International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

Location Based Security

Mudra Verma[1], Milind Rahatwal[2], Aakash Yadav[3], Manmit Sian[4], Nilam Parmar[5]

[1]*Mudra Verma: Student, Dept. of Computer Engineering, Thakur Polytechnic, Maharashtra, India*
[2]*Milind Rahatwal: Student, Dept. of Computer Engineering, Thakur Polytechnic, Maharashtra, India*
[3] *Aakash Yadav: Student, Dept. of Computer Engineering, Thakur Polytechnic, Maharashtra, India*
[4] *Manmit Sian: Student, Dept. of Computer Engineering, Thakur Polytechnic, Maharashtra, India*
[5]*Nilam Parmar: Teacher, Dept. of Computer Engineering, Thakur Polytechnic, Maharashtra, India.*

ABSTRACT – *Data security is a very important task in today's life. Data security can be done using GPS device. Among soul largely use information in electronic format. How to offer a security for information is vital. In this paper, we have a tendency to propose a Location based mostly Data-Security System to secure information by applying Encryption-Algorithm and co-ordinate exploitation GPS device. Encryption means of efficient secure integer comparison. The secret writing technology cannot prohibit the placement of knowledge decipherment. In order to satisfy the demand of a location-dependent approach location-dependent encoding rule is required. A target latitude/longitude co-ordinate is determined firstly. The co-ordinate is incorporated with a random key for encoding. The receiver will solely decode the cipher text once the co-ordinate noninheritable from GPS receiver is matched with the target co-ordinate. GPS-based secret writing is Associate in nursing innovative technique that uses GPS-technology to write location info into the secret writing keys to supply location based mostly security. GPS-based secret writing adds another layer of security on high of existing secret writing strategies by limiting the decipherment of a message to a specific location. Our experimental results not solely validate the effectiveness of our theme; however additionally demonstrate that the planned number comparison theme performs higher than previous bitwise comparison theme. The wide unfold of LAN and also the quality of mobile devices will increase the frequency of knowledge transmission among mobile users. However, most of the info secret writing technology is location-independent. An encrypted data can be decrypted anywhere. The coding technology cannot limit the placement of information coding. In order to satisfy the demand of mobile users within the future, a location-dependent approach, known as Location-Dependent encoding rule (LDEA), is planned during this study. A target latitude/longitude coordinate is determined firstly. The coordinate is incorporated with a random key for encoding. The receiver can only decrypt the cipher text when the coordinate acquired from GPS receiver is matched with the target coordinate. However, current GPS receiver is inaccuracy and inconsistent. The location of a mobile user is troublesome to precisely match with the target coordinate. A Toleration Distance (TD) is additionally designed in LDEA to extend its usefulness. The security analysis shows that the chance to interrupt LDEA is sort of not possible since the length of the random secret is adjustable. A prototype is also implemented for experimental study. The results show that the cipher text will solely be decrypted below the restriction of TD. It illustrates that LDEA is effective and sensible for information transmission in mobile atmosphere.*

Keywords – encryption, decryption, security, GPS technology, location, feedback.

1. INTRODUCTION:

Most of the data encryption techniques are location-independent. They cannot limit the situation of shoppers for information decipherment. In projected system, a unique location-dependent approach is employed for incorporating location data into information transmission.
It is vital to supply a secure and convenient information transmission. We propose a location-dependent approach for higher information security. The consumer places the coordinates manually in application for encoding. Then our application produce a encrypted file so we tend to send that encrypted file exploitation e-mail or by any external device to our destination .The client only decrypt the cipher text once the coordinate noninheritable from GPS receiver matches with the target coordinate. According to our discussion, the approach can meet the confidentiality, authentication, simplicity and practicability of security issues. As a result, the planned approach will meet the demand for private and industrial knowledge security.

