IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 19-26
www.iosrjournals.org

A Generalized Study on Encryption Techniques for Location Based Services

Y. Lakshmi Prasanna[1], Prof. E. Madhusudhan Reddy[2]
[1]*(Department of CSE, Research Scholar, JNTUH, Hyderabad, India)*
[2]*(Department of IT, Madanapalle Institute of Technology & Science,Madanapalle,India)*

Abstract: *Location-based service (LBS) is the concept that denotes applications integrating geographic location (i.e., spatial coordinates) with the general notion of services. Examples of such applications include emergency services, car navigation systems, tourist tour planning etc. The increasing spread of location-based services (LBSs) has led to a renewed research interest in the security of services. To ensure the credibility and availability of LBSs, the needed requirement is to address access control, authentication and privacy issues of LBSs. In this paper a study of the encryption techniques used for ensuring the security of location-based services (LBSs) is done. According to our discussion, the approach can meet the confidentiality, authentication, simplicity, and practicability of security issues. As a result, the proposed encryption techniques can also meet the demands of mobile information systems.*

Keywords: *Cryptography, Data Security, Location-based encryption, Location-based Services, Trusted Location Devices*

I. Introduction

Location-based services can be defined as the services that integrate a mobile device's location or position with other information so as to provide added value to a user. Location-based services have a long tradition since the 1970s, the U.S. Department of Defense has been operating the global positioning system (GPS), a satellite infrastructure serving the positioning of people and objects. Initially, GPS was conceived for military purposes, but the U.S. government decided in the 1980s to make the system's positioning data freely available to other industries worldwide. Since then, many industries have taken up the opportunity to access position data through GPS and now use it to enhance their products and services. For example, the automotive industry has been integrating navigation systems into cars for some time.

In traditional positioning systems, location information has typically been derived by a device and with the help of a satellite system (i.e., a GPS receiver). However, widespread interest in location-based services (LBS) had started to boost only in the late 1990s, when a new type of localization technology and new market interest in data services was sparked by mobile network operators. In approximately 1997, mobile networks were widely deployed in Europe, Asia, and the United States, and income from telephony services had proven to be significant to mobile operators. Yet, even though mobile voice services continue to be a major revenue generator for telecommunications, growth of mobile telephony is limited and the price per minute is decreasing. Consequently, operators have started to look around for means to stabilize their bottom line and find new areas for future growth. One major way is to offer data services, many of which will be location enhanced.

In LBSs, the location of a device, representing one of most important contextual information about the device and its owner, is exploited to develop innovative and value-added services to the user's personal context. Many individual, commercial and enterprise-oriented LBSs are already available and have gained popularity. Analysts project revenues for LBSs to grow from $2.8 billion in 2010 to hit a $10.3 billion by 2015. The increasing popularity of LBSs has led to a renewed research interest in location-based security.

Traditional encryption is used to provide assurance that only authorized users can the secure content. However, it would still be useful to have an additional layer of security that provides assurance that the secure content can only be used at authorized location and time. Location-based encryption can be used to ensure security so that data cannot be decrypted outside a particular facility, for example, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location. The term "location-based encryption" is used here to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system.

Adding security to transmissions uses location-based encryption to limit the area inside which the intended recipient can decrypt messages. The latitude/longitude coordinate of the target node can be used as the key for the data encryption. When the target coordinate is determined, using GPS receiver, for data encryption, the ciphertext can only be decrypted at the expected location. A guiding principle behind the development of cryptographic systems has been that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, only that they be designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithm so that the best attack requires an exhaustive search of the key space, and using sufficiently long keys that exhaustive search is infeasible.

The essential task of data security is to prevent any unauthorized third party from revealing or modifying the data. Confidentiality can be achieved by using encryption, while data integrity can be achieved by using digital signatures and/or MAC. During transmit the data can be protected by using protocols such as SSL and IPSec. Meanwhile, at the storage the data confidentiality can be achieved using user encryption schemes. Stream ciphers are widely used to protect sensitive data at fast speeds. Although block ciphers have been attracting more and more attention, stream ciphers still are very important, particularly for military applications and to the academic research community. Stream ciphers are more suitable in environments where tight resource constraints are applied, i.e. in wireless mobile devices, or wireless sensor networks. When there is a need to encrypt large amount of streaming data, a stream cipher is preferred.

