International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

GEO ENCRYPTION USING GPS CO-ORDINATES

Surabhi Suryakant Dabholkar

Graduate Student, Department of Computer Engineering, Terna Engineering College, India.

Abstract - *Geo Encryption basically uses global positioning system (GPS) co – ordinates for the purpose of security. The main concept of this technique is developed because no unauthorized user should be able to decrypt the message which will help us to prevent any unauthorized user from accessing the confidential data. Basically, the sender will use the idea of the GPS co – ordinates and encrypt the information. Use of AES algorithm helps us to secure the confidential information. AES is the most advance algorithm in terms of security. AES is comparatively more secure and has more advanced features than DES & RSA algorithms. Additional parameters such as latitude, longitude, time and Armstrong numbers will also be used in order to make a unique technique for encrypting the confidential information. These parameters will ensure higher security for the data. A GPS module SKYLAB SKGI3 OEM with active antenna will be used in order to detect the receiver's location through the GPS co-ordinates which would be entered manually by the sender, sending the confidential message or information. This technology can only be used when there is a transfer of highly confidential messages such as military or research centers*

Key Words: Geo Encryption, GPS Co – Ordinates, Armstrong Number, Security Algorithm, Location based encryption, GPS Module, Visual Studio, VB.net.

1. INTRODUCTION

Nowadays, data security has been playing a major role as there are various hacking techniques developed. This leads to revealing of important & confidential information. There are lot of social applications like Gmail, WhatsApp, Facebook which are more likely hackable. This concept cannot be used for the regular purpose or day to day basis. It would be helpful where there would be transferring of highly confidential message. Our approach of making this technique is to be made useful for military purposes where data security is very important aspect and if not taken proper care would cause a great loss for our country. This technique would also be use in research work. Our major approach is to encrypt the highly confidential message or information in such a way that the specified user will be able to decrypt the message at a particular location & time. AES is the best algorithm which would be used in this process. Use of parameter such as "Armstrong number" and "Time" will give more secure approach towards encrypting the confidential information. Tool will be able to encrypt or decrypt the message based on the encryption parameter set for the message such as location, Armstrong number and the day at which the message should be decrypted.

1.1 Present Scenario

Nowadays, data security has been playing a major role as there are various hacking techniques developed. This leads to revealing of important & confidential information. There are lot of social applications like Gmail, WhatsApp, Facebook which are more likely hackable. This concept cannot be used for the regular purpose or day to day basis. It can only be used in that places where there is a transfer of highly confidential data.

1.2 Drawbacks of the current system

The current system uses latitude and longitude as its Parameters. Loss of a GPS Module or loss of multimedia device can cause a major damage as all the information may be lost. Therefore, it is important to keep all the devices safe to prevent such losses.

1.3 Suggested Improvements

Additional Parameters such as Armstrong Number, Timestamp, Personal Key are added to increase the security.

2. ENCRYPTION ALGORITHM

[1]. In encryption process, the set of derived keys are called as the ROUND KEY. There are three bits available i.e. 128- bit, 192- bit and 256- bit.

[2]. Derive the set of round keys from the cipher key.

[3]. Initialize the state array with the block data (plaintext).

[4]. Add the initial round key to the starting state array.

[5]. Perform nine rounds of state manipulation.

[6]. Perform the tenth and final round of state manipulation.

[7]. Copy the final state array out as the encrypted data

3. SYSTEM OVERVIEW

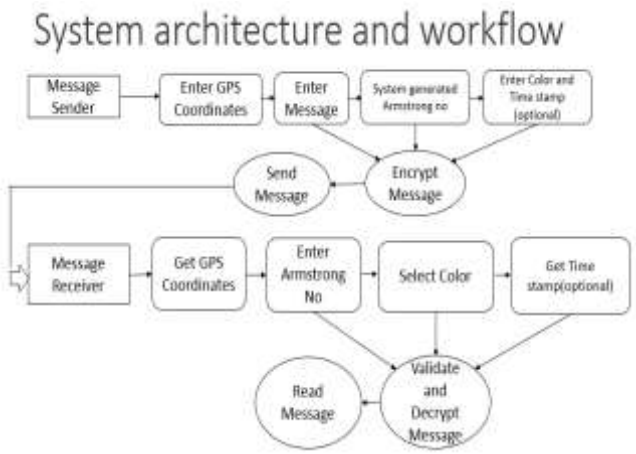

Fig – 1: System Architecture

4. PROPOSED METHODOLOGY

In this project, our goal is to reduce user effort associated with encryption technology to increase the security as compared to traditional password-based techniques.

