Survey on Data Security for Mobile Devices

Nisha P Gholap
KJ College of Engineering and Management Research, Pune University

Mandar Mokashi
KJ College of Engineering and Management Research, Pune University

Soumitra S Das
KJ College of Engineering and Management Research, Pune University

ABSTRACT
Nowadays data security is making a way into market. New techniques of data security have gained interest of many researchers. Encryption-Decryption technique is one such way of data security. These techniques not only provide confidentiality, integrity of data but also help in authentication of user. Authentication is possible because encryption-decryption of the data is only possible with the legitimate key possessed by legitimate user only. In this paper we study different technique used in encryption method so to increase security of data especially location based encryption and decryption process.

Keywords
Data security, Encryption-Decryption, Confidentiality, Integrity, Authentication, Legitimate, Location based

1. INTRODUCTION
Years ago apart from valuable jewelries, money, antique materials no other things were given much priority for security reasons. Later it became necessary for message security especially during wars and territory assignment. This necessity gave rise to so called confidentiality, which means that the message should only be disclosed to legitimate users and no other people. For this we had to verify the user if is legitimate or not thus giving rise to authentication. Attacks took place, capturing confidential messages took place and till today every person is still striving hard to make his data more and more secure. Today what is changed is the approach towards security, techniques and mechanism of security all of which have science and mathematics base for it. Today what is more important is the complexity to achieve the data by unauthorized user, to extract the message and to transfer the data securely. Technologies have developed to make things more comfortable for us in an era of wireless communication. Every data or communication is taking place through this media not only this but today it is also possible to store data to a location apart from user and access this data when ever required. Wireless, wired data transfer, remote storage of data, exploitation of others data, theft of devices, hacking of data all these factors increased more concern for data security, thus leading to increase in security measures and their research. Recent techniques for data security give more emphases on factors such as ease of data access to authorized users, infeasibility to unauthorized users for data access, complexity in encryption decryption and achievements of all security goals.

Mobile devices have become popular in the community for the ease it provides to the user, it's not only a way of communication but a technology which can help to store, transfer data. Important aspect which we cannot neglect is m-commerce which is now getting a hike in business. All of these benefits have raised the chances of theft to the devices and the data stored in it. Security has become great concern to the users as well as business which make use of such devices. In business world information is the most important part and always should be handled with care. In such circumstances it becomes a need to secure the data in industries or companies from falling into wrong hands. A step towards security today is that companies or industries restrict the use of personal mobile devices for work purpose to their employees. To overcome this problems location based scheme tries to build in the security assuring for mobile devices, so that the users can freely use their mobile devices to store and transfer data without bothering about data security.

2. SURVEY
Rohollah Karimi and Mohammad Kalantari in their paper, try to apply position and time into the encryption and decryption processes so that provides an additional layer of security and present a modified geo-encryption protocol that will allow mobile nodes to communicate to each other safely by restrict decoding a message in the specific location and time period. The recipient can decrypt messages if he stays in specific area and limited time.

Mobile fund transfer, e-commerce, e-wallet and theater booking all these applications should make use of strong encryption techniques for data security. Because mobile devices have low-computation capabilities and limited battery life, it is not suitable to use conventional asymmetric cryptographic techniques, with them. On the other hand, most of the data encryption technology is location-independent and cannot restrict the location of data decryption. This paper, try to present a modified geo-encryption protocol and improve its efficiency. Furthermore consider all types of possible attacks to the Geo protocol and propose some solutions to deal with them [1].

A geo-mapping function is employed during encryption process to combine the recipient's geographic location, time and an encryption key to produce geo-secured key for transmission with message. The message can only be decrypted if the recipient is physically positioned at considered location. Geo-mapping function creates geo-tag value by using position-velocity-time (PVT) to this function which latitude, longitude and time constitute the inputs. Geo-tag value is used to generate geo-secured key from session key and recover session key from geo-secured key. Model takes advantage of GPS technology and it's suitable for mobile device, which has low-computation capability and short battery life [1]. The strongest of key depends on the current receiver's location and DTD. Therefore, the probability to break the secret key is impossible because no one knows the estimate coordinate since it is not yet at this position. Also DTD can be a fractional number with small interval which makes the key more secure. The geo-tag key is incorporated by the secret key which makes the final key very strong. Current design of our algorithm is based on the MD5 hash and DES algorithm.

