Enhancing Security And Confidentiality For Mobile Device

Prof Sanjay S. Kadam
Ankita Shinde,Harshada Durge

Bharati Vidyapeeth College of Engineering
Sector-7,C.B.D,Belpada,Navi Mumbai-400614,India.

Abstract—This paper related to security and confidentiality on mobile devices by using location based encryption

Mobile devices are very easy to handle.With the help of mobile devices we can communicate with each other. Mostly mobile devices are used for sending message from one location to another location[1].

Most of the mobile security application cannot restrict the location and time of the message or data. That is independent from location and does not provide more security if mobile devices are GPS(Global Positioning System) enabled[2]. Therefore we provide such security by using Geo encryption technique that is based on location or restrict the location & time of the messages.

In this paper we are going to find weaknesses in existing Geo encryption system and try to used location and time into the encryption and decryption processes therefore that provides more security and safety for mobile data[3]. In that mobile devices will allow to communicate to each other safely by restrict decoding message in the specific location and time.

Receiver can only decrypt the encrypted message(ciphertext) when receiver's GPS location matches with the specified location.

Keywords-*Geo--encryption;GPS; Location;Security; Encryption; Decryption ;Mobile devices.*

I. Introduction

The use of mobile devices has become a very important part of our daily routine. Most of the time mobile devices are used for communication , access internet, transaction, sending mail etc. by using our cell phones and new services continue to be added. But all of them need security for their communication.

To send GPS coordinates to other mobile through (SMS) short message service based on GPS technology.This application also enables the users to get their current location coordinates[1].

GPS can show you to your exact location on the earth in any weather conditions anywhere in the world,24 hours a day.

In this paper, we are going to solve weaknesses in the existing Geo encryption system and try to used position and time into the encryption and decryption processes[2]. Therefor that provides more security and safety for mobile data or messages.

Most of the mobile security application cannot restrict the location and time of the data or message i.e. independent from and does not provide more security. We provide such security by using 'Geo-encryption' technology i.e. it is based on location or restrict the location and time of the message.

The term "location_based encryption" means that the any method of encryption where the encrypted message can only be decrypted at a specified location. If an attempt of decryption is made at another location , the decryption process fails and not get information about the plaintext[5].

For encryption purpose we used symmetric key algorithm i.e. (AES). In symmetric key algorithm,it use the same key for encrypting and decrypting plaintext.

In Geo encryption model the plaintext is encrypted ,using an encryption key .The encryption can be done on both receiver location and message. In Geo-decryption phase the given specified location match with current location of receiver, then receiver decrypt the message otherwise this process is failed.

II. Our Model

The above fig. shows our simple model.

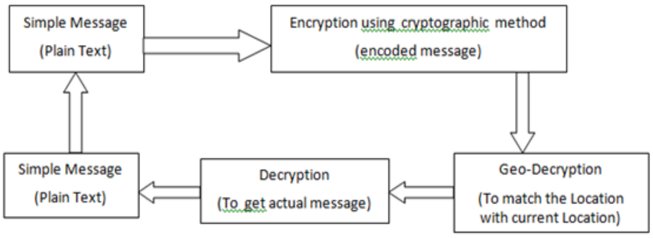


Fig. Geo encryption Model

The simple message is encrypted using an encryption key. In this encrypted message the receivers location also exists, both message and receivers location is encrypted.

In Geo-decryption phase the given or specified location match with current location of receiver.

If the specified location is match with current location of receiver then receiver decrypt the message otherwise this process is failed[3].

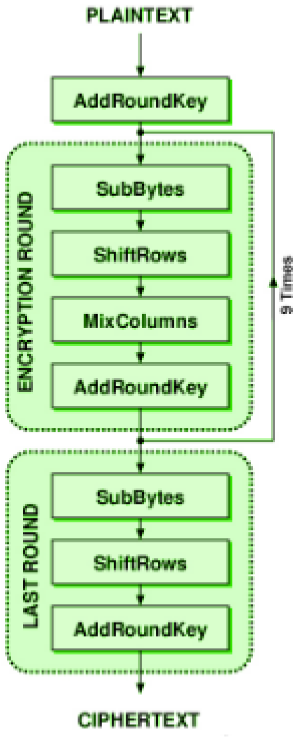
III. Geo Encryption Algorithm

- Encryption algorithm divided into two categories.
  A. Symmetric algorithm
  B. Asymmetric algorithm
- Symmetric algorithm use the same key for encrypting and decrypting plaintext.
- Asymmetric algorithm use the different key for encrypting and decrypting plaintext.

Use AES Algorithm :

The Advanced Encryption Standard or AES is a symmetric block cipher ,is a symmetric encryption algorithm.

AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.



This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century." It was to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext[6].

AES Analysis:

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered.

IV. CONCLUSION

Geo encryption is an approach to location based encryption that includes cryptographic algorithm. It provides full protection against location independence. Some encryption technology cannot restrict the location of mobile devices for data providing more security.

Therefore we are try to used location dependent data encryption algorithm i.e. restrict location of mobile devices for data decryption.

V. REFERENCES

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

[2] L.Hsien-Chou, C.Yun-Hsiang, “A New Data Encryption Algorithm Based on the Location of Mobile Users”, Info. Tech. J. , 2008.

[3] Al.Omar, Al.Ala, D.Dyk, N.Akerman, “Mobility Support for Geo-Encryption”, IEEE ICC International Conference, 2007.

[4] V.Vijayalakshmi, TG.Palanivelu, “Secure Localization Using Elliptic Curve Cryptography in Wireless Sensor Networks”, I CSNS Int.J.Comput.Sci.Network.Secur, 2008.

[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]https://en.wikipedia.org/wiki/Advanced_Encryption_Standard