There are various encryption methods. All of them require key. We will use GPS coordinates as key. We will pre-process coordinate so as to obtain stronger key. Hashing is one pre-processing method but mathematically results in weaker key. This is due to fact that hashing always return fixed length string (also contains no special characters etc.)

We will be using 2 keys for the encryption:

1. GPS coordinates

2. An Armstrong numbers

5. IMPLEMENTATION

The process starts with user entering the cipher text in Visual Studio. Then we have to add Additional Parameters such as Armstrong Number, Color, Timestamp, Co-ordinates. Then, using these parameters a key is generated which is used for encrypting the cipher text. This Encrypted Cipher text is sent to the receiver through any multimedia device.

The receiver will decrypt the message using GPS module. The message will get decrypted only if the Target co-ordinates of the sender and receiver get matched.

5.1 The Steps are as follows

[1]. Get target GPS coordinates manually

[2]. Let user type the message

[3]. Encrypt the message using step 1 as key (pre-processing can be done for stronger key)

[4]. Let the message be transported to target location

[5]. Ones at target location; connect GPS module

[6]. Get actual location from GPS; and try decryption.

[7]. If coordinate in step 1 and 6 are same; proper encryption will occur

6. GPS MODULE

There are in excess of 12 kinds of module accessible in Indian market. We will utilize GPS Receiver SKYLAB SKG13C OEM with dynamic reception apparatus. It is anything but difficult to use with PC or MCU. The Skylab SKG13 arrangement is a total GPS beneficiary module that highlights super affectability, ultra-low power and little shape factor, Dual Power Source. The GPS flag is connected to the radio wire contribution of module, and a total sequential information message with position, speed and time data is displayed at the sequential interface with NMEA convention or custom convention. It depends on the elite highlights of the MediaTek 3329 single – chip design. Its -165dBm following affectability broadens situating inclusion into place like urban ravines and thick foliage condition where the GPS was unrealistic previously. The little frame factor and low power utilization make the module simple to coordinate into compact gadgets like PNDs, cell phones, cameras and vehicle route frameworks. This module helps in recognizing the correct co-ordinates of the sender just as collector. I have additionally made a CRT screen which is appeared as follows. It demonstrates the scope, longitude just as height taken from the distinctive satellites by this GPS Module.

Fig -2: GPS Receiver SKYLAB SKG13C OEM.

6.1 Features

[1]. It has 165dBm ultra – high sensitivity**.**

[2]. At low level signal it is extremely fast.

[3]. It has a high accuracy time pulse up to 1PPS

[4]. It also has a low power consumption.

6.2 Applications

It is used in mobile phones.

[1]. It is also used for vehicle navigation system.

[2]. It is used in Location Based Service (LBS).

[3]. It is also used in Portable Navigation Device (PND).

7. ENCRYPTION PROCESS

In Cryptography, encryption is the process of converting plaintext into ciphertext. It also encodes messages in such a way that only authorized person can read it. In an encryption scheme, the message, is referred to as plaintext, is encrypted using an encryption algorithm and by generating cipher-text. The message is only read after being decrypted. The encryption technique uses a pseudo - random encryption key generated by an algorithm. An authorized recipient can easily decrypt the message with the key provided by the sender to recipients but not to unauthorized interceptors or users. The key acts as a password. The key must be known to both the sender as well as the receiver. The encryption process is done by creating a screen on visual studio which is shown below.

