Securing Data with Encryption and Color Encoding Scheme for Mobile Device

Nisha P Gholap
KJCOEMR, Pune University

Mandar Mokashi
KJCOEMR, Pune University

Soumitra S Das
KJCOEMR, Pune University

ABSTRACT
Today most data is stored & transferred from mobile device like laptops. These devices are prone to theft, also we transfer the data via network which is not secured. All above reasons forms the backbone for our paper which implements an encryption scheme and color encoding for such mobile devices; it uses location based key formation. This key is used to encrypt data will ACIII value of Cipher text is used in color encoding of the encrypted data. This color encoded document can be saved as jpeg, jpg and send in a secure manner as an e-mail attachment

Keywords
Encryption scheme, Color encoding, Location based key.

1. INTRODUCTION
Data security is a concept which is gaining a boom in research area, as it's a need of every individual to have his information in feasible and safe manner. Securing the data from unauthenticated user can be easily done using password access to the digital data, but it's highly impossible to avoid mischievous attack when the authentication breaches. Today almost all the people store their important data in digital format for quick accessibility and mobility thanks to many factors such as cloud where the data can be stored with security ,internet due to which data can be accessed anywhere-anytime and compact computing devices which can fit into pockets and provide mobility. Thus the enhancement of technology has not only brought us in digital era but made it pretty sustainable for upcoming years, but as with pro we have cons there is a problem of data security raising its head. It was easy in the times when our important data was sealed, documented and kept in a lock and key security but today for availability, mobility, ease and comfort we require data conversion to digital format. This digital data is to be made secure from the unintended users who might hack our computing device for mischievous data usage. Also the chances of theft to our mobile computing devices have increased which adds on to the problem of data security. Whenever a device is lost the data stored in it which might be received or transferred data is lost hence it not only a case of device theft but also the case of data theft. Considering these problem many companies avoid employee's mobile device usage for company data transfer and storage. Today the main concern is for data that is transferred to be secure as the other end user might not be the legitimate user. To overtake this problem this paper presents an encryption scheme which is enhancing its security by using dynamically changing security key based on location. This paper presents this scheme for mobile cell phones as well as for the personal computers which have mobility.

2. LITERATURE SURVEY
Smartphone's, PDAs, laptops, tablets and other types of devices are ubiquitous; they improve productivity and flexibility for individuals and employees .Almost everyone who has a Smartphone or PDA uses it for both personal and business purposes which sometimes may be subject to privacy [9]. When it comes to security part there is a huge list of expectations that should be fulfilled to be called as secure. Security not only means authentication & through access control but it also means easy access control to authenticated user with no hindrance in availability. Many a times it so happens that even if the authentication is through miss handling of devices lead to data loss, example even if the device is secured with a password it might happen that the password is entered and the authenticated user leaves the devices alone for some times in this duration any unauthenticated user might misuse the data in it. Thus this forms an unseen part of security system where more emphasis on data encryption should be given. Data encryption is a part of cryptology where the data or important information is converted into not understand able format know as cipher text this cipher text is reversed and converted back to sensible data by use of decryption technique. The cryptography system has 3 main points to be noted while in use first is substitution/transposition, second is the number of keys used and last is the method of encryption i.e either blocks encryption or stream encryption [1]. Further it is also classified as symmetric & asymmetric depending on single key used or more key used respectively. Depending on the way of encryption strategy it is also classified as block cipher or stream cipher. Block cipher technique uses block of plain text to be processed and produces cipher text of same length it uses same key to encrypt and the cipher block is not depended on preceding blocks. Stream cipher technique performs a bit or one byte encryption of plain text the cipher text is depended on many preceding byte ciphers and key. Data Encryption Standard (DES) require plain text and a key as input, key should be of length 56 bits and plain text block of 64 bits. The execution takes place in 3 phases permutation phase, second is 16 rounds consisting combination of permutation and substitution function, third is inverse permutation. DES forms one technique for data security but due to its complexities it so happens the it tends to consume more battery in mobile devices. Along with it to carry out encryption over personal computer it takes long time as every block is executed serially. To enhance its performance Dhanraj, C. Nandini in his paper presented an 'Improved extended Data Encryption Standard'[2]. This proposed system is implemented based on thread process concept. Improved Extended Data Encryption Standard is specially designed to produce different cipher texts by applying same key on same plaintext. 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 but as known most of symmetric key algorithm has key distribution problem. Another approach to encrypt the data is to use self encryption technique which uses message stream bits for key formation by randomly selecting them from message and reduces the message length. The length selection is totally depended on user's security requirement [3]. As per the self encryption scheme the encrypted data and the key are stored separately providing additional security. Here in this scheme the main task is to correctly place the message bits after decryptions which were randomly selected for key and the message length was reduced.