Dhanraj, C. Nandini, and Mohd. Tajuddin presented a new block cipher symmetric key algorithm named as "Improved extended Data Encryption Standard". This proposed system is implemented based on thread process concept. A single process might contains multiple threads; all threads within a process share the same state, same memory space, and can communicate with each other directly, due to the shared variables It is unique independent approach which uses several computational steps along with string of operators and randomized delimiter selections using XOR operator [2]. Benefits of using XOR operator is, easy to implement with small code and good secure against attacks (only if key length == string length). Improved Extended Data Encryption Standard is specially designed to produce different cipher texts by applying same key on same plaintext. The Algorithm is successfully implemented on text file, corresponding image and audio files. The improved extended DES is one of the best performing partial Symmetric key algorithms among the other symmetric key algorithms like DES, AES particularly for the text message with limited file size [2].

The proposed system has been implemented based on thread concept.

Encryption:
The file content is read from input i.e. plaintext. The input is subjected to transposition process, then to substitution along with binary operations. Each character from the modified text file is read and their ASCII value is determined. Binary equivalent of ASCII value is calculated in 32- bit format and stored as a binary string. The next step involves performing a set of mathematical operations, using operators from the operator string over the bits, using the secret key. The secrecy of operators used above is maintained by encoding the operators from the look-up table. The corresponding character of the generated random number is added to code sequence. To make the code sequence more secure a suitable encrypted methodology is applied. From a predefined stack, a random delimiter is chosen and added at the end of the modified secure code sequence [2].

Decryption:
The first character from cipher text is read and then its corresponding ASCII value is calculated. The key is examined and the character before the delimiter in the modified secure code sequence is verified. Similar mathematical operations are performed on this character. The modified secure code sequence is required to decode and inverse operation for each and every character is required to perform. The inverse of the corresponding binary operation is applied. Then the reverse substitution method is performed. Then the reverse transposition is performed.

The proposed method has been implemented based on multi threading concept, which helps in efficient utilization of CPU. Hence encryption and decryption time is very optimum as compared to existing methods.

Table 1: shows the time (seconds) required for encryption and decryption of text file of size 2765 bytes [2]

Algorithm	Input Text file	DES	AES	PRPOSED
Encryption	2765 bytes	2.30	2.78	1.06
Decryption	2765 bytes	2.5	3	1.04
Total	2765 bytes	4.8	5.78	2.10

The following table shows that memory requirement of proposed system is lesser as compared to existing system. Basically the encryption time increases as the key length increases.

Table 2: Shows Memory Space Requirement [2]

Algorithm	Key length (bits)	Plain text (bits)	Cipher text (bits)
DES	56	64	64
AES	128	128	128
PROPOSED	32	32	32

In case of proposed method, different cipher texts are produced making it immune to brute-force attack, cryptanalysis attack, man-in middle attacks and thus enhancing the security level. Also memory and time requirement is less.

In paper by Hsien-Chou Liao and Yun-Hsiang Chao proposed technology is designed to meet the demand of mobile users in the future, a location-dependent approach, called location-dependent data encryption algorithm (LDEA), is proposed in this paper.

A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for data encryption. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receive is inaccuracy and inconsistent. The location of a mobile user is difficult to exactly match with the target coordinate. A toleration distance (TD) is also designed in LDEA to increase its practicality. The security analysis shows that the probability to break LDEA is almost impossible since the length of the random key is adjustable. The results show that the cipher text can only be decrypted under the restriction of TD. It illustrates that LDEA is effective and practical for data transmission in mobile environment [3].

LDEA provide a new function by using the latitude/longitude coordinate as the key of data encryption. A toleration distance (TD) is also designed to overcome the inaccuracy and inconsistent of GPS receiver. The security strength of LDEA is adjustable when necessary