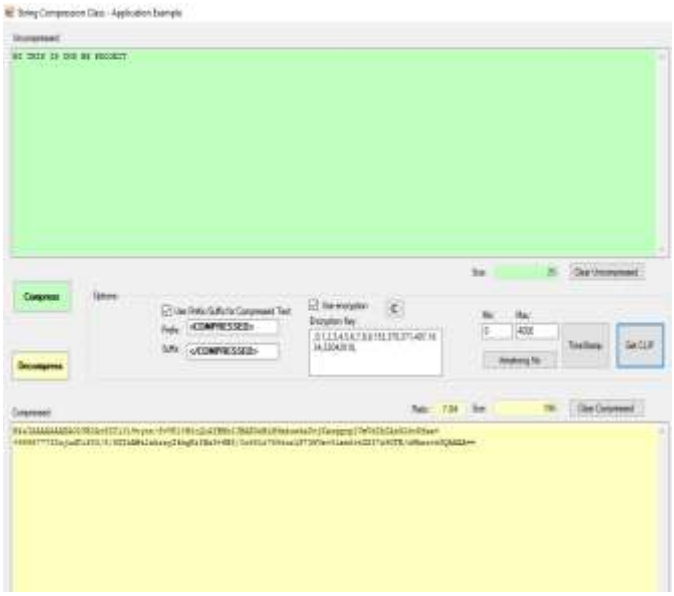

Fig – 3: Encryption Screen.

8. DECRYPTION PROCESS

The Receiver will only be able to decrypt the message when he is located at particular location where the Sender has mentioned particular co – ordinates. Once the target co-ordinates are matched and all the other parameters are satisfied, automatically the message is been decrypted and the receiver is able to read the confidential message. In this way the message gets decrypted. The decryption process is done by creating a screen on visual studio which is shown below.

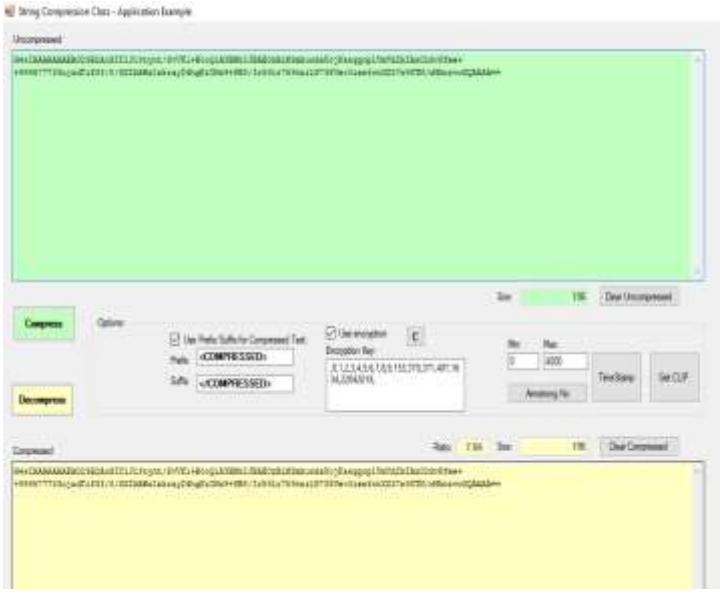

Fig – 4: Decryption Screen.

Fig – 5: CRT(Cathode Ray Tube) SCREEN.

9. FLOWCHART.

There will be two types of users in this kind of system, one will be sender of the message and other will be the receiver of the message. The Sender will get the GPS coordinates from receiver for its location or can decide the location coordinates where the message is supposed to be received.

