Location Dependent Cryptographic Algorithm based on Open Source Application

Mainak Sen
CSE Dept.
Techno India University
Kolkata-700091

Sachin Tibrewal
CSE Dept.
Techno India University
Kolkata-700091

Sumana Majumder
CSE Dept.
Techno India University
Kolkata-700091

Nehal Ahmad
CSE Dept.
Techno India University
Kolkata-700091

Kishlay Kumar Singh
CSE Dept.
Techno India University
Kolkata-700091

ABSTRACT
The use of Location Based Services has helped in enhancing information security to a great extent but there's no denial that there are flaws in its applications. Sometimes these identities are forged or duplicated which would lead data breach and thus compromised security. In present world scenario, the ability to securely store data and transfer sensitive information has proved to be critical when it comes to success in business as well as war. Hence, we need a better form of cryptographic technique. In this paper we focus on the concept of Location Dependent data Encryption Algorithm.

The Android operating system is may be the most profitable and gainful options of an open source platform. Android is based on the Linux kernel and it consists of APIs with class bearing potential reference to Location Based Services which gives facility to obtain a mobile phone's location from any location provider such as GPS or A-GPS and is designed to be open for other location based systems.

Keywords
Location based services, location based encryption algorithm, open source application, geographic positioning system, android sdk.

1. INTRODUCTION
Location based Cryptography is based on the theory that geographical positions can be used to derive the credentials which determine the key features of the identities used by the involved parties which are sharing the information. This form of cryptography employs a method of not only integrating the location of the participating nodes into encryption and decryption processes but also incorporates these locations into the process of construction of keys that are required to cipher and decipher the plain text data. We have tried to demonstrate that a particular location provided by the receiver node can be used as a key and incorporated into the encryption process to manipulate the plain text and convert it into a cipher text. For the purpose we have used the symmetric-key cryptographic mechanism which means that the cipher text can be decrypted using the location of the receiver node. The concept and utility of Location Dependent data Encryption Algorithm was initially proposed by Hsien-Chou Liao and Yun-Hsiang Chao [11].

Traditional encryption assures that users who have certain kind of authorization can access secure content. Location-based service [20] integrates a mobile device's location related information such as latitude, longitude to provide extra security to user [1, 2]. The increasing popularity of Location Based Services has brought us to a new field of research such as location-aware emergency response, location-based advertisement, location-based entertainment, location based cryptography. Location-based encryption refers to a method of encryption in which the cipher text can only be decrypted at a specified locality like headquarters of a government agency or corporation, or an individual's working place. If an attempt is made to decrypt the cipher text at some other place, the decryption process fails and reveals no information about the plain text. Also time, bio-statistics, space can be posted as additional constraints on the decryption location.

Encryption based on location enhances security by position integration into cryptographic processes. But later, it was found that simple encryption or decryption based on time and location was not enough when it came to security. Hence, it was decided to use the location for a key generating process [8], [10]. Later the concept of Geo-encryption came to play in which the cipher text is only decrypted when the person is at a specified location. If an attempt is made trying to decrypt data at any other location, the decryption process does not work thus saving the information. In this method, the key depends on target geographic location which powers it to use in real time applications [6].Then came the concept of biometric encryption. In this encryption type along with the location some biological features of the receiver are required for the decryption process. These features if not provided lead to the failure of the decryption process thus keeping the plain text safe from any unwanted source or third party.

Feature phones which people used to have few years ago, had very limited applications and were not able to support many location-based services. But today's smart phones are hugely popular and they come with a wide variety of features [3]. This has helped in bringing about great changes in LBS. Smart phones come with much more reliable and strong operating systems with different features. This has made the development of various applications comparatively easy. Mobile devices can be differentiated into different gadgets such as PDAs, wireless notebooks, portable GPS, auto navigators, and mobile phones. Current smart phones can support all of these functions with the help of embedded or installed applications. Smart-phone based LBS using GPS or WI-FI shows high level of accuracy and can be applied in many business areas.

Different location retrieval approaches have been proposed. Within a short range, to locate individuals, generally, indoor localization techniques such as Infrared, Ultrasound, Radio frequency, Blue-tooth and Wireless LAN are being used. Global Positioning System, Differential GPS, Assisted GPS (A-GPS) [4] also provides user's location. Mobile phone network localization techniques are the latest amongst these. A mobile phone after switched on, logs on to the best acceptable network. Network base stations then recognize the entry of a user into a serving cell and whether the user is within the serving contiguity of that station's surroundings. Then, the base station automatically locks on to the mobile and hands the call from one base station to its next base station and serving cell within its network [5].