II. Literature Review

Before discussing the encryption techniques for location based services, a review of some cryptographic terms, concepts and algorithms is provided.

1. Review on Cryptographic Concepts

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

The basic goal of most cryptographic system is to transmit some data, termed the plaintext, in such a way that is cannot be decoded by unauthorized agents. This is done by using a cryptographic key and algorithm to convert the plaintext into encrypted data or cipher text. Only authorized agents should be able to convert the cipher text back to the plaintext. A cryptographic algorithm, also called cipher, is used to perform the transformation. The cipher is a mathematical function that used for encryption and decryption. There are two general types of key-based algorithms: symmetric and asymmetric (or public-key). Symmetric algorithms are the algorithms where encryption key can be calculated from decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same as shown in Fig.1. These keys are often called session keys. Public-key algorithms are designed so that the keys used for encryption and decryption are different as shown in the Fig. 2. These keys cannot be mutually derived i.e. one cannot derive the decryption key from the encryption key. The encryption key is often called the public key and the decryption key is called the private key.

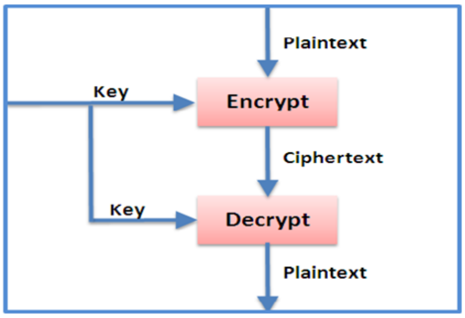


Fig. 1 Symmetric Algorithm

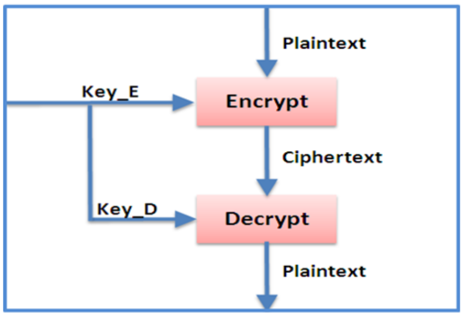


Fig. 2 Asymmetric Algorithm

The most widely used symmetric algorithms are DES, Triple-DES and AES. There are two reasons why public-key algorithms are not used interchangeably with symmetric algorithm. First, public-key algorithms are slow, about 1000 times slower than the symmetric algorithms. Second, the public-key cryptosystems are vulnerable to chosen-plaintext attacks. Therefore, in most practical implementations, public-key algorithm is used for key management, to secure and distribute session keys. The plaintext is encrypted using symmetric algorithm. This is called a hybrid algorithm. Here, a random key, sometimes called the session key, is generated by the originator and sent to the recipient using an asymmetric algorithm. This session key is then used by both parties to communicate securely using a much faster symmetric algorithm. The hybrid approach has found wide application, most notably on the Internet where it forms the basis for secure browsers (Secure Socket Layer (SSL)) and secure e-mail.

Authentication is another important concept in cryptography. It allows the receiver of a message to ascertain its origin. Authentication is not necessarily used in encryption or decryption protocols but it is a key concept in verifying the source of a message. It will be used for signal authentication. Hash functions are a fundamental building blocking for many of the authentication protocols. A hash function is a function that takes a variable length input and converts to a fixed length output, called hash value or hash digest. Hash functions are relatively easy to compute but significantly harder to reverse. Beside one-way-ness, the other important property of hash functions is collision-free: It is hard to generate two inputs with the same hash value. A Message Authentication Code (MAC) also known as data authentication code (DAC) is a one-way hash function with the addition of a key. The hash value is function of both of the input and the key. Unlike encryption, authentication doesn't hide the plaintext but tag the MAC at the end of the plaintext for the recipient to verify whether the plaintext has been modified on the way of distribution.

Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control relies on and coexists with other security services in a computer system. Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation. Authorizations in this database are administered and maintained by a security administrator. The administrator sets these authorizations on the basis of the security policy. Users may also be able to modify some portion of the authorization database, for instance, to set permissions for their personal files. Auditing monitors and keeps a record of relevant activity in the system. It is important to make a clear distinction between authentication and access control. Correctly establishing the identity of the user is the responsibility of the authentication service. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor

III. Encryption Techniques for Location-based Services

1. The Geo-Encryption Algorithm

Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing.