Since the removal of signal-degrading Selective accessibility (SA) from GPS (Global-Positioning System) signals on the first might 2000, it is now possible to use hand-held GPS to navigate to within a few meters. The differential GPS (DPGS) will even give the accuracy to but one meter. Now, GPS receiver is fashionable employed in our lifestyle, like automotive navigation, fleet management

then on. In the past, GPS receiver is connected to the mobile devices, like personal organizer (Personal Digital Assistant), via cable or Bluetooth. It is a little inconvenient for users. Therefore, a personal organizer with associate integral GPS receiver, referred to as GPS personal organizer, is intended and declared on the middle of 2005. GPS personal organizer is additionally equipped with most of the wireless communication capabilities, together with GSM/GPRS/EDGE, quad-band GSM phone capabilities, IEEE 802.11 g, etc. The size and weight of GPS personal organizer is getting ready to the movable. But it's computing power and programming interface is best than mobile phones. It is expected that the mobile phones are replaced by such quite personal organizer within the future. Unlike the mobile phones that information transmission is generally supported SMS (Short Message Service), the kinds and quantities of information transmitted among GPS PDAs should be numerous and huge just like desktop PCS. That is, the information transmission among mobile devices can become a lot of and a lot of frequent in line with the on top of trend.

On the opposite hand, several ways area unit projected for the safety of information transmission; for instance, Aikawa et al. (1998) projected a light-weight cryptography rule for the copyright protection. Jamil (2004) projected associate increased rule for the standard DES rule, called AES. Jiang (1996) projected a multiprocessing rule for the RSA. Lian et al. (2004) projected a quick video cryptography theme supported chaos. McLoone and McCanny (2000) designed a hardware circuit for DES supported the FPGA technique. Shaar et al. (2003) projected a replacement encoding rule, referred to as HHEA. Smid and Branstad (1998) analyzed the past and way forward for DES rule. Zhang et al. (2004) projected a stream cipher rule with relevancy the standard block-based cipher approaches. However, these methods are location-independent. The sender cannot prohibit the situation of the receiver for knowledge coding. If the information secret writing formula will offer such perform, it's helpful for increasing the safety of mobile knowledge transmission within the future. Therefore, a Location-Dependent encryption formula (LDEA) is planned during this study. The latitude/longitude coordinate is employed because the key for encryption in LDEA. When a target coordinate is set for encryption, the ciphertext will solely be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent betting on what number satellite signals received. It is tough for receiver to decipher the ciphertext at identical location precisely matched with the target coordinate. It is impractical by victimization the wrong GPS coordinate as key for encryption. Consequently, a Toleration Distance (TD) is meant in LDEA. The sender {can also|also will|can even|may also|may} confirm the TD and also the receiver can decipher the ciphertext inside the vary of TD. In order to verify the performance of LDEA, a image tool is additionally enforced and tested in an outside experimental web site. The experimental result illustrates that LDEA is effective and sensible for knowledge transmission in mobile setting.

The popular of indoor or out of doors positioning devices cause the Location-Based Service (LBS) is obtaining necessary. LBS may be a service betting on a particular location. Systems will offer LBSs consistent with the situation of users. For example, a user may query where the nearest restaurant is. Liao et al. (2007) planned a location-dependent encryption approach for mobile system. The approach is predicated on a reverse hashing principle. A series of session keys is generated based mostly unidirectional hash perform. They are generated for mobile consumer and server in a very secure network at the same time. When the mobile consumer is operated in Associate in Nursing insecure network of the out of doors setting, the session key's incorporated with the GPS coordinate for making certain the information is decrypted at the desired location.

Besides Scott and Denning et al. (2003) planned a knowledge secret writing formula by victimization the GPS, called Geo-Encryption. Geo-Encryption was supported the normal secret writing system and communication protocol. For the sender, the data was encrypted according to the expected PVT (Position, Velocity and Time) of the receiver. A PVT-to-GeoLock mapping perform was accustomed get the GeoLock key. GeoLock key was performed bitwise exclusive-OR with a generated random key to urge a GeoLock session key. This session key was then transmitted to the receiver by victimization uneven secret writing. For the receiver, an anti-proof GPS receiver was used to acquire the PVT data. Then, identical PVT-to-GeoLock mapping perform was accustomed get the GeoLock key. The key was playacting exclusive-OR operation with the received GeoLock session key to urge the ultimate session key. The final session key was accustomed decipher the ciphertext. However, the PVT-to-GeoLock mapping perform is that the primary mechanism to confirm that the information will be decrypted with success. It is hard for sender and receiver to have identical mapping perform before the information transmission if they convey often. The design of LDEA will improve the on top of downside by skipping such mapping perform.

