Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406
International Journal of Advance Engineering and Research Development
"Emerging Technologies in the Computer World", January -2017

Enhancing Security Using Location And Time

Pradnya Dalvi[1], Monal Patel[2], Charuta Dhalpe[3], Atul Chaudhari[4] Prof. P.S.Gaikwad[5]

[1,2,3,4] *Computer* Engineering, *AISSMS's IOIT*
[5]*Prof., Department of Computer Engineering, AISSMS's IOIT*

Abstract – *Now a days mobile networks and devices are growing rapidly, we can use them to send and receive emails, important documents, photos and electronic media etc. In such cases we need to secure communicated data and to do so encryption-decryption techniques are use. So these systems cannot withstand the data security and chances of hacking data is more. Since these systems do not take into account the location and time for decryption. For such purpose the concept of "Location and Time based encryption" is being used. In this paper, we will enhance the security by adding additional level of security that is location and time of the receiver. Receiver can only decrypt the message if the user is present at the location and time specified by sender. This will resolved the security issue.*

Keywords *- Security, location and time, encryption, decryption, mobile nodes, GPS.*

I. INTRODUCTION

Nowadays mobile communication is gaining more importance in day to day life. As the world is moving towards ubiquitous computing the use of mobile devices is increasing, since they can be access anywhere anytime. Mobile devices such as PDAs (Personal Digital Assistance), mobile phones, laptops, tablets, smart devices, etc. are widely used. Communication in these devices mostly occurs through wireless technology. These devices are not only used for voice communication but also used to access internet, to perform online transactions, send and receive emails, to transfer important document, etc. and new services continued to be added further.

Large amount of sensitive data get transfer over the network but this data is not that secured and authenticated. Hence to secure and authenticate this data, encryption and decryption techniques are being used. But these techniques do not take into account the location and time for encrypting and decrypting the data. Adding location and time provides additional layer of security to the data.

This paper proposes new system which uses location and time to secure the data. At sender side message will be encrypted using receiver's location and time. Location can be given through GPS, IP address, satellite or by manually entering the co-ordinates. At the receiver side there will be mapping of location and time. If the receiver is present at specified location at specified time, then the message will be decrypted else the message will not be decrypted.

II. OBJECTIVES

To create a new encryption technique which uses AES algorithm and provides higher level of security to the confidential data against the intrusion in the transmission of data. To use location and time as constraint for providing higher level of security

III. PROBLEM STATEMENT

A new encryption technique that uses the advanced encryption algorithm that provides high level security against any intrusion in the transmission of emails or any other message.

IV. RELATED WORK

Cryptography is used for safer communication of data over network. It is a technique in which plain text is transformed into cipher text and vice versa. Cipher text is a way of representing the data which is unreadable by humans. It consists of special symbols and text which is not decodable. The process of converting plain text to cipher text is known an Encryption and the reverse process is known as Decryption. Cryptography is used in emails, digital signature and in many other security applications. Such techniques do not take location and time into consideration. Hence the concept of "Geo-encryption "came into existence. Geo-encryption approach is built on the existing cryptographic algorithm and protocols which provides an additional layer of security to traditional algorithms. In this approach the data is encrypted based on specific location or area and time as constraint.

It benefits some of the applications such as location based services, managing secure data and digital movie distribution where controlling access is a major concern. Such location based encryption system and its use in digital cinema distribution is proposed [1]. In this application large media files are encrypted and used at many theatre locations with distinct Geo-Locked keys specific to the location of recipient. Point-to-multipoint distribution model for delivery through satellite or DVD is provided. Based on Position, Velocity and Time (PVT) of the recipient the Geo-Lock is computed using Geo-Lock mapping function [2]. A new concept of "Geo-encryption" and location-based encryption is developed to overcome the short comings of the above two systems [3]. Confidentiality, authentication, simplicity and practicability of security issues are met by this new encryption technique which uses GPS technology. It makes use of geo-tags which are used for encryption.

Another access control model that works like three factor authentication to get access to the system was proposed [4]. Authentication is based on geodetic location parameter received from GPS or GSM and time. It improves computer and network security. Such systems can be used in applications such as military. A brief survey of location based services is presented [5]. It consists of the technologies used to track location of mobile user and the accuracy and reliability associated with such measurements. To enable these location based services, the network infrastructure elements deployed by the wireless network operators are also described.