In principal, one could cryptographically bind or attach a set of location and time specifications to the cipher text file and build devices that would decrypt the file only when the user is within the specified location and time constraints. However, this approach presents potential problems: the resultant file reveals the physical location of the intended recipient. The military frowns on this sort of things at least for their own forces. Furthermore, it provides vital information to someone who wants to spoof the device.

As another possibility, one could use location itself as the cryptographic key to another strong encryption algorithm such as AES. This is ill advised in that location is unlikely to have sufficient entropy (that is uncertainty) to provide strong protection. Even if an adversary does not know the precise location, enough information may be available to enable a rapid brute-force attack analogous to a dictionary attack. For example, suppose that location is coded as a latitude-longitude pair at the precision of one centimeter and that an adversary is able to narrow the latitude and longitude to within a kilometer. Then there are only 100,000 possible values each for latitude and for longitude, or 10 billion possible pairs (that is, keys). Testing each of these pairs would be easy. Applying an obfuscation function to the location value before using it as a key could strengthen this approach. However, the function would have to be kept secret to prevent the adversary from doing the same. In general, security by obscurity is scoffed at because once the secret method is exposed, it becomes useless.

The purpose of Geo-encryption is to provide security to the transmission of information. As such, it is important that every linkage of the Geo-encryption chain is secure. This includes not only the protocol itself but also the broadcast of RF signal. The security of the RF navigation signal is provided by message authentication. Authentication is about the verifying the source of the data/messages. One goal is to prevent the user from being fooled into believing that a message comes from a particular source when this is not the case. Another goal is to allow the receivers to verify whether the messages have been modified during transmission.

GeoEncryption algorithm addresses these issues by building on established security algorithms and protocols. Referring to Fig. 3, this approach modifies the previously discussed Hybrid algorithm to include a GeoLock. On the originating (encrypting) side, a GeoLock is computed based on the intended recipient's Position, Velocity, and Time (PVT) block. The PVT block defines where the recipient needs to be in terms of position, velocity & time for decryption to be successful. The GeoLock is then XORed with the session key (Key_S) to form a GeoLocked session key. The resultant is then encrypted using an asymmetric algorithm and conveyed to the recipient. On the recipient (decryption) side, GeoLocks are computed using an AntiSpoof GPS receiver for PVT input into the PVT→GeoLock mapping function. If the PVT values are correct, then the resultant GeoLock will XOR with the GeoLocked key to provide the correct session key (Key_S).

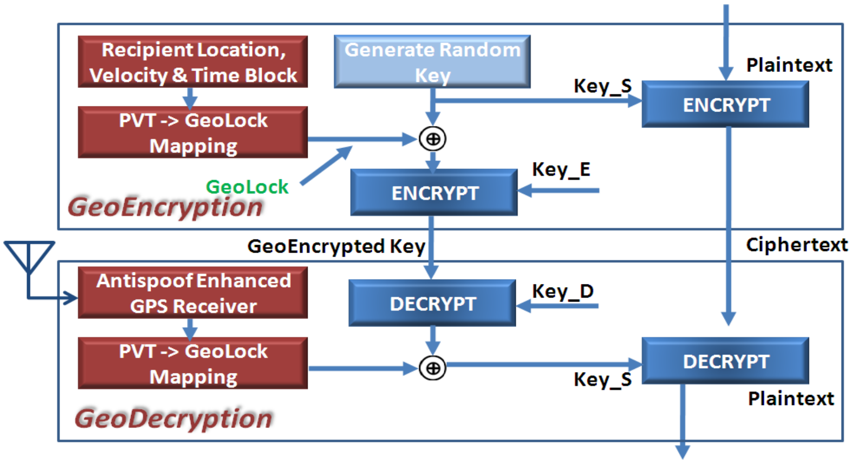


Fig. 3 GeoEncryption Algorithm

Successive Geo-encryption can be used to force data and/or keys to follow a specific geographical path before it can be decrypted. This is achieved by applying multiple geo-locks at the origination node prior to transmittal. As each required node is traversed, one layer of GeoLocking is removed, thus ensuring the desired path has been followed.