2. PROPOSED WORK:

Enhancing the safety is that the prime facet of the projected system. By adding the placement primarily based services with the coding method one will create the information safer.

System consists of following components:

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

2.1 Login and Registration:

Login and registration module give user the access rights to act with the system. Registration contains some basic details relating to username, password and email id. Login uses username and arcanum to permit the user to pass in to the system. For storing the details, we use SQL server 2005. For username and password separate table is maintained. Tables are handled by administrator.

2.2 Encryption:

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

For this purpose, we have a tendency to use various algorithms like M. Aikawa et al. proposed a light-weight coding rule for the copyright protection. T. Jamil projected AN increased rule for the standard DES rule, called AES (Advanced Encryption Standard). J. Jiang projected a data processing rule for the RSA. S. Lian et al. proposed a quick video coding theme supported chaos. M. McLoone and J. V. McCanny designed a hardware circuit for DES supported the FPGA technique. M. Shaar et al. proposed a new data encryption algorithm, called HHEA. M. E. Smid and D. K. Branstad analyzed the past and way forward for DES rule. Y P. Zhang et al. proposed a stream cipher rule with relevance the normal block-based cipher approaches [2].
Location co-ordinates square measure used as a „key" for encrypting the contents.

2.3 GPS Interfacing and Location Matching:

Global Positioning System satellites broadcast signals from area that square measure employed by GPS receivers to produce current location by creating use of line of longitude and latitude.

The interfaced GPS device can seem as virtual port on laptop to that one will communicate through our designed code which may transmit receive by this port like HyperTerminal or custom made software.

Location matching is that the key method for self-made decipherment of information. The co-ordinates fetched by GPS should be matched with the co-ordinates that were entered whereas encrypting the information. As current location retrieved by GPS device won't be specifically same anytime thanks to weather, etc. Tolerance distance (TD) vital role in rounding error up or down the co-ordinate values at bound extent.

2.4 Decryption:

The location co-ordinates that were used as key whereas coding should be matched with co-ordinates values fetched by GPS device at receiver aspect. If this condition is glad then solely user will decode the information otherwise encrypted file are going to be discarded from the system mechanically.

2.5 Feedback:

The user or admin can communicate with each other in a feedback format which is very similar as a messenger, the user can send feedback about changes or any other requirement to the admin. After processing the feedback the admin may fulfill the user requirements.

3. SYSTEM ARCHITECTURE:

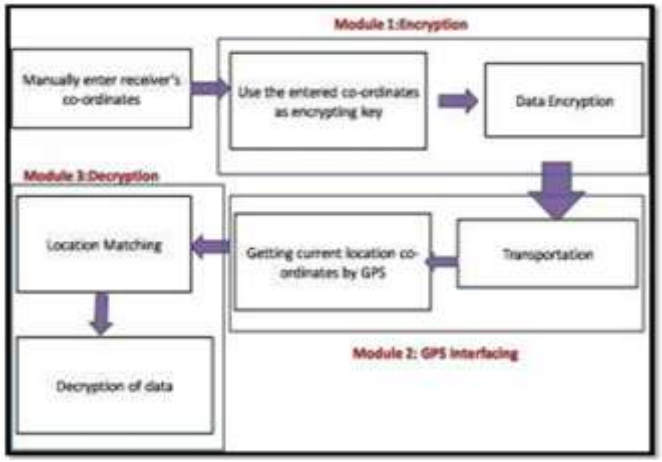

Fig. Block diagram of the system architecture.

The planned approach is extended to the opposite application domain e.g. Authorization of software. If the system computer code is allowed inside a pre-defined space, like for explicit organization the execution of the computer code could bring home the bacon the placement check supported planned approach. Decryption method is allotted once the licensed user is found in mere space. This approach is used for mobile applications like in Smartphone.