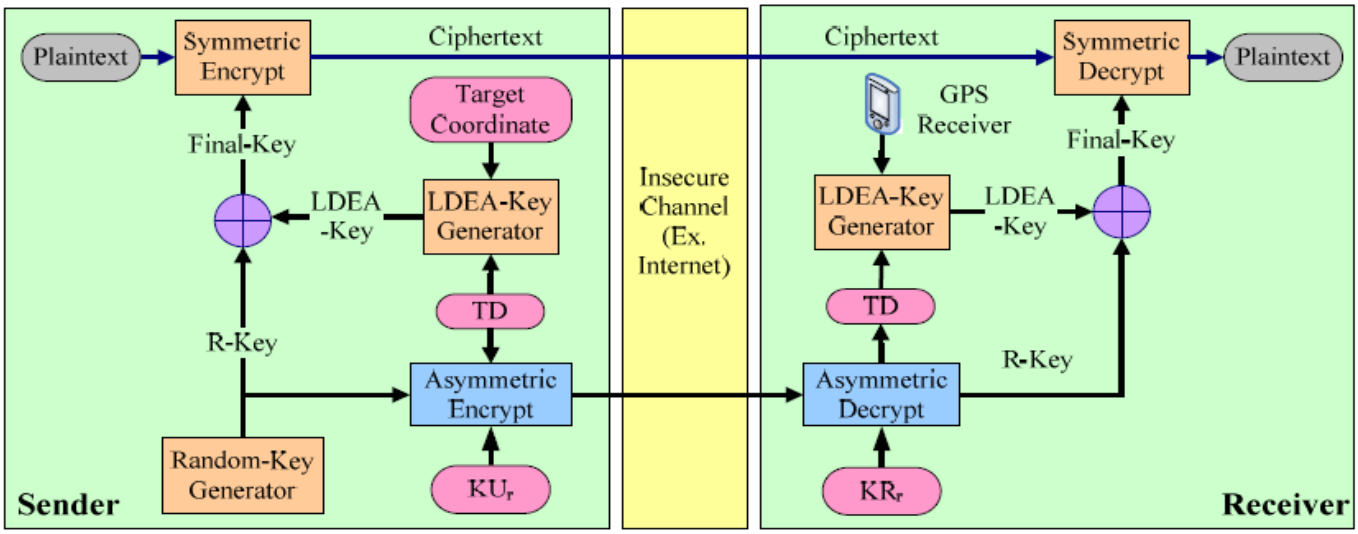

Figure 1 Shows encryption and decryption put forth by Hsien-Chou Liao and Yun-Hsiang Chao [3]

Figure 1 shows two keys KUr and KRr which are public and private keys from the receiver side, KUr and TD is send by the receiver to the sender. Later TD and a random key is transmitted by using asymmetric encryption then using target co-ordinate ,TD(combination of which form LDEA) as well as random key send by the receiver a final key is formed which is used for encryption of message. When this message reaches the receiver he needs to XOR his location received from the GPS (in terms of latitude/longitude) with the random key which he has, he then successfully retrieve the key and decrypt the message if he is in the intended location by the sender.

The process for GPS co-ordinate acquisition described by Hsien-Chou Liao and Yun-Hsiang Chao is that the readings are in the format of types WGS84(world geodetic system in 1984) defined in NMEA(National Marine Electronics Association) specification. Example “E 12134.5971” means 121 degree and 34.5971 min east longitude and “N 2504.7314” means 25 degrees and 4.7314 min north latitude [3]. These coordinates are multiplied with 10000 to form an integer form and then divided with the value of tolerable distance known ad TD.in addition to that the answer or the ultimate co-ordinate form generated is padded with either zero or one to determine its east/south or north/west direction.

During Xor-ing of coordinate and random key MD5 hash algorithm is used to generate the digest this makes the key more secure form crypt analysis. Symmetric encryption done is using DES algorithm but this method is flexible enough to accommodate new encryption algorithm [3].

Secondly we studied an approach described by Hsien-Chou Liao and Po-Ching Lee in which location information is incorporated into data transmission for mobile information system [8]. Approach is divided into two sub-parts first describing register phase and second operation phase. The former sub-part consist of acquiring random seed and MAC function C from information server by the mobile client under a secure channel such as Intranet or VPN. Information server maintains details about random seed and MAC function C for every client. Random seed is the initial value of one way hash-function, such as MD5 which is used to generate number of session keys [8]. Different session keys are used for different session depending on random seed. If Mobile client is under insecure channel he only needs to submit his target location coordinates to information server before message transmission the server then sends the message in encrypted form to the co-ordinate prescribed with the specific session key. Whenever mobile client is under secure channel it sends request for a new random seed and new MAC function C for future session key formation.

