

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 1 ISSUE : 3 Print / Issue Publication Date: 08-Oct-2016

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 114-116
Published Online December - January 2016 in IJEAST (http://www.ijeast.com)



GEO-ENCRYPTION TO ACCESS THE DATA USING AES ALGORITHM

Himanshu Pant
G.L. Bajaj, Greater Noida, India

Vinay Kaushik
G.L. Bajaj, Greater Noida, India

Priyanshi Singhal
G.L. Bajaj, Greater Noida, India

Vishal
G.L. Bajaj, Greater Noida, India

ABSTRACT - The location based encryption or Geo-Encryption technique that uses GPS technology to enhance the data security. This concept is developed so that at a particular position and time, the specific recipient will decrypt the files. The breaching of data due to stolen laptops are a major problem. This technology will be used to restrict unauthorized user for any violation. Our approach is to use a security system to secure data by using an encryption algorithm and particular coordinates of the recipient with tolerance distance. It will set a limit to decrypt that encrypted data. It is an innovative technique to encode the location information into the encrypted keys. If an unauthorized person attempts to decrypt the file at some other location, the security system will not reveal any information about that original plain text. Firstly, we need an encryption algorithm and latitude and longitude of the receiver's location. The receiver can decrypt the file when the coordinates acquired by GPS devices are matched with the target coordinates. AES is one of the best encryption algorithms in terms of data safeguard and gives a high level of confidentiality as compared to DES and RSA encryption algorithm.

General Terms – AES (Advanced Encryption Standard) algorithm, GPS devices, Encryption

Keywords - Geo-encryption, location-based encryption, data security

I. INTRODUCTION

Data revealing has become a major matter of concern nowadays. Lost/broken laptops being one of the causes of this unintentional disclosure of our personal information. According to FBI, more than $3.5 million are lost due to laptop theft. These leaks can expose our financial account information, health records, owner's account numbers, and other crucial data. As we are heading towards the electronic systems, we rely more on our personal laptops for storing sensitive data.

We can prevent such leak of data by authenticating users and encrypting sensitive data. In a survey, it is indicated that only half of the companies encrypt data while others view the technology as an unnecessary burden. Users often prefer convenience over security as users and admin want a system that works with little or no actions on their part.

However, there is often a trade-off between security & user effort.

In this paper, our goal is to reduce user effort associated with encryption technology to increase the security as compared to traditional password-based techniques. We tend to lower the threshold and examine how much security we can achieve having no per laptop secrets on devices by applying zero user effort (i.e. no password entry, biometric entry, or possession of cryptographic tokens). Our approach is to encrypt user-specified confidential files in a 'trusted location' and leave all other insensitive files unencrypted and always accessible. If the system is idle for an instance or the user is inactive, logs off, or puts the computer to sleep, the files are automatically re-encrypted. In case, if a user wants to access the file in any another location other than the trusted location, user have the alternative to enter a key and access them. This acts as a fail-safe mechanism if there is an unavailability of the required location specific services like Internet connection. Implementing the system requires a minimal time depending on the security level, location-specific information and technique used. Once the key is known, we can access any file we intend to.

Rather than entrusting on something users know, have, or are, we explore using *where the user is* to perform access control.

II. GEOENCRYPTION

The term "location-based encryption" refers to an encryption approach wherein the ciphertext can only be decrypted at a specified location. Plaintext encrypted using any sort of cryptographic algorithms, using coordinates of a peculiar location as the key values for that algorithm. If an attempt is made to decrypt the data at a vague location then the decryption process fails and no information about the plaintext is revealed.

The client can access or encrypt data when the acquired coordinates match the definite coordinates. Decryption is performed by the device that determines its location using some location detection applications & sensor, for

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 114-116
Published Online December - January 2016 in IJEAST (http://www.ijeast.com)

example, a GPS receiver, Google maps or some other satellite or radio frequency positioning system. This location-dependent approach can satisfy the confidentiality, simplicity, authentication and practicability of security issues.

A DYNAMIC TOLERANCE DISTANCE is also considered in final key, which provides a range of location coordinates to the client to decrypt the data, it increase the accuracy & inconsistency of coordinates.
Time, as constraints could be used on the decryption location. Data can be encrypted using time constraints, for example, data can access only for a particular time period like an organization provides the access of data in working hours only.

III. LITERATURE WORK

Enhancing the security of data using location based encryption is an efficient approach. System for this consists of following modules:

i. Login & registration
ii. Encryption of plain text
iii. GPS interfacing & matching coordinates
iv. Decryption of cipher text.

3.1 Login & Registration:

In this module, the user is provided with the interface to interact with the system. Registration is to acquire details about the user like username, password, and user id. Login is to allow the user to interact with data.
To store user information, we can use SQL servers.

i. Encryption Of Plain Text

There are different cryptographic algorithms for encryption of data, but we use Advanced Encryption Standard (AES) algorithm, which will use target coordinates as key value pairs for encryption. It is used for high security and as well as for high speed. Both Hardware and software implementation are possible quite efficiently. New encryption standard is recommended by NIST (National Institute of Standards and technology) to replace DES. Encrypts data blocks of 128 bits in ten (10), twelve (12) and fourteen (14) round depending on key size as shown in Figure. It can be implemented on various platforms. It can be used in small devices. It is carefully tested for many surveillance applications.

ii. GPS Interfacing & Matching Coordinates

In this module, through GPS or any other location detecting sensors coordinates of accessing devices acquired with DTD, i.e., Dynamic Tolerance Distance, which reduces the problems arises in GPS receiver in accuracy and inconsistent of data.