2. Location Dependent Encryption Algorithm - LDEA

LDEA is mainly to include the latitude/longitude coordinate in the data encryption and thus to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver. There are two phases: register and operation phases. Firstly, a mobile client requests a random seed and a MAC function C from the information server in the register phase. The information server records the issued random seed and the function C for each individual client. They are very important for ensuring data security in the operation phase. So, they must be transmitted under a secure channel, such as Intranet or VPN (virtual private network). The random seed is the initial value of one-way hash function, such as MD5. A series of session keys is generated according to the random seed. When the mobile client is moving under an insecure channel in the operation phase, the mobile client submits a target coordinate before message transmission. The information server sends the message encrypted by using the coordinate and a specific session key. The session key is changed for every session. Since the information server and the mobile client own the same set of session keys, a key synchronization process is also designed for information server to identify the correct In advance, the register phase and the key synchronization of operation phase is presented in Fig. 4.

When a random seed and a MAC function C is transmitted to a mobile client. The same series of session keys is generated by using a one-way hash function on the both side. One session key K_i is the input of hash function to generate the next key K_{i+1}. The principle of one-way hash function prevents the computation of input value from the output value. Therefore, the usage order of the keys is reversely with the generation direction. When a client starts a new session, a new key is used in the period of the session. So, the key is changed for every session in a reverse order. The transmission is only based on the synchronized session key. The message can be encrypted and transmitted to the mobile client securely.

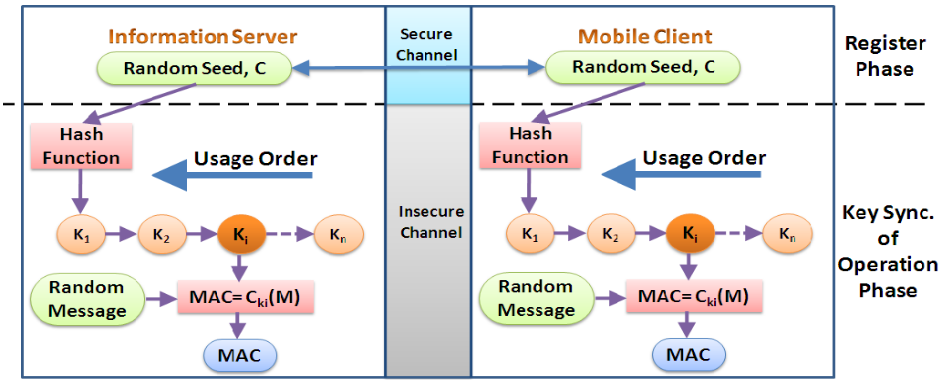
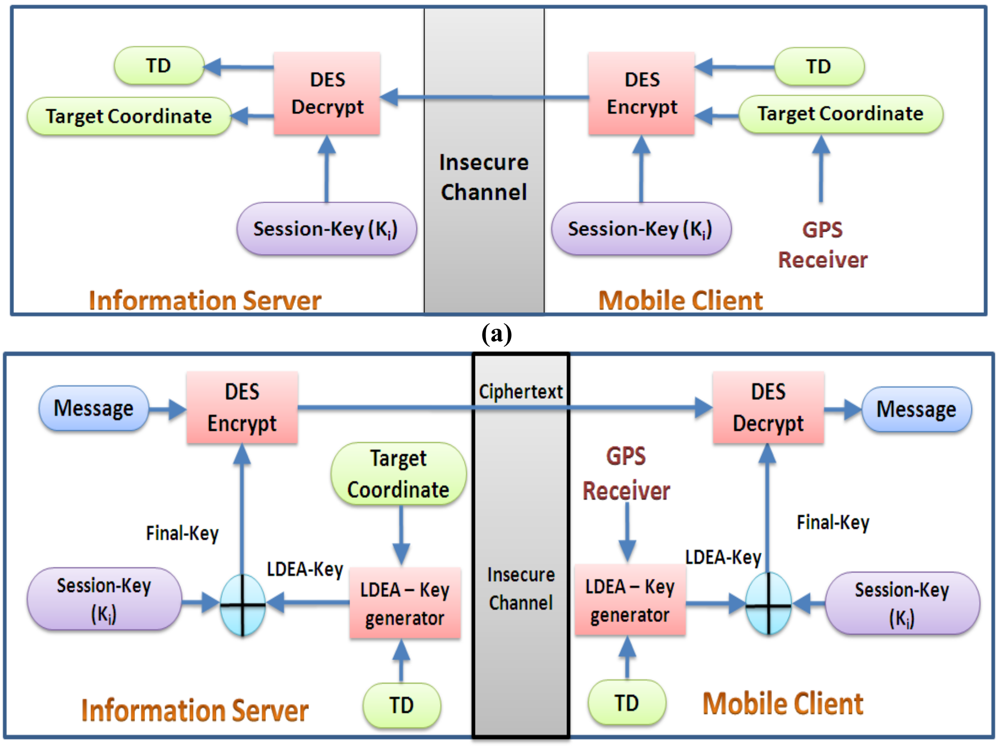