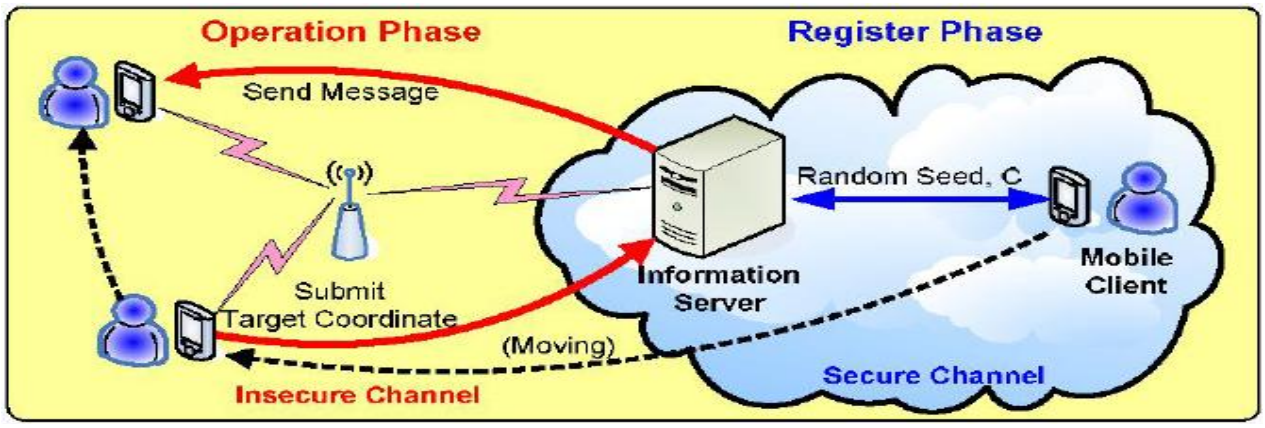

Figure 2 shows the registration phase proposed by Hsien-Chou Liao and Po-Ching Lee [8]

Every Nth session key is required to generate N+1 session key. For security purpose session keys are use in inverse order to the order in which they are generated. Both information server and the client side use the same session key generated using the hash function thus incorporating the need of synchronization process. Using the MAC function key synchronization is checked, if the MAC function generated over the server side is matching to the client side MAC then we can conclude that synchronization is correctly executing. Then the server can anytime encrypted and send the message to the mobile client [8].

Key generation described by Hsien-Chou Liao and Po-Ching Lee in there paper is by XOR-ing session key and LDEA (GPS co-ordinate + TD) this lead to final key formation using which server encrypts the data. On the other-side when client receive this message it first need to obtain his GPS co-ordinate add to it the TD value which form LDEA later XOR-ing with the session key he generates the final key which can be used for the decryption [8]. Client can successfully decrypt the message only if he is in the TD area else he cannot. These constraints can provide confidentiality, authentication, simplicity and practicability according to Hsien-Chou Liao and Po-Ching Lee. Approached used by them use MD5 has and DES algorithm. This approach can be extended for authorization of mobile software using location based constraints [8].

Traditional encryption technology cannot restrict the location of mobile users for data decryption. In order to meet the demand of mobile users in the future, for more security LDEA algorithm is proposed.

Similarly in paper proposed by Hatem Hamad and Souhir Elkourd proposes a new method of message security by using the coordinates in GPS service, where it can specify the path of movement by taking some coordinates during travel of mobile node MN and estimate the following situation of MN in a constant time interval. This new estimated coordinate is applied in our secret key. Dynamic Toleration Distance (DTD) is also designed in our key to increase its practicality. The security analysis shows that the probability to break this key is almost impossible due to the security of coordinates and DTD, and adjusting the length of the Random key. Experimental study shows that the cipher text can only be decrypted under the restriction of DTD.

The paper proposes a new method of key security where the receiver MN registers some coordinates and speed during the travel. This new estimated coordinate is applied in our secret key. Dynamic Toleration Distance (DTD) is also designed in our key to increase its practicality. The security analysis shows that the probability to break this key is almost impossible due to the security of coordinates and DTD, and adjusting the length of the Random key. The receiver MN determines the DTD and the sender can decrypt the cipher text within the range of DTD[4]. This algorithm is very strong, since we use a function path that applies the estimate coordinate, we also use a dynamic tolerance distance (DTD), and velocity of MN. This parameter and the type of movement make our system more secure than the static encryption, which depends only about on a position of MN and static tolerance distance. The static location protocol is simple however; its performance varies with the mobility of the mobile [4].