Along with encryption strategy what is important is the Key formation technique, for the encryption to be more secure the length of the key should be more and also the key should be changing for every message. In paper of Rohollah Karimi location and time is used into the encryption and decryption processes. 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. Geo-tag value is used to generate geo-secured key from session key and recover session key from geo-secured key. This geo-secured key is used for encryption of message which could be decrypted only if the recipient is at the intended location and time which formed geo-tag value[4] . Also on same ways a paper based on LDEA describe the use of location based encryption where latitude/longitude distances is used for encryption-decryption process [5]. The author has used toleration distance (TD) so that the user can decrypt the message in a certain diameter of area. It helps to allow mobility of the user to some extend and also helps in overcoming some fluctuation in GPS reading. In some cases it so happens that there is slight accuracy change in the reading generated by GPS system for variation in time factor or device, also it is not possible for the recipient to be on the same position till he receive a message at this situation it is not possible to decrypt the message hence leading to unavailability of data .These challenges are all overcome in LDEA by use of TD. Traditional encryption technology cannot restrict the location of mobile clients for data decryption. In order to meet the demand of mobile information system in the future, a location-dependent data encryption is a need [6]. Secure communication between wireless hosts is necessary in certain applications and GPS-based encryption complements traditional encryption techniques by restricting the decryption of a message to a particular geographical area and time period [7]. In another paper message security is provided by using the coordinates in GPS service, where it can specify the path of movement by taking coordinates in mobility of mobile node and estimate the future position of MN in a constant time interval. This new estimated coordinate is applied in to secret key along with Dynamic Toleration Distance (DTD)[8].

3. PROPOSED SYSTEM

3.1 Message Format

Every time when ever an important data is to be delivered or transferred via a mobile device it becomes necessary to maintain its confidentiality, integrity and access control, for this reason this paper implements an encryption scheme which accomplishes the security goal. In cell phones important message is encrypted using the location of recipient in key generation function, this message is then transferred to the recipient using telephony message service. To decrypt the message user just has track his own location and decrypt his received message in the inbox. While in case of laptops the important data is converted to encrypted format, then to color code encoding which is transferred to the recipient. This color code file formation technique also uses location of the recipient for encrypting the data and then encoding it into color code. Fig1. Shows format of encrypted message for both cell phones and personal computers.

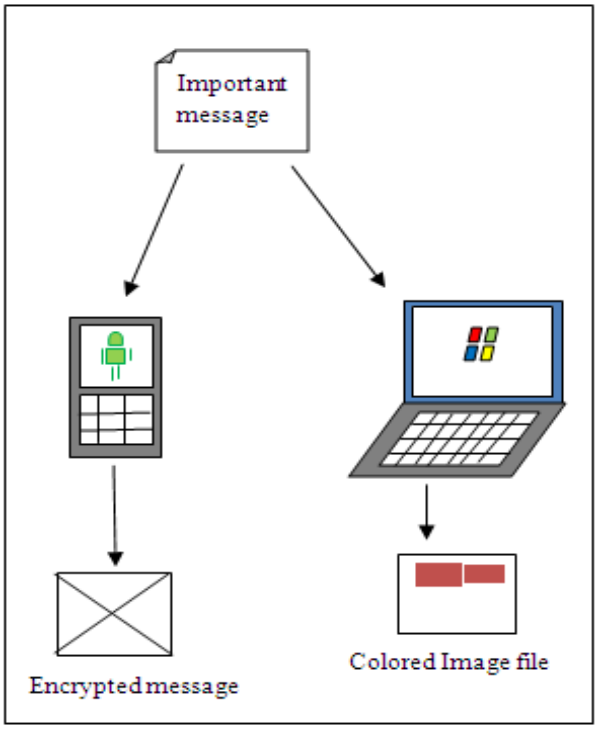

Fig 1: Shows format of encrypted message.