ADEL (Android Data Extractor Lite) [21] is a forensic tool for retrieving and evaluating data out of data sources for further data processing and data storage or migration for versions 2.x of Android. This tool includes numerous scripts written in Python and can be easily extended. It can automatically dump previously defined SQLite database files from Android devices and extract the contents stored in the dumped database. Firstly, ADEL establishes a link to an Android device through the Android debugging Bridge (ADB). Then it dumps the preset SQLite database files from the phone and stores them on the investigator's machine. All the next steps are carried out on copies of the database files in the read-only mode to ensure the accuracy and consistency of data. Secondly, the contents of the dumped database file copies are analyzed and extracted. For this, a specially designed parser module for the SQLite database file format is developed. After the contents are extracted, an XML-based report is generated for further use and data presentation. The report can be viewed using an ordinary web browser. In the initial state, the following information can be dumped and analyzed

- Telephone and SIM-card information,
- Phone book and call lists,
- Calendar entries,
- Browser history and bookmarks,
- SMS messages.

But ADEL can be used only with mobile phones that provide root access to applications because of its necessity to access the ADB interface.

2. TYPES OF CRYPTOGRAPHIC SYSTEM

2.1 Symmetric Key Algorithm

In symmetric algorithms, the encryption key and the decryption key are the same as shown in Figure 1.

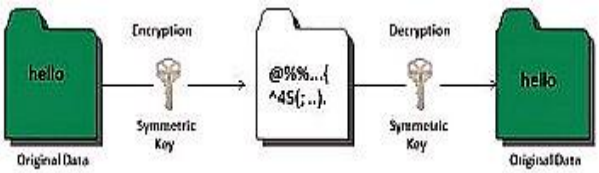

Fig1: Symmetric key algorithm

Here on the sender side data is being encrypted by a key, then the cipher text is being sent over the public channel to the receiver side. On receiving the cipher text, the receiver does decryption process using the same key.

2.2 Asymmetric key Algorithm

In Public-key algorithms two keys are used for encryption and decryption process as shown in Figure 2, one is known as private key and other one is known as public key.

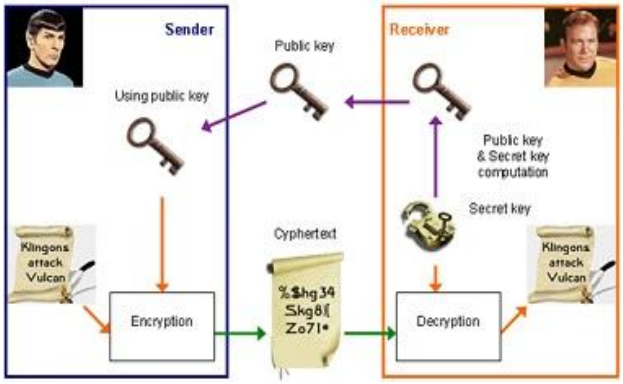

Fig 1: Asymmetric key algorithm

3. ENCRYPTION DECRYPTION USING LOCATION BASED SERVICES

3.1 The Geo-Encryption Algorithm

In this algorithm, data is encrypted for a specific place or a broad geographic area and it supports constraints in time as well as in space. This algorithm is compatible with both fixed and mobile applications and supports a range of data sharing and distribution policies [9].

3.2 Location Dependent Encryption Algorithm -LDEA

LDEA includes the latitude and the longitude coordinates for the data encryption and decryption phases [7] [15]. Concept of LDEA process is shown in Figure 3. It generally has two phases: register and key synchronization for operation phase. During register phase, a random seed value and a MAC function C is transmitted to a mobile device. Generally one way hash function is used to prevent the computation of input value from obtained output value and a new key is created for each session. A key synchronization process is done to make sure that both sides use the same key for encryption and decryption algorithm. After synchronization of key is done, the plain text can be encrypted and transmitted to the mobile client securely.