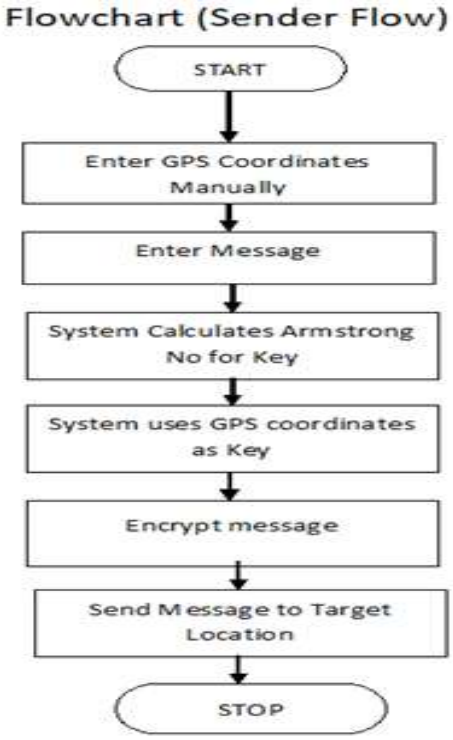

Fig – 6: Sender Flowchart

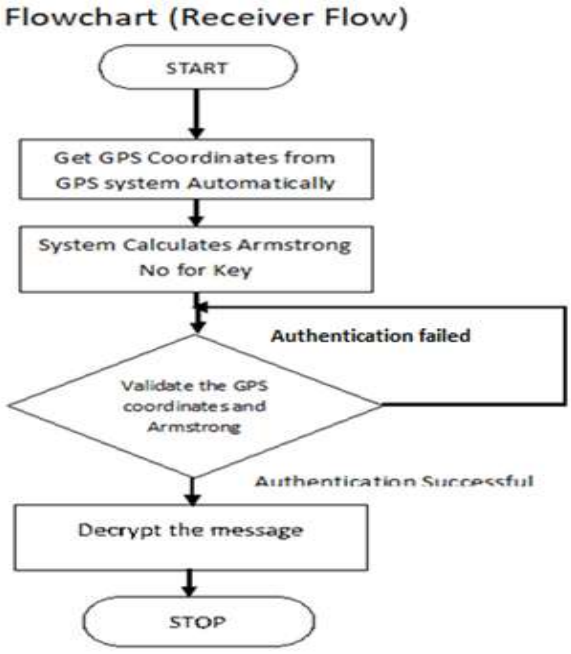

Fig – 7: Receiver Flowchart

9.1 Flowchart for the sender and receiver

[1]. Get target GPS coordinates manually

[2]. Let user type the message

[3]. Encrypt the message using step 1 as key

[4]. Give the Armstrong Number to make the key stronger

[5]. Let the message be transported to target location

[6]. Flow at the receiver end will be as follows:

[7]. When message receives at target location; connect GPS module

[8]. Get actual location from GPS; and try decryption.

[9]. If coordinate in step 1 and 6 are same; proper encryption will occur.

10. OVERVIEW OF THE LANGUAGE USED

The language used for this project is .NET. The screen is been created on the Visual Basic. The advantages of .Net are many which includes its horizontal scalability and also the use of multiple languages which allows the user to modify its program accordingly. It has a best user interface practices when performed on Windows and Microsoft and thus it can perform with ease. It allows you to call methods from C# and VB.net. Other languages can also be used such as C++ and Java.

11. HARDWARE DESCRIPTION

The selection of hardware is very important in the existence and proper working of any software. When selecting hardware, the size and requirements are also important. The Processor used is i3/i5/i7, +2 GHz with 2 GB RAM and 1 GB Hard Disk Drive. The resolution is 1024*786, full colors.

11.1 Proposed system is developed on

Processor is i5, 2.7 GHz with 4 GB RAM and 40 GB Hard Disk Drive. The monitor used is Display Panel (1024 X 764) with the display adapter Trident super VGA. Network adapter used is SMC Ethernet Card Elite 16 Ultra.

11.2 Software description

The operating system used in this is Windows XP/7/8 32 bit having the front end as the visual studio and back end is MS SQL SERVER 2005 EXPRESS if required.

12. CONCLUSION

Hence this GPS Module will be very useful in military purposes where there is transfer of highly confidential Information. This module is used in place like urban canyons and dense foliage environment where the GPS was not possible before. Thus, this will help us to provide more secure approach for the purpose of encryption and decryption.

13. REFERENCES

[1]. "Handbook of Applied Cryptography", Alfred J. Menezes, Paul C. Van Oorschot and Scott R. Vanstone. July 8, 2011.

[2]. "A location-based encryption technique and some of its application", Logan Scott, Geo codex LLC, LS consulting Dorothy E. denning Geo codex LLC, Naval post graduate school.

[3]. "Cryptography theory and practice", third edition, Douglas R. Stinson, University of Waterloo, Ontario, Canada, published in 2006

[4]. "Cryptography Engineering: Design Principles and Practical Application", Niels Ferguson, February 2010.

[5]. "Geo Encryption - A New Direction to secure traditional SSL VPN, Information Technology: New Generation (ITNG)", April 2011.

[6]. "Geo Encryption: Using GPS to enhance Data Security", Soft Logan and Denning, D.E, April 2003.

[7]. "An Improved Geo-Encryption Algorithm in Location based Service", Pranjala G. Kolapwar, CSE Department, SGGSIET, Nanded, May 2015.

[8]. "Geo Encryption to access the data using AES

[9]. Algorithm", Himanshu Pant G.L Bajaj, Priyanshi Singhal G.L Bajaj, Vishal G.L Bajaj, Dec-Jan 2016.