Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 01, January-2018

Location Based Cryptography

Encryption and Decryption of data using live location of device

Harshil Darji
B. E. Information Technology
Dharmaj (Gujarat, India) – 388430

***Abstract*— There have been many changes in the ways people live, work, play and share in the past three decades due to introduction of Information Technology. Information Technology has enormous impact on various domains like business, educational fields, healthcare departments, and also the defense department. This also introduced a risk of information theft and vital archive leaks. For these reasons, it is now necessary to secure such information using various encryption methods available. We can improve the security level of such encryption methods by making them location aware. This will add an extra layer to the security of the crucial data.**

***Keywords*— Location, Latitude, Longitude, Encryption, Decryption, Cryptography, GPS**

I. INTRODUCTION

There are many methods available in the technological world to encrypt and decrypt data, but most of them does not consider location of device at the time of encryption.

In this paper, I will be describing a method to use device's live location in combination with a password as the encryption key to avoid brute-forcing because location will be fetched using either device's GPS or IP address. This means once you encrypt the data at a particular location in the world, you must be at that particular place to decrypt it.

This will add an extra level of security because no matter how hard a person will try to decrypt the text, he/she won't be able to do so without being at a particular place.

II. PROPOSED METHOD

Main purpose of the proposed system is to improve the security of the existing algorithms by making the live location of the device a part of key that can be used as encryption key.

Proposed method comprises of following five phases:

A. Device's location
B. Passphrase (Alphanumeric)
C. Generating key
D. Encryption
E. Decryption

In following sections, I will explain each of the above components in as much details as I can.

A. Device's location

Device's location can be acquired using various ways such as:

i. Using in-built GPS (Global Positioning System)
ii. Through network provider (in mobile devices)
iii. Using device's IP address

B. Passphrace (Alphanumeric)

An alphanumeric passphrase is a combination of alphabets and numeric characters that can be used as a password which will be combined with live location of the device.

C. Generating key

In proposed method, an encryption key is the combination of device's location with the passphrase provided by the user.

This combination is then converted into MD5 hash to make it more secure, unique and of equal length. So, the encryption key will be calculated as following:

Encryption key = MD5(location + passphrase)

The same procedure is repeated during decryption process to generate decryption key.

D. Encryption

Encryption is the process of converting simple plain text into a form that is not human readable or that makes no sense without processing.

There are currently various algorithms that can be used with proposed methods such as:

i. Advanced Encryption Standards (AES), developed by Vincent Rijmen and Joan Daemen
ii. Data Encryption Standards (DES), designed by IBM in 1970.
iii. Vigenere Cipher, invented by Giovan Battista Bellaso
iv. RSA (Rivest–Shamir–Adleman), designed by Ron Rivest, Adi Shamir, and Leonard Adleman

The above listed are only few popular algorithms that can be used as an encryption algorithm with proposed system.

E. Decryption

Decryption is the process of deciphering encrypted data by entering passphrase, combining it with location of the device and creating MD5 hash of the combination and using it as the decryption key to retrieve original data.

The catch here is even if you provide correct passphrase, but you are trying to decrypt at location other than location where you encrypted the data, you will not be able retrieve the original data. This is the main advantage of location-based cryptography system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 01, January-2018

III. DIAGRAMS

A. *Encryption*

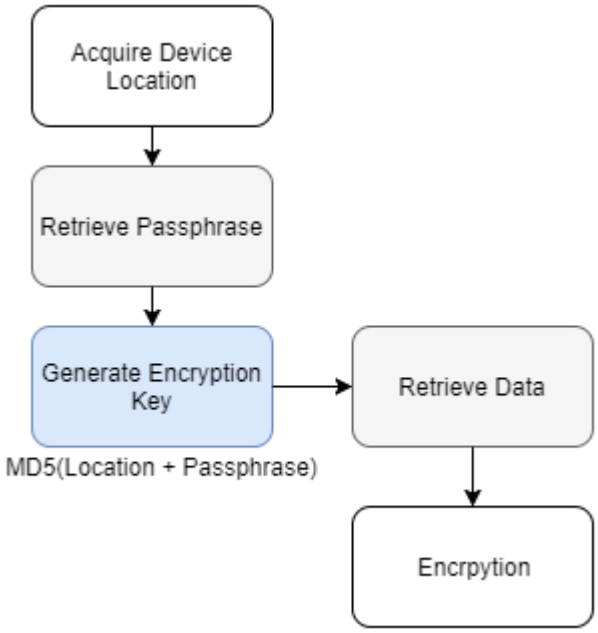

Figure 1. Encryption Diagram

B. *Decryption*

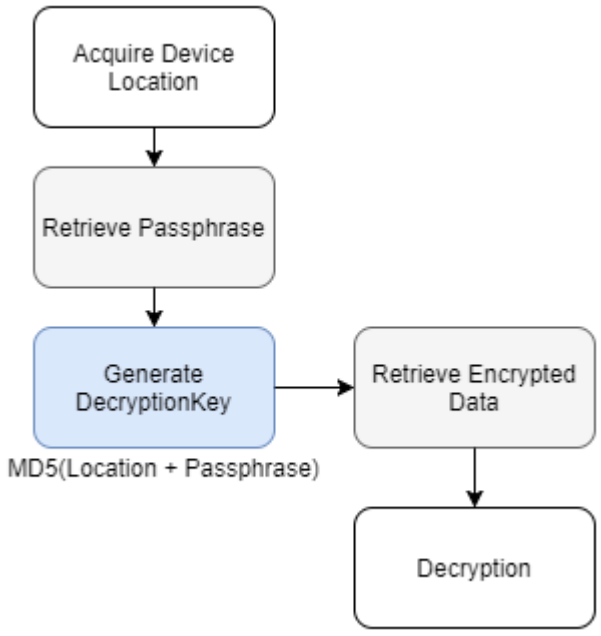

Figure 2. Decryption Diagram

IV. ADVANTAGES

- Location based cryptography method works like a two-factor authentication used in web applications to provide enhanced and improved security to existing algorithms as:
    1. First factor: Location of the device which will act as first level of security,
    2. Second factor: Passphrase entered by user which will be used in combination with location of the device
- Another major advantage is necessity of being at the encryption location to decrypt the data. So even if encrypted data is stolen during the hack, hacker will not be able to retrieve original data from it because of the change in location.
- Device's location is a physical attribute which cannot be brute forced.

V. APPLICATIONS

Proposed method is useful in various fields including:

- Defense Departments,
- Space Agencies,
- Educational Bodies,
- Finance Ministries and Agencies
- Healthcare Organizations
- Intelligence and Spy Bureaus
- Tech Giants (such as Google, Microsoft, Facebook etc.)

VI. CONCLUSION

A physical attribute such as location is when combined with a secret passphrase, it creates a unique combination. In addition, when the MD5 hash of such combination is used as the key for cryptography, it becomes hard to crack or brute force the resulted encryption text.

VII. NOTE

I have created a demonstration program using Python to support my paper which encrypts and decrypts string data using combination of location and passphrase as the key.
Link:
https://github.com/harshildarji/location_based_cryptography

VIII. REFERENCES

[1] Borse Manoj V., Bhandure Harshad D., Patil Dhiraj M., Bhad Pratik B., "Location Based Encryption-Decryption Approach for Data Security", International Journal of Computer Applications Technology and Research, Volume 3– Issue 10, 610 - 611, 2014