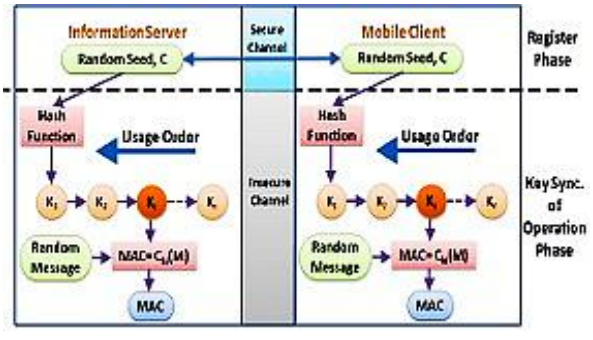

Fig 2: LDEA process

3.3 Self-Encryption

It treats the data set as a binary bit stream and generates the key stream by extracting n bits in a pseudo-random manner based on a user's unique PIN and a nonce.

3.4 Mobile User Location-specific Encryption – MULE

Mobile User Location-specific Encryption uses location-specific information to derive a decryption key and allow access to the sensitive files. When the user is inactive for some reason the files are automatically re-encrypted and the key is deleted from the computer [13, 14], [16, 17].

4. PROPOSED WORK

Here we have designed an LDEA based encryption algorithm. A smart phone has been used here as the mobile device which gives the latitude and longitude of BOB [18, 19]. The encryption and decryption phase was done by using C language.

4.1.1 Consideration

Alice will send information to BOB, encryption of the information done at ALICE's end by the latitude and longitude of BOB.

4.1.1.1 *Proposed Encryption Algorithm:*.

Step 1: BOB will find his latitude and longitude using GPS application from his smart phone.

Step 2: BOB will share his position via email/text message to ALICE.

Step 3: ALICE will then encrypt the information based on the latitude of BOB.

Step 4: Next ALICE will encrypt the newly formed information by longitude of BOB and creates the cipher text.

Step 5: ALICE will send the cipher text to BOB.

4.1.1.2 Proposed Decryption Algorithm:.

Symmetric algorithms always decrypt the cipher text in the same way as it was formed from the plain text.

Step 1: After getting the cipher text at his end, BOB will now decrypt it by first using his own latitude.

Step 2: The cipher text thus obtained is the intermediate state.

Step 3: Then BOB will perform decryption by his longitude to get back the plain text.

5. EXPERIMENTAL RESULTS

In this work, first BOB shares his location via GPS mobile app as shown in the Figure 4.

Here first we have done the experiment where both ALICE and BOB are in the same city. On receiving the latitude and longitude from BOB, ALICE will encrypt the plain text. Then ALICE sends the plain text via public domain and BOB decrypts it by his latitude and longitude. Intermediate results of each encryption and decryption are shown in figure 5. Further, we have done our experiment based on locations of two different cities. BOB is from DELHI and ALICE is from KOLKATA. Location of BOB is shown in figure 6.

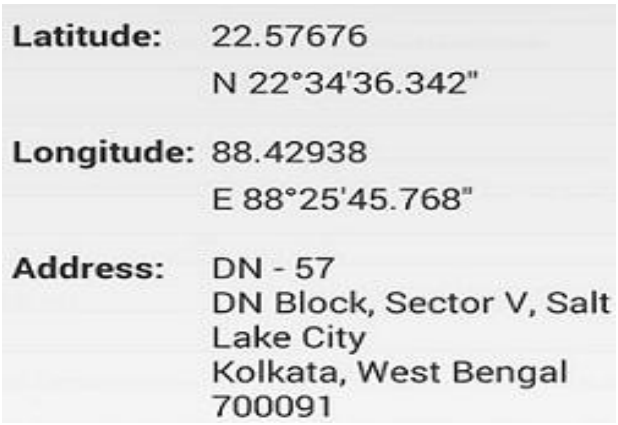

Fig 3: Latitude and Longitude of BOB from same city

In this first experiment, BOB shares his latitude and longitude from his native location. Receiving them ALICE encrypts the plain text by BOB's latitude and longitude respectively. Then ALICE sends the cipher text via internet which is then being decrypted by BOB on his side. Figure 7 gives the detail output.