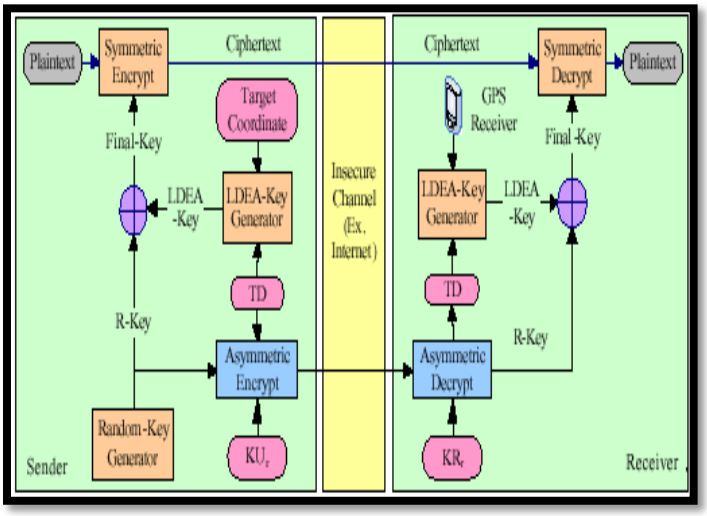

Fig. Encryption and decryption process carried out in the system.

When the target coordinate and TD (Toleration Distance) is given by the sender on the left-hand facet, associate LDEA-key is generated from latitude/longitude coordinate and TD. The random-key generator problems a session key, referred to as R-key. Then, the final-key for encrypting the plaintext is generated by exclusive-or R-key with LDEA-key. The final-key are often used for the regular cypher rule, like DES, AES, triple-DES, etc. In the bottom of, KUr and KRr is the public and private keys generated on the receiver side. KUr is transmitted to the sender side firstly. Then, TD and R-key is transmitted via uneven cryptography rule. When the receiver gets the TD and R-key, the LDEA-key are often generated from TD and also the coordinate nonheritable from GPS receiver. The final-key are often generated by exclusive-or R-key with LDEA-key. If the acquired coordinate is matched with the target coordinate within the range of TD, the cipher text can be decrypted back to the original plaintext. Otherwise, the result is indiscriminate and meaningless.

The target coordinate are often determined by the sender or receiver. If it's determined by the sender, the sender will inform the receiver the physical location for encryption. A secure communication, like phonephone, is convenient and safety for the sender to notify the receiver. If the target coordinate is decided by the receiver, the receiver will inform the sender within the same approach, e.g., telephone. After the sender gets the target coordinate, the data can be received by the receiver according to the above mentioned processes.

The generation of LDEA-key, R-key and final-key is conferred in additional details. An example shown is used to illustrate the generation process.

3.1 Transform latitude/longitude coordinate:

The format of coordinate nonheritable from the GPS receiver isWGS84 (World geophysics System 1984) outlined in NMEA (National Marine physical science Association) specification. The coordinates square measure increased ten thousand to be associate whole number. Then, the whole number is split by a worth comparable to the TD so as to permit the coordinate quality. According to CoordTrans tool of Franson Company, the values are 5.4 and 6 for latitude and longitude corresponding to 1 m, respectively. In advance, one bit is place before of the integral a part of the on top of result. The bit is zero for east and south and one for west and north.

3.2 Combine and hash:

The transformation results of the on top of step square measure combined by playing a bitwise exclusive-OR operation. Then, MD5 hash rule is employed and generates a 128-bit digest for the combined result. Then, the digest is split into 2 64-bit values, called LDEA-keys. This step causes that the target coordinate is not able to be derived or decrypted from the LDEA-keys.

3.3 Generate final-key:

A session key (R-key) is generated at random with an equivalent length of LDEA-key, i.e., 64 bits in the example. LEDA-keys square measure exclusive-OR with the R-key on an individual basis to come up with the final-keys. Two final-keys square measure used because the secret key and initial price of DES regular cryptography rule.

4. APPLICATIONS:

•Military- In military this technology is wont to keep the information secured from the attackers throughout wars.

•Banks- This technology can be used in banking for the purpose of money transaction as well as for passbook sharing.
•Individual use- It also can be accustomed to store one's confidential information. For e.g.: for business purpose.
•Multinational Industries-In Industries vital information is secure by mistreatment this technology.
•Educational purpose -In schools and college's confidential data can be secured by pattern using this technology. For e.g. Question paper.

