International Journal of Computer Applications Technology and Research
Volume 3– Issue 10, 610 - 611, 2014

Location Based Encryption-Decryption Approach for Data Security

Borse Manoj V.
Sandip Institute of Engineering and Management
Nasik, India

Bhandure Harshad D.
Sandip Institute of Engineering and Management
Nasik, India

Patil Dhiraj M.
Sandip Institute of Engineering and Management
Nasik, India

Bhad Pratik B.
Sandip Institute of Engineering and Management
Nasik, India

Abstract: Data security is an important task in today's life. Data security can be done using GPS device. Among computer user mostly use data in electronic format. How to provide a security for data is important. In this paper, we propose a Location Based Data-Security System to secure data by applying Encryption-Algorithm and co-ordinate using GPS device. Encryption means of efficient secure integer comparison. The encryption technology cannot restrict the location of data decryption. In order to meet the demand of a location-dependent approach location-dependent data encryption algorithm is needed. A target latitude/longitude co-ordinate is determined firstly. The co-ordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher text when the co-ordinate acquired from GPS receiver is matched with the target co-ordinate. GPS-based encryption is an innovative technique that uses GPS-technology to encode location information into the encryption keys to provide location based security. GPS-based encryption adds another layer of security on top of existing encryption methods by restricting the decryption of a message to a particular location. Our experimental results not only validate the effectiveness of our scheme, but also demonstrate that the proposed integer comparison scheme performs better than previous bitwise comparison scheme.

Keywords: encryption; decryption; security; GPS technology; location.

1. INTRODUCTION

Most of the data encryption techniques are location-independent. They cannot restrict the location of clients for data decryption. In proposed system, a novel location-dependent approach is used for incorporating location information into data transmission.

It is important to provide a secure and convenient data transmission. We propose a location-dependent approach for better data security. The client put the coordinates manually in application for data encryption. Then our application create a encrypted file and then we send that encrypted file using e-mail or by any external device to our destination .The client only decrypt the cipher text when the coordinate acquired from GPS receiver matches with the target coordinate. According to our discussion, the approach can meet the confidentiality, authentication, simplicity and practicability of security issues. As a result, the proposed approach can meet the demand for personal and industrial data security.

2. PROPOSED WORK

Enhancing the security is the prime aspect of the proposed system. By adding the location based services with the encryption process one can make the data more secure.

System consists of following components:

1. Login and Registration
2. Encryption
3. GPS Interfacing and Location Matching
4. Decryption

2.1 Login and Registration:

Login and registration module provide user the access rights to interact with the system. Registration contains some basic details regarding to username, password and email id. Login uses username and password to allow the user to pass in to the system.

For storing the details, we use SQL server 2005. For username and password separate table is maintained. Tables are handled by administrator.

2.2 Encryption:

The process of converting the plaintext to human non understandable form, so that if the data is obtained by third party person then they will not able to understand or retrieve it.

For this purpose, we use various algorithms like M. Aikawa et al. proposed a light-weight encryption algorithm for the copyright protection. T. Jamil proposed an enhanced algorithm for the typical DES algorithm, called AES (Advanced Encryption Standard). J. Jiang proposed a parallel processing algorithm for the RSA. S. Lian et al. proposed a fast video encryption scheme based on chaos. M. McLoone and J. V. McCanny designed a hardware circuit for DES based on the FPGA technique. M. Shaar et al. proposed a new data encryption algorithm, called HHEA. M. E. Smid and D. K. Branstad analyzed the past and future of DES algorithm. Y P. Zhang et al. proposed a stream cipher algorithm with respect to the traditional block-based cipher approaches [2].

Location co-ordinates are used as a 'key' for encrypting the contents.

2.3 GPS Interfacing and Location Matching:

Global Positioning System satellites broadcast signals from space that are used by GPS receivers to provide current location by making use of longitude and latitude.

The interfaced GPS device will appear as virtual serial port on PC to which one can communicate through our designed software which can transmit receive by this serial port like HyperTerminal or custom made software.

Location matching is the key process for successful decryption of data. The co-ordinates fetched by GPS must be matched with the co-ordinates which were entered while encrypting the data. As current location retrieved by GPS device will not be exactly same every time due to weather conditions, etc. Tolerance distance (TD) important role in rounding up or down the co-ordinate values at certain extent.

2.4 Decryption:

The location co-ordinates which were used as key while encryption must be matched with co-ordinates values fetched by GPS device at receiver side. If this condition is satisfied then only user can decrypt the data otherwise encrypted file will be discarded from the system automatically.

3. SYSTEM ARCHITECTURE

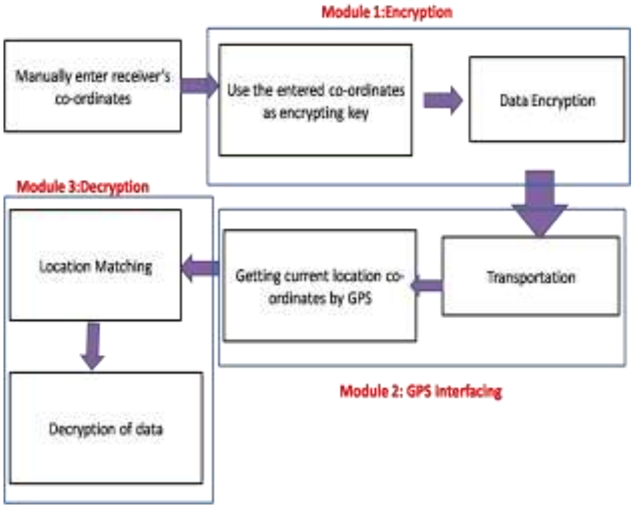
Module 1:Encryption
Manually enter receiver's co-ordinates
Use the entered co-ordinates as encrypting key
Data Encryption
Module 3:Decryption
Location Matching
Getting current location co-ordinates by GPS
Transportation
Decryption of data
Module 2: GPS Interfacing

Figure. 1 System Modules

The figure shows the overall flow of the proposed system.

4. APPLICATIONS

•Military- In military this technology can be used to keep the data secured from the attackers during wars.

•Banks- This technology can also be used in banking for the purpose of money transaction.

•Individual use- It can also be used to store one's confidential data. For e.g.: for business purpose.

•Multinational Industries-In Industries important data can be secure by using this technology.

•College-In college's important data can be secure by using this technology. For e.g. Question paper.

5. CONCLUSION

Location's latitude/longitude co-ordinates plays vital role in the formation of encrypted data along with decryption process.

The proposed approach can be extended to the other application domain e.g. Authorization of software. If the system software is authorized within a pre-defined area, such as for particular organization the execution of the software may achieve the location check based on proposed approach. Decryption process is carried out when the authorized user is located in specified area.

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

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

[4] V. Rajeswari, V. Murali, A.V.S. Anil, "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), 2012.