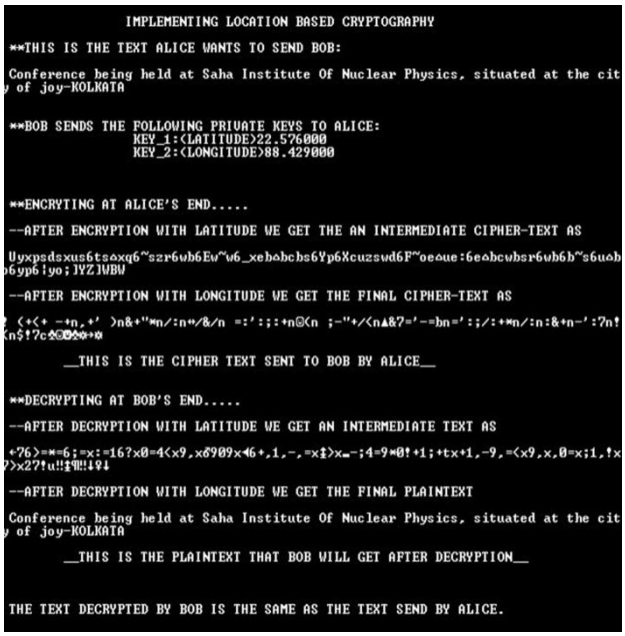

Fig 4: Output 1

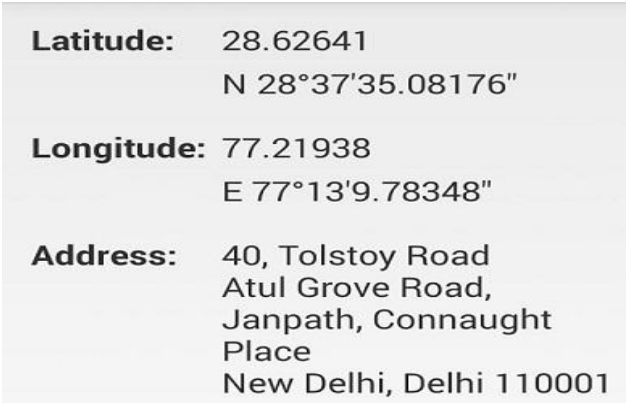

Fig 5: Latitude and Longitude of BOB form different city

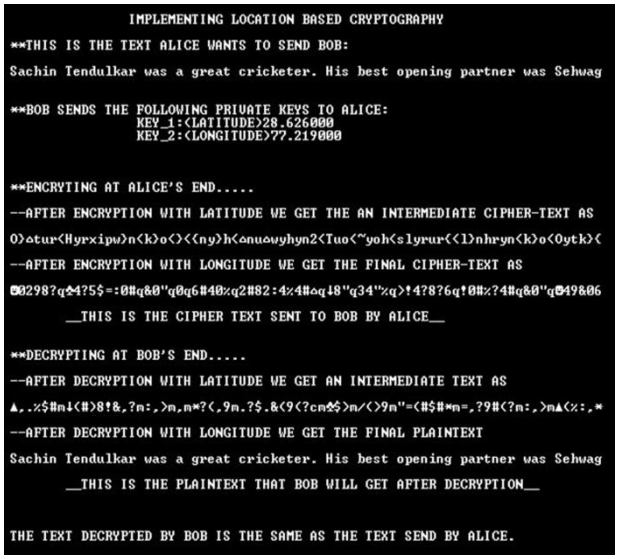

Fig 6: Output 2

After doing so, we consider the latitude and longitude of BOB. In our source C program, we have calculated the summation of ASCII values of plain text on ALICE side and also the summation of decrypted text on BOB side. In both cases we found a match which has been shown in figure 8 as a chart. The blue columns show the latitude, longitude and their corresponding plain text, cipher text ASCII value marked as Series 1. Series 2 show the latitude, longitude and their corresponding plain text, cipher text ASCII value cases we found a match which has been shown in figure 8 as a chart. The blue columns show the latitude, longitude and their corresponding plain text, cipher text ASCII value marked as Series 1. Series 2 show the latitude, longitude and their corresponding plain text, cipher text ASCII value.

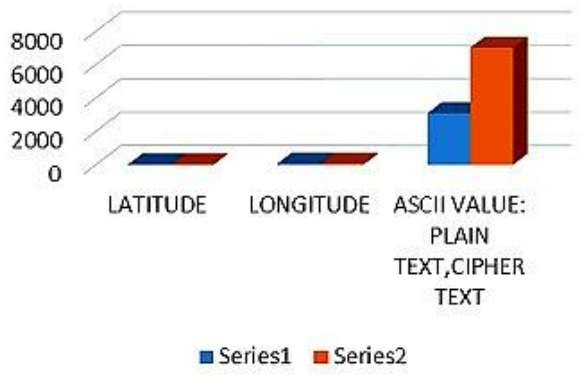

Fig 7: Chart

6. CONCLUSION

Location Dependent data Encryption Algorithm is not strong enough as it uses the static location of mobile node and they are using the static tolerance distance to overcome the inaccuracy and inconsistent of GPS receiver. Reference [12] proposed a protocol that uses dynamic location of mobile node and dynamic tolerance distance which makes it very strong to attack. Also with the increasing research on DNA computing, cryptographic concepts can be merged with Biometric that would add one more layer to the security. New age smart phones with embedded ultrasonic biometric sensors can be used to add identity based services with location dependent data encryption techniques.