5. RESULT:

Firstly the registration process occurs for the admin and the user,

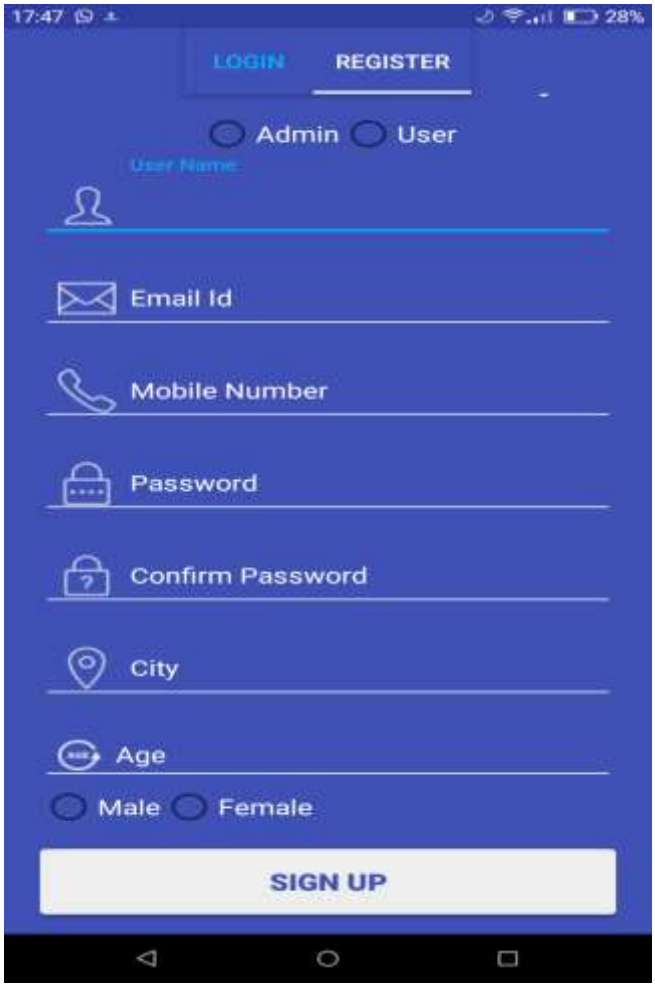

Fig. Registration of admin and user

After registration is completed the user or admin can login,,

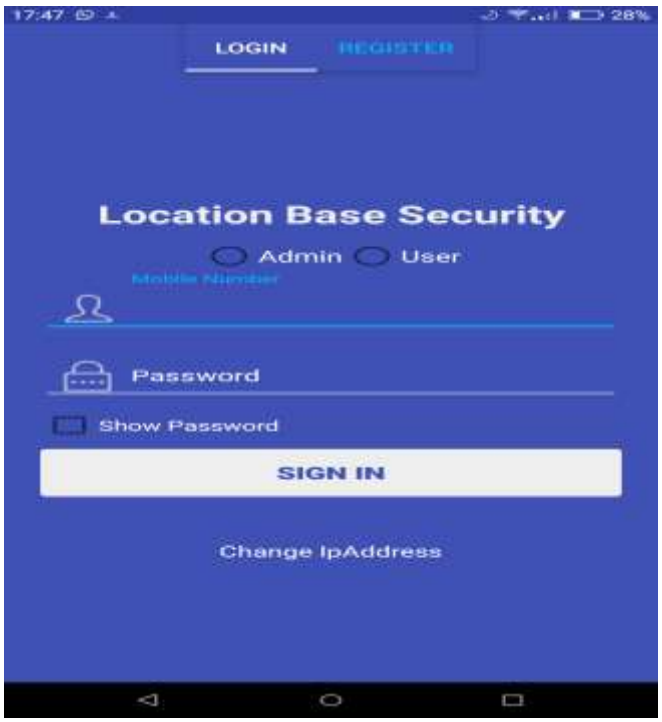

Fig. Login process of admin and user

The admin first sends a file to the user selecting all the necessary criteria of constraints to be followed by the user,