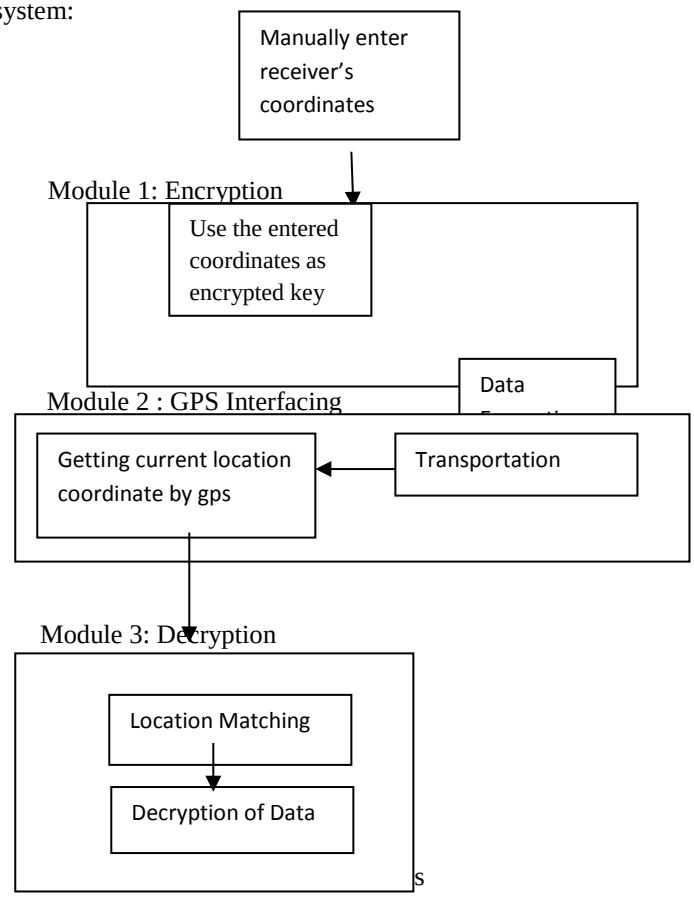
Matching coordinates are to check the acquired coordinates with target coordinates (i.e. Longitude, longitude or altitude).

iii. DECRYPTION OF CIPHER TEXT:

If the location coordinates satisfy the condition, then decryption is possible and the only client accesses the data or encrypted information. Again, any decryption algorithm should be designed to decrypt the data.

IV. SYSTEM ARCHITECTURE

The fig.1 shows the overall flow of the proposed system:



➢ ALGORITHM STEPS**:**

These steps are used to encrypt 128-bit block.

- The set of round keys from the cipher key.
- Initialize state array and add the initial round key
- To the starting state array.
- Perform round = 1 to 9:

➢ USUAL ROUND: Execute the following operation which are described above.

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key, using K (round)



- FINAL ROUND: In this round, Execute the following operations which are described above
- Sub Bytes
- Shift Rows
- Add Round Key, using K(10)
- ENCRYPTION: In encryption, each round consists of the following four steps:

- SUB BYTES: The first transformation, Sub Bytes is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
- SHIFT ROWS: In the Encryption, the transformation is called Shift Rows.
- MIX COLUMNS: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
- ADD ROUND KEY: Add Round Key precedes one column at a time. It adds one round keyword with each state column matrix; the operation in Add Round Key is matrix addition.

The last step consists of XORing the output of the previous three steps with four words from the key schedule. And the last round of encryption does not involve the "Mix columns" step.

V. CONCLUSION

Users and corporate IT personnel want security solutions that straightforwardly work and want to avoid any schemes that require additional effort or administrative overhead. In this work, we designed Location-specific Encryption, a system that requires zero user effort and limited IT administration in the common case. It remains secure when facing an Outsider Thief (OT), a laptop thief. On the basis of observation the majority of access to sensitive documents occur while located in a trusted location, we designed Derivation protocols that allow a laptop to derive the key needed to access sensitive files based on a location automatically. It provides automatic protection of sensitive files with limited delay during the initial access. Usually, it takes less than 5 seconds to automatically derive the key and decrypt the files.

Location's latitude/longitude co-ordinates play an important role in the formation of encrypting data along with decryption process. This approach can be extended to the other application domain (e.g. Software authorization). If the system software is authorized and located within a pre-defined location or area, such as for particular organization the execution of the software may achieve the location check based on proposed approach.

This approach can be used for mobile applications such as in Smartphone.

VI. REFERENCES

[1] Swapna B Sasi, Betsy K Abraham, JInil James, Riya Jose "Location Based Encryption using Message Authentication Code in Mobile Networks", In IJCAT International Journal of Computing and Technology Volume 1, Issue 1, February 2014.

[2] 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.

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

[4] V. Murali, V. Rajeswari, "A Navel Approach to Identify Geo-Encryption with GPS and Different Parameters (Locations and Time)", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4),

[5] ISO/IEC 7810, Identification cards - Physical characteristics, Third ed. 2003-11-01, Ref. no. ISO/IEC 7810:2003(E)

[6] Martin E.Hellman, Whitfield Diffie, "New Directions in Cryptography", IEEE Trans. on Information Theory, Vol. IT-22, No. 6, Nov. 1976

[7] Logan Scott, "GPS Interference and jamming issues for civil and military users"

[8] GSM 11.11, Specification of the Subscriber Identity Module, GSM Technical Specification, Version 5.0.0, Dec. 1995

[9] Forouzan, "Data Communication and Networking", TMH

[10] A.S. Tanenbaum, Computer Networks, Pearson Education

[11] Behrouz A. Forouzan: Cryptography and Network Security, TMH

[12] B Schneier: Applied Cryptography, John Wiley & Sons

[13] Bernard Menezes," Network Security and Cryptography".

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

- Himanshu Pant
- Vinay Kaushik
- Priyanshi Singhal
- Vishal

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com
www.ijeast.com
India

2455-2143