7. REFERENCES

[1] Xu, H., S. Gupta. 2009. The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services. Electronic Markets, Vol. 19, No. 2: 137-149,.

[2] Barnes, J.S. 2003. Known by the Network: The Emergence of Location-Based Mobile Commerce" In E.P. Lim and K. Siau (eds.). Advances in Mobile Commerce Technology. Hershey, PA: Idea Group: 171–189.

[3] Park, J., S. Yang, and X. Lehto.2007. Adoption of Mobile Technologies for Chinese Consumers. Journal of Electronic Commerce Research, Vol. 8, No. 3:196-206.

[4] G.M. Djuknic and R.E. Richton. February 2001. Geolocation and Assisted GPS. Bell Laboratories, Lucent Technologies, Computer (ISSN 0018-9162).

[5] J.E.Spinney.2003. Mobile positioning and LBS application. Geography 88 (4) 256-265.

[6] Pranjala G Kolapwarand and Prof. H. P. Ambulgekar. Use of Advanced Encryption Standard to Enhance the Performance of Geo Protocol in Location Based Network. International Journal of Science and Research, ISSN:2319-7064.

[7] Y. Lakshmi Prasanna and Prof. E. Madhusudhan Reddy.2014. A Generalized Study on Encryption Techniques for Location Based Services. Journal of Computer Engineering e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, PP 19-26.

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

[9] V. Rajeswari, V. Murali and A.V.S.Anil. 2012. A Novel Approach to Identify Geo-Encryption with GPS and Different Parameters (Locations And Time). International Journal of Computer Science and Information Technologies, Vol. 3(4), 4917-4919.

[10] Techniques used for location based services: A survey, Technical report: CSM-428, ISSN:1744-8050.

[11] Hsien-Chou Liao and Yun-Hsiang Chao. 2008.A New Data Encryption Algorithm Based on the Location of Mobile Users. Information Technology Journal 7 (1), 63-69.

[12] Hatem Hamad and Souhir Elkourd. 2010. Data encryption using the dynamic location and speed of mobile node. Journal Media and communication studies, 67-75.

[13] H. C. Liao, Y H. Chao and C. Y Hsu. 2006. A Novel Approach for Data Encryption Depending on User Location. The Tenth Pacific Asia Conference on Information Systems (PACIS).

[14] Nisha Gholap, Prof S. S. Das and Prof Londhe D N.2013. Location And Authentication Based Encryption Scheme Application Design For Mobile Device. International Journal of Engineering Research & Technology Vol. 2, Issue 4, ISSN: 2278-018.

[15] H.Liao, P.Lee, Y.Chao and C.Chen.2007. Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. 9th International

Conference on Advanced Communicate Technology, 625-626.

[16] Mundt TM.2005. Location dependent digital rights management system.9th International Conference on Advanced Communicate Technology, 625-628.

[17] H.Hamad and S.Elkourd.2010. Data encryption using the dynamic location and speed of mobile node. Journal Media and Communication Studies, Vol. 2,67-75.

[18] Hatem Hamad and Souhir El Kourd.2012. Key strength with encryption and dynamic location of mobile phone. 6th International Conference on Sciences of electronic, technologies of information and telecommunications, 468-473,doi: 10.1109/SETIT.2012.6481958.

[19] Muhammad Waseem Khan.2013.SMS Security in Mobile Devices: A Survey. Int. J. Advanced Networking and Applications Volume: 05, Issue: 02,1873-1882, ISSN: 0975-0290.

[20] Gurjeet Kaur and Monika Sachdeva.2012. Implementation of Secure Authentication Mechanism for LBS using best Encryption Technique on the Bases of performance Analysis of cryptographic Algorithms. International Journal of Security, Privacy and Trust Management, Vol.1, No 6.

[21] Michael Spreitzenbarth, Sven Schmitt and Felix Freiling. 2012. COMPARING SOURCES OF LOCATION DATA FROM ANDROID SMARTPHONES. 8th IFIP WG 11.9 International Conference on Digital Forensics, Pretoria, South Africa, January 3-5.