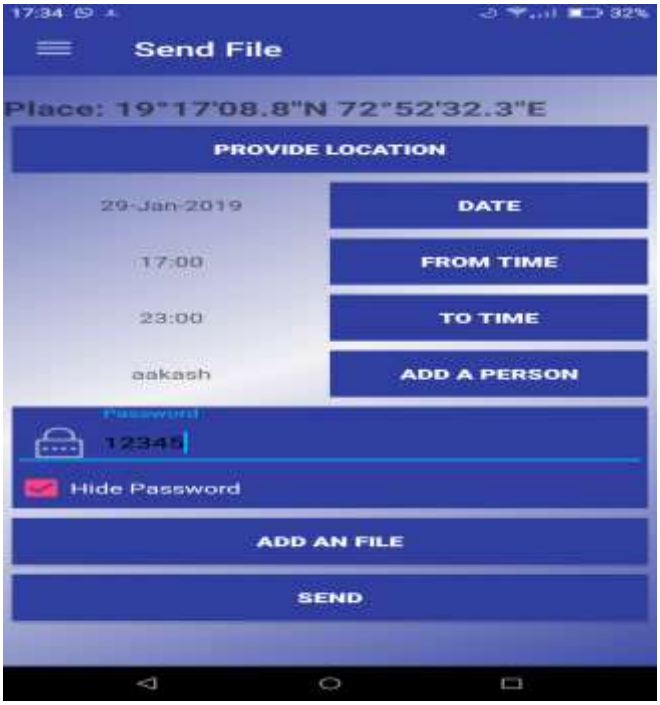

Fig. Sending a file to a user

After filling all the fields the file can be selected from the admins device directory,

Fig. Successful selection of the file

The admin and users workspace looks as follows,

Fig. Admin work space

The user has all the files sent by admin in his/her directory,

Fig. user's directory with all the files received.

After selecting the file the user can see all the constraints imposed on him by the admin however the user cannot view the file unless it is decrypted for which the user needs the key which the admin has set. This key will be received to the user via mail,

Fig. Constraints imposed on the user by the adimin.

Fig. Key to be entered by the user received via mail to decrypt the file.

6. CONCLUSION:

Traditional coding technology cannot prohibit the situation of mobile users for knowledge decoding. In order to satisfy the demand of mobile users within the future, LDEA algorithmic rule is planned during this analysis. LDEA give a replacement perform by mistreatment the latitude/longitude coordinate because the key of knowledge coding. A Toleration Distance (TD) is additionally designed to beat the quality and inconsistent of GPS receiver. The security strength of LDEA is adjustable once necessary. The experimental results of the epitome conjointly shows that the decoding is forced by the vary of TD. As a result, LDEA is effective and sensible for the info transmission within the mobile atmosphere.
Current style of LDEA algorithmic rule is especially supported the DES algorithmic rule. Other algorithms, like AES (Advanced coding Standard), triple-DES, etc., will want to replace the DES algorithmic rule once necessary. Location's latitude/longitude co-ordinates plays important role in the formation of encrypted data along with decryption process.

7. REFERENCES:

1. Swapna B Sasi, Betsy K Abraham, JInil James, Riya Jose "Location Based Encryption using Message Authentication Code in Mobile Networks", In IJCAT International Journal of Computing and Technology Volume 1, Issue 1, February 2014.

2. L. Scott, D. Denning, "A Location based mostly coding Technique and a few of Its Applications", Proceedings of ION NTM 2003.

3. V. Rajeswari, V. Murali, A.V.S. Anil, "A Navel Approach to spot Geo-Encryption with GPS and completely different Parameters (Locations And Time)", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4), 2012.

4. Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, 1998. A lightweight coding technique appropriate for copyright protection IEEE Trans. Consum. Electron., 44: 902-910.

5. Becker, C. and F. Durr, 2005. On location models for ubiquitous computing. Personal Ubiquitous Comput., 9: 20-31.

6. Gruteser, M. and X. Liu, 2004. Protecting privacy in continuous location-tracking applications. IEEE Security Privacy Maga., 2: 28-34.

7. http://www.ijraset.com/fileserve.php?FID=4227