Fig. 4 The process of the register phase and key synchronization of operation phase

The target coordinate submission process is shown in Figure 5 (a) and (b). The mobile client acquires the coordinate from a GPS receiver and assigns a toleration distance (TD). The inaccuracy of the GPS receiver causes the acquired coordinate is difficult to match with a specific GPS coordinate. Therefore, the TD is defined to allow the encrypted message can be decrypted within an area formed by the target coordinate and TD but not a point. TD can be any value such as 10 or 20 meters. When the server receives the coordinate and TD, a LDEA-key is generated. The final-key is generated by exclusive-OR LDEA-key and session key. The message is encrypted by using the final-key. When the mobile client receives the encrypted message, the acquired coordinate from GPS receiver and the known TD is used to generate the LDEA-key. Then the generated final-key is used to decrypt the ciphertext. If the mobile client is within the constraint of the target coordinate and TD, the message can be decrypted successfully. Otherwise, the decrypted message is indiscriminate and meaningless.



(a)

(b)

Figure 5: The process of the operation phase (a) submit target coordinate (b) encrypt and decrypt message

3. Self Encryption

Self-encryption (SE) technique is a light-weight approach which treats the data set as a binary bit stream and generates the keystream by extracting n bits in a pseudorandom manner based on a user's unique PIN and a nonce. The length of the keystream n is flexible and depends on the security requirements. Then the remaining bit stream is encrypted using this keystream and is stored in the mobile device, whereas the keystream is stored separately. It is very difficult to recover the original data stream from the ciphertext even if an adversary has the knowledge of the encryption algorithm. The variable length keystream makes brute force attacks infeasible, and the decrypted data stream is still unrecognizable unless the keystream bits are inserted to the original position.

The sensitive data is broken into two parts using the self-encryption stream cipher scheme. The ciphertext is stored in the mobile device, and the keystream with other parameters is protected in the secure server. The ciphertext is encrypted using the keystream. When the user needs to access the data, he or she has to input a correct PIN to pass the authentication procedure. Then the server will send the keystream to decrypt ciphertext and merge them together to recover the original plaintext. When a mobile device is lost, at most the adversary can access the ciphertext, from which it is computationally infeasible to get meaningful information.

The process of the Self-Encryption scheme is depicted below in the Fig. 6. The seed of the random number generator is calculated by the hash function taking the user's PIN and a nonce as the input. Then, according to the size of the sensitive document and the security level, a sequence of random numbers is generated with length n. By treating the file as a binary stream, this random number sequence indicates which bits in the data file are abstracted to form the keystream. Then the ciphertext is calculated as normal stream cipher does. The ciphertext is stored in the mobile device, the keystream, user's PIN, and the nonce are stored the secure server.

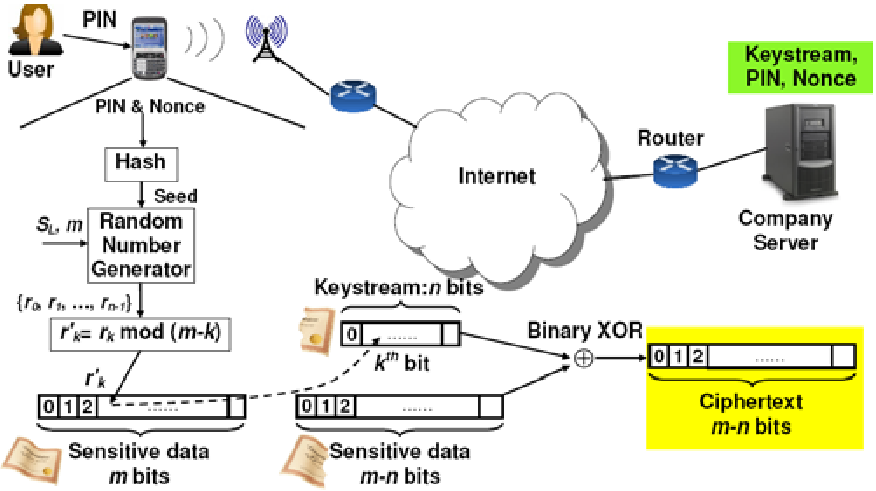


Fig. 6 Self Encryption Algorithm Illustration.