3.2 System Model

This paper presents an encryption scheme for both cell phones and personal computers. In case of cell phones the process followed is as shown in Fig 2. In this figure sender represents the person who wants to send important message in encrypted format while the recipient is the receiver who is suppose to decrypt the message received from the sender. Here the sender has to first request the recipient to send his current location. The recipient then tracks his location using GPS tracker, computes a key for that location using key generation function and then sends his location to the requester (sender) in form of latitude and longitude. Since the key generation function on both the ends will be same. The sender will generate key, encrypt his message, and transfer it to the recipient. On the recipients side he needs to first verify his location so as to validate the key which he had first formed during location transfer to sender. Once the key is validated he can use the key for decryption of message. The purpose here to use location based key is to make the key process dynamic and the main reason is that here the sender is given a choice to send the message after knowing the location of recipient. Best example is when a company employee wants to send an important message to his colleague he first enquire about his (colleagues) location if his colleague is out-side office area the message might fall in wrong hands hence he can reject message sending. Or if the sender gives his office location and by the time message reaches him he leaves his office area at such conditions the scheme is beneficial as it avoids message decryption in unsecured zone.

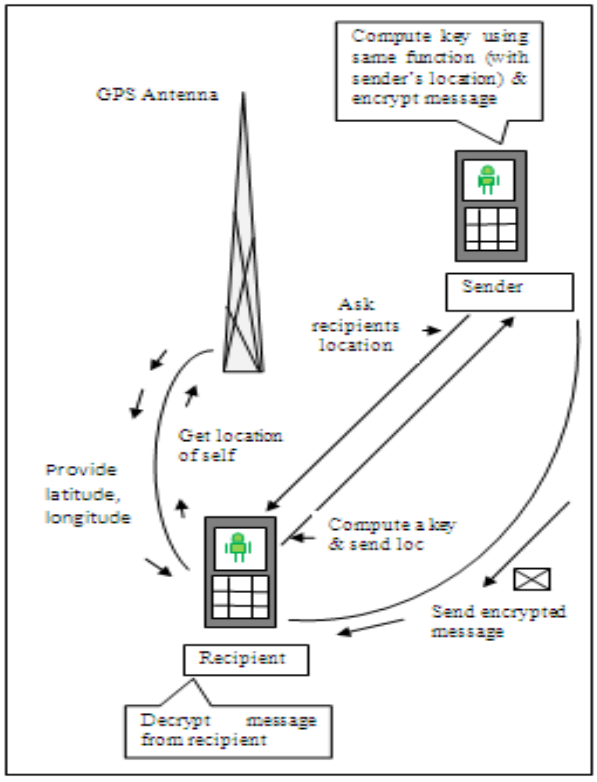

Fig 2: Shows the process model on cell phones.

In case of personal computer the proposed scheme is followed as shown in Fig 3. In this model we have used mobile phones to track user's location and location transfer as they have GPS tracker and to maintain key security independently. Whereas the sender sends the encrypted, encoded data which is color code file format to the recipient via mail. Here also the key is location dependent so the recipient needs to be in the intended location for decryption of message.