Another location-dependent approach known as location-dependent data encryption algorithm (LDEA), was proposed [6]. It determines the target latitude or longitude coordinate and incorporates random key with it for data encryption. It makes use of GPS which is inaccurate or inconsistent. So it becomes difficult to exactly match the target coordinates. Hence to increase the practicality a toleration distance (TD) is designed in LDEA. Decryption of data is possible under the restriction of TD. To enhance the performance of Geo-protocol and to overcome the weaknesses of Geo-encryption algorithm Advanced Encryption Standard-Geo Encryption with Dynamic tolerance distance (AES-GEDTD) is used instead of Data Encryption Standard-GEDTD (DES-GEDTD) [7]. Location based Services (LBS) uses Location Based Data Encryption Methods (LBDEM) to enhance the security [8]. It uses position, time, latitude and longitude coordinates of mobile nodes for encryption and decryption process. To give higher security AES-GEDTD is used as LBDEM. It also describes the use of this approach in some applications like Digital Cinema Distribution, Patient Tele-monitoring System (PTS) and Military Application.

V. PROPOSED SYSTEM

The rapid change in technologies and increase in data intrusion has led to the development of different encryption algorithms. We are going to propose a system which enhances security level at the time of data transmission. In this system, location and time these two parameters are considered which will improve the security. A new text based encryption technique that uses the advanced encryption algorithm that provides high level security against any intrusion in the transmission of emails or any other message is proposed. Any data that is to be transmitted in the form of texts can be secured from intrusion. The system will be using the AES algorithm for the encryption and decryption purpose.

AES is a symmetric key algorithm i.e. the public and the private keys are same. It uses Key of length 128, 192 or 256 bits. The possible key combinations are 2^{128}, 2^{192} and 2^{256}. Permutation-Substitution Network Structure is used in AES. Due to long key length it is more secure and powerful algorithm. It is impossible to crack AES algorithm. The additional layer of security will be provided by adding location and time as constraint.

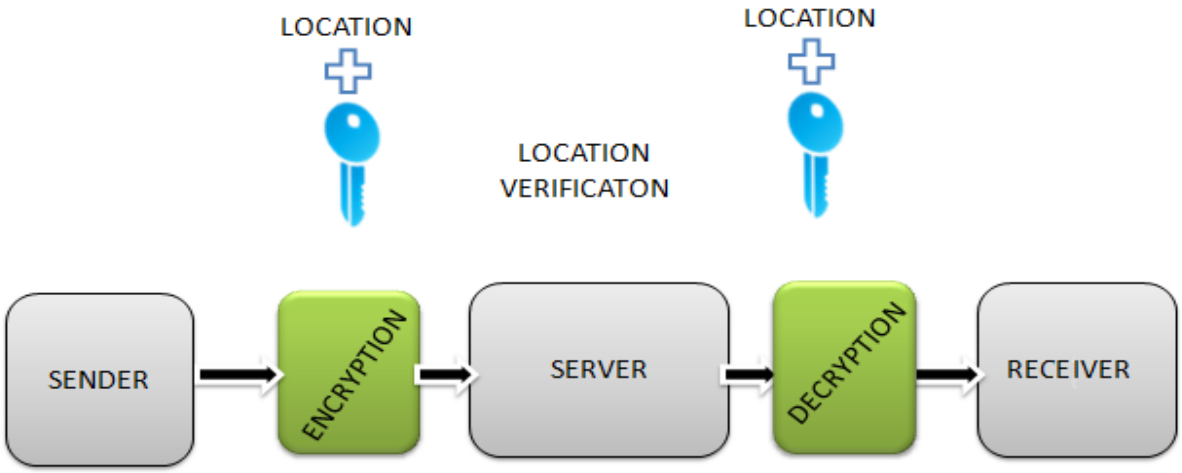

Figure 1: System Overview

The Figure 1 shows the system which will be consisting of sender, receiver and a server. The sender will encrypt the message using the AES algorithm and will transmit it to the server along with the location and time of the receiver. The server will verify the location of receiver and send the message to the receiver adding the time constraint. The receiver will then decrypt the message using the key only if the receiver is present at the location and time specified by the sender. The security provided to the system is very high in nature.

VI. CONCLUSION AND FUTURE SCOPE

By taking location and time into consideration, the security applications can be improved and enhanced. This will give a great elevation to secure the network communication. The system can be strengthened by using AES algorithm along with location and time as constraint. Since the time is taken from the server it cannot be manipulated. This system can be used to send multimedia files.

VII.REFERENCES

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

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

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

[4] Suresh Limkar, Nivedita Kadam, Rakesh Kumar Jha, "Access Control Based on Location and Time", SPIT 2011, LNICST 62, pp.102-107, 2012.

[5] H P Ambulgekar, Manisha S Manindraker, Pranjala G Kolapwar, "A Survey on Location Based Data Encryption Algorithms for Mobile Devices", IJARCSSE, vol. 4, issue 5, pp. 1010-1015, 2014.

[6] 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.

[7] 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.

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

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

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