4. Mobile User Location-specific Encryption - MULE

Mobile User Location-specific Encryption (MULE) uses location-specific information from the trusted location to automatically derive a decryption key and allow access to the sensitive files. Once the user is inactive, logs off, or puts the computer to sleep, the files are automatically re-encrypted and the key is deleted from the computer. In the rare case that a user wants to access sensitive files outside the trusted locations, the user can enter a secondary password to gain access. This password based access also provides a fail-safe mechanism in case location specific information or services are no longer available in a trusted location.

MULE's goal is to protect sensitive files on mobile devices with zero user effort in the common case. Standard user login works independent of MULE and provides a form of weak user authentication. All non-sensitive files are left unencrypted and are always accessible. Only user-specified sensitive files are encrypted. Figure 1 depicts an overview of the operation of MULE. When a user tries to access a sensitive file, MULE contacts a Trusted Location Device (TLD) which helps the location-based device to derive the key needed to decrypt sensitive files with zero user effort. The TLD generates a nonce and transmits it over the constrained channel, also called as a location-specific message (m) because the properties of the constrained channel ensure that only devices within the trusted location can access the message associated with the current run of the protocol. A TLD is unable to authenticate requesters without proper access parameters and will respond to any key derivation request. However, the key derivation calculations are such that a TLD produces the wrong output if the requester uses the wrong m in calculations (e.g., the client is in a different location). After the TLD has helped derive the key, the user can access sensitive files without having performed any extra actions. During the rare occasion when a user accesses sensitive files outside of a trusted location, MULE will lack the correct location-specific information and key derivation will fail. In that case, the user is asked to enter a password as part of a location-independent key derivation scheme. The password allows the TPM on the laptop to decrypt a location independent key which can decrypt the files. Once a valid key is available, the sensitive files are decrypted. When a user is idle for some set period of time, logs off, or puts the device to sleep, the device will re-encrypt the files and delete the key.

IV. Requirements And Security Analysis

When location-specific information is used for key derivation, the information must fulfill the following requirements to ensure successful and secure operation of the encryption algorithms which also includes confidentiality, authentication, simplicity, and practicability issues.

1. Requirements for Location-Specific Information Used to Derive Keys

1.1. Easily Accessible: Once the location-based device is placed in a trusted location, and the user is logged in, the device should have access to the information required for key derivation.

1.2. Unique to a Location: If the information is not unique, the location-based device may automatically decrypt a user's files while outside of the originally defined location which is obvious security vulnerability.

1.3. Bounded Range: Location information should only be accessible within the location. Information accessible from outside of a building will apply to more than the location the user trusts.

1.4. Significant Entropy: Information used to derive the key within a location needs to be provided with significant and appropriate encryption procedures so that it is hard to guess. Limited encryption procedures would enable an attacker to guess the necessary values, spoof the location, and recover a key.

2. Security Analysis

2.1 Confidentiality: Only the registered users own a shared key. The server and client must use the same session key for decrypting message successfully. It prevents the ciphertext-only attack.

2.2 Authentication: The users must know the correct session key and the encryption functions in order to preserve the sensitive data which is further submitted to the server. If an attack uses a replay attack, the key synchronization step will be fail since a correct session key cannot be identified. The server will ignore the request from the attacker.

2.3 Simplicity: The encryption algorithms studied uses simple encryption algorithms, exclusive-OR operation and hash functions. Hence these are simple and efficient for executing on the mobile device with limited computing resources.

2.4 Practicability: The mobile information system is an emergent trend in the future. The security strength can still be further improved according to the requirement on the security level. The algorithms studied are practical and satisfies the requirement of mobile information system by incorporating the location into the data encryption algorithm.