The static location protocol is simple however; its performance varies with the mobility of the mobile. Specifically, if a MN is moving quickly, the error to detect region of encryption will be high. That means the successful rate of decryption is 0% even if the distance and static tolerance distance are equal to zero; if it is moving slowly, the error will be low and the successful rate of decryption augmented, but the dynamic location in this protocol will be more accurate. Thus, when the MN is moving fast, localization will be carried more precisely. When it moves slowly and the successful rate of decryption decreases in the two cases, but in high speed it gives better result than low speed as shown in our results The results also show that the region of decryption is less because the range of DTD is small, where the successful rate is probably narrow[4].

Self-encryption (SE) scheme means encrypting the data by key stream generated from randomly extracted bits from the stream. The most challenging part of mobile device data protection is limited computing power, storage space, and battery lifetime, a light-weight rather than computing intensive and complex encryption algorithm is desired in the mobile devices. In addition, portability makes mobile devices prone to being stolen or lost. It is very challenging to protect the weakly encrypted information on a mobile device, which might end up in the hands of an adversary, to break the encryption while it should be computationally infeasible for adversaries to decrypt the data. This paper proposes a novel data encryption and storage scheme to address this challenge.

Approach followed is:

1) Setting up connection with the remote server.

2) Retrieving the key stream and nonce for local decryption.

3) Generating a new key stream with a new nonce and encrypting the document.

4) Transmitting the updated key stream and new nonce back to server.

Treating the data set as a binary bit stream, we generate the key stream by extracting n bits in a pseudorandom manner based on user's unique PIN and a nonce. The length of the key stream is flexible and depends on the security requirements. Then we encrypt the remaining bit stream using this key stream. The encrypted remainder is stored in the mobile device, whereas the key stream is stored separately. It is very difficult to recover the original data stream from the cipher text even if an adversary has the knowledge of the message, and the length of the message body decreases as bits are abstracted , the pointers to the key stream bits need to be normalized following the changing message size. Hence it becomes complex. Therefore instead of abstracting the bits from message we can copy the bits to from key stream, thus reducing the complexity. It enables legitimate user to enjoy the security of data, high efficiency and convenience brought by mobile devices. User can use the service within the territory of the server [5]. But paper by Paolo Gasti & Yu Chen presents Breaking and Fixing the Self Encryption Scheme hence limiting its use [6]. Thus we could say that Mobile service raises a number of security and privacy challenges. To address this, we need to present an approach in which the mobile information security is enhanced [7].

3. CONCLUSION

Thus study of different encryption strategies emphasize on confidentiality of data. In addition to the security aspect mobility and availability of data is given importance in above papers. For a mobile user his data should be readily available wherever possible with security and hence location oriented security has been put up. It also helps in authentication of user

based on his location for data reception. In location oriented security more important is the way data is encrypted and the way it will be decrypted under specific constraints. These constraints require mathematical calculations and desirable predictions to be made which have been stated in a good way in papers studied above.

4. ACKNOWLEGMENT

A special thanks to my guide Prof Mandar K. Mokashi and co guide Prof Soumitra S Das who gave me best of their support in my paper work . I am also thankful to Prof Mininath Nighot and Dr S.J Wagh for the motivation that they gave me.

5. REFERNCES

[1] Rohollah Karimi and Mohammad Kalantari, IEEE confrence paper year 2011, Enhancing Security and Confidentiality on Mobile Devices by Location-based Data Encryption.

[2] Dhanraj, C. Nandini, and Mohd. Tajuddin (International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, August 2011, ISSN: 2079-2557). An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard

[3] Hsien-Chou Liao and Yun-Hsiang Chao Information Technology Journal 7 (1): 63-69, 2008 ISSN 1812-5638 © 2008 Asian Network for Scientific Information A New Data Encryption Algorithm Based on the Location of Mobile Users

[4] Hatem Hamad and Souhir Elkourd Journal Media and Communication Studies Vol. 2(3)pp. 067-075, March, 2010, Data encryption using the dynamic location and speed of mobile node

[5] Yu Chen and Wei-Shinn Ku Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE Publication Year: 2009, Self-Encryption Scheme for Data Security in Mobile Devices.

[6] Paolo Gasti & Yu ChenParallel, Distributed and Network-Based Processing (PDP), 2010 18th Euromicro International Conference on 17-19 Feb. 2010, Breaking and Fixing the Self Encryption Scheme for Data Security in Mobile Devices.

[7] TieJun Pan LeiNa Zheng Management of e-Commerce and e-Government 2008, A New Mobile Information Security Solution Based on External Electronic Key.

[8] 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