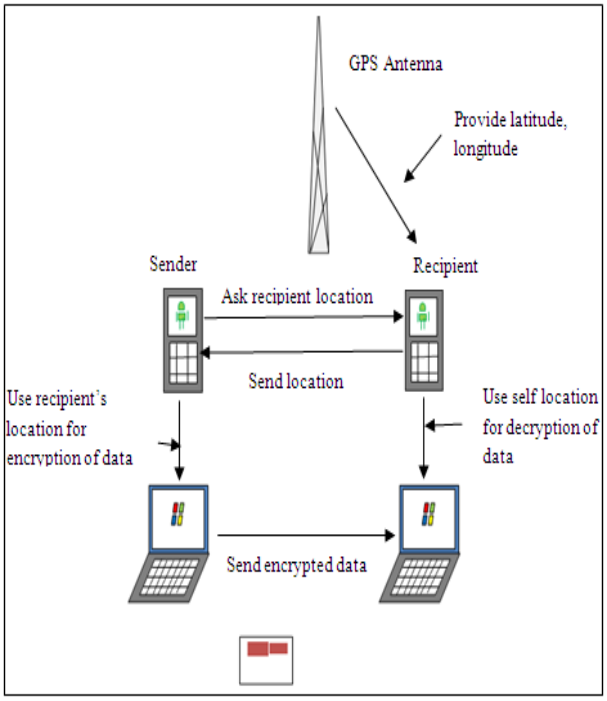

Fig 3: shows the process model on personal computer

3.3 Algorithm used for Encryption

Algorithm used for message encryption is simple to compensate with the battery drainage caused by GPS tracker which we have used for location dependency in proposed scheme. In case of personal computers to transfer any important message we first encrypt the data by using simply Xoring of the message with the key which is the location value generated. Here the length of key need not be same as the length of message. After encrypting the message we encode this data that is we convert it into color coding where every cipher text byte value is considered as the intensity of the color block used to represent the encoding. The color encoding could be either red, blue or green. On mobile phones we only carry out encryption using shifting of data depending on hash value generated by hash function.

Algorithm: In this scheme following algorithm is followed for mobile encryption:

Step 1. . Request recipient for his location.

Step 2. Recipient uses GPS tracker to get his current location, forms a key using hash function.

Step 3. The key formed can be made tolerable to a certain diameter of location where the message could be decrypted.

Step 4. This key is then stored in a variable by the recipient and copy is then forwarded to the message sender for encryption of message.

Step 5. The sender then encrypts his message by the key and sends it to the recipient.

Step 6. Recipient request for decryption of message. Decryption function calls GPS tracker function for recipient's location, which helps in deducing key. This key is then compared to the key stored in variable if both are equal then decryption of message takes place or else decryption is denied.

Algorithm: In this scheme following algorithm is followed for laptop based encryption :

Step 1. Request recipient for his location.

Step 2. Recipient uses GPS tracker to get his current location, forms a key using hash function.

Step 3. The key formed can be made tolerable to a certain diameter of location where the message could be decrypted.

Step 4. Key is then forwarded to the message sender for encryption of message.

Step 5. The sender then encrypts his message by the key further encodes the cipher text to color coding and sends it to the recipient.

Step 6. Recipient request GPS tracker for his location. This is used in deducing key. This key is then used for decryption of message.

This approach provides following benefits to the important data. It provides:

Confidentiality: Data encryption provides encapsulation for the data also this approach generates a key using hash function for a particular location. Hence it becomes difficult to estimate the location, estimate the hash function and also the tolerance distance within which data can be decrypted.

Access control: The recipient in this approach is restricted to a specific location and hence avoids message decryption whenever message is eavesdropped in middle of transmission.

Simplicity: Data encryption is done using shifts and Xoring of characters in the message and hence helps in less battery drainage to compensate with the battery loss due to GPS tracking.

User Friendliness: Message is well secured by the use of location based key hence it gives assurance to important data. Along with it GPS tracking, key generation, encryption and decryption are made simple in this approach so as to provide best usability for any novice user.

4. CONCLUSION

Important data can be well protected by the use of color encoding and encryption. Important data could be sent in color code form which could be accessible only to the authenticated user in a restricted field. Thus it could be best for every email to be this way encoded and send for its protection from theft**.**

This technique could be further enhanced for other type of data transfer via network. This technique could be enhanced to suit for online banking purpose so that transactions become more secure and easy

5. 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.

6. REFERENCES

[1] Cryptography & network security Principles and Practice by William Stalling.

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

[3] Yu Chen and Wei-Shinn Ku, "Self Encryption Scheme for Data Security in Mobile Device."CCNC09.

[4] Rohollah Karimi, Mohammad Kalantari, "Enhancing Security and Confidentiality on Mobile Devices by Location-based Data Encryption", 2011 IEEE, ICON 2011

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

[6] 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". ISBN 978-89-5519-131-8 93560, Feb. 12-14, 2007 ICACT2007.

[7] Ala Al-Fuqaha, Omar Al-Ibrahim, Joe Baird, "A Mobility Model for GPS-Based Encryption", IEEE Globecom 2005

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

[9] Mobile Devices Security guidelines, Mauritian Computer Emergency Response Team, National Computer Board.