V. Conclusion

Securing sensitive and/or private data in mobile communication has been an important topic in security research community. Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information systems, additional layer of security is to be incorporated into the location-based services, which uses the latitude/longitude coordinate as the key of data encryption. Here in this paper, we have studied a few such techniques which protect the data in the location-based services and hence provide security to the location-based services. Analysis of the security issues is also done by using these techniques to provide an effective data transmission between information system and mobile clients.

Acknowledgements

The authors would like to acknowledge and express their heartfelt gratitude to the Swarna Bharathi Institute of Science and Technology [SBIT] Management, Chairman, Director, Principal and Dean R&D. for their vital encouragement, support and facilities providing by them to achieve this task and at they would like to thank Anonymous Reviewers for their valuable suggestions and comments. This paper has greatly benefited from their Efforts.

References

[1] JochenSchiller, Agnès Voisard, Location-Based Services (San Francisco, CA 94111, Morgan Kaufmann Publishers Elsevier).

[2] Logan Scott , Dorothy E. Denning , A Location Based Encryption Technique and Some of Its Applications, Proceedings of the 2003 National Technical Meeting of The Institute of Navigation, Anaheim, CA, January 22 - 24, 2003,734-740.

[3] Hsien-Chou Liao, Po-Ching Lee, Yun-Hsiang Chao, and Chin-Ling Chen, A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security, Proceedings of 9th International Conference on Advanced Communication Technology (ICACT2007), Korea, February 12 - 14, 2007,625-628.

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

[5] Yu Chen and Wei-Shinn Ku, Self-Encryption Scheme for Data Security in Mobile Devices, CCNC'09, Las Vegas, NV, USA, Jan. 10 – 13, 2009,.

[6] H. C. Liao, Y H. Chao, and C. Y Hsu, A Novel Approach for Data Encryption Depending on User Location, The Tenth Pacific Asia Conference on Information Systems (PACIS 2006), 5-9 July 2006.

[7] Dorothy E. Denning and Peter F. MacDoran. Location-Based Authentication: Grounding Cyberspace for Better Security. In Proceedings of the Computer Fraud and Security, Elsevier Science Ltd, February1996.

[8] A. O. Freier, P. Karlton, and P. C. Kocher, The SSL Protocol, Version 3.0, Internet draft, Networking Group, March 1996.

[9] Y. Jiang, C. Lin, M. Shi, and X. Shen, Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 9, Sep. 2006.

[10] A. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, Networking Group, Nov. 1998.

[11] S. Rafaeli and D. Hutchison, A Survey of Key Management for Secure Group Communication, ACM Computing Surveys, Vol. 35, Issue 3, Sept. 2003.

[12] Whitfield Diffie And Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. -22, No. 6, November 1976 ,pp 644-654.

[13] Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, PROCEEDINGS OF THE IEEE,VOL. 67, NO. 3, MARCH 1979,pp 397-427.

[14] A. V. N. Krishna, S. N. N. Pandit, A. Vinaya Babu, A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography Vol. 10 (2007), No. 1, pp. 73–81.

[15] L. Scott, D. Denning, Geo-encryption: Using GPS to Enhance Data Security, GPS World, April 1 2003.

[16] A. Al-Fuqaha, O. Al-Ibrahim, Geo-encryption protocol for mobile networks, Journal of Computer Communications 30 (2007), pp 2510–25.

[17] PrasadReddy.P.V.G.D, K.R.Sudha and S.Krishna Rao, Data Encryption technique using Location based key dependent Permutation and circular rotation, (IJCNS) International Journal of Computer and Network Security, Vol. 2, No. 3, March 2010 pp46-49.

[18] Prasad Reddy.P.V.G.D, K.R.Sudha and S.Krishna Rao Rao, Data Encryption technique using Location based key dependent circular rotation, Journal of Advanced Research in Computer Engineering, Vol. 4, No. 1, January-June 2010, pp. 27 – 30.

AUTHORS PROFILE

Mrs. Y. Lakshmi Prasanna, working as an Associate professor in the Department of Computer Science and Engineering, pursuing her Ph.D. in Computer Science and Engineering from JNTUH, Hyderabad. Her research areas include Network Security, Computer Networks, Mobile Computing and Data Warehousing and Data Mining.

Dr.E.Madhusudhana Reddy, working as a Professor in the Department of Computer Science & Engineering. His areas of specialization include Cryptography & Network Security, Biometrics, Data Mining and Warehousing, Artificial Intelligence & Neural Networks and Human Computer Interaction.