. In order to keep from the new attacks and implement the AES for secure communication, and give out a new implementation scheme for increasing complexity of nonlinear transformation in design of S-box. The default algorithm in this method is AES with 256 bits keys. The principle weakness is the problem of linearity in the S-box and key schedule [1].

V. Conclusion

Advantages of Proposed System are Lower memory space requirement. Improvement of execution time and system performance. Proposed system specifies it is not fully dependent on Key and for the same plain text it produces different modified secure code.

Thus we can say that this paper presents an encryption scheme application which can help companies to secure their information exchange in between their branches located at different location. This application emphasizes on authentication and also location based security as it restrict the recipient to be a legitimate employee and to be present at the specific location to decrypt the message. Location based decryption has proved to be additional layer of security but it also has involved a task of exactly locating recipient and transferring his location to server for location matching. Thus GPS system is to be involved for location tracking of recipient.

VI. References

1. An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard Dhanraj, C. Nandini, and Mohd. Tajuddin Dept of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, IndiaEmail:draj148@gmail.com, laasyanandini@gmail.com, mohd.tajuddin@dsce.com

2. "Enhancing Security and Confidentiality on Mobile Devices by Location-based Data Encryption"RohollahKarimi Department of Computer Qazvin Azad University, Ira**rukarimi@qiau.ac.ir**, Mohammad Kalantari Department of Computer Qazvin Azad University, Iran **mkalantari@qiau.ac.ir** .IEEE conference paper year 2011

3. Logan Scott & Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003, pp 288-297.

4. "A New Data Encryption Algorithm Based on the Location of Mobile Users" Hsien-Chou Liao and Yun-Hsiang Chao Department of Computer Science and Information Engineering, Chaoyang University of Technology, 168 Jifong E. Rd., Wufeng Township Taichung County, 41349, Taiwan (R.O.C.)Information Technology Journal 7 (1): 63-69, 2008 ISSN 1812-5638 © 2008 Asian Network for Scientific Information

5. "Self Encryption Scheme For Data Security in Mobile Devices."

6. "A Mobility Model for GPS-Based Encryption" Ala Al-Fuqaha, Omar Al-Ibrahim, Joe Baird Department of Computer Science Western Michigan University Kalamazoo, MI

7. "Data encryption using the dynamic location and speed of mobile node." HatemHamad and SouhirElkourd* Islamic University of Gaza, Palestine. Accepted 29 December, 2009.