Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Location Based Encryption for Secure Banking Transactions in mobile data environment

Prof. Lata Sankpal[1], Aishwarya Rathod[2], Bhagyalaxmi Kodre[3], Nida Sayyed[4], Ronak Sayta[5]

[1]Department of Computer Engineering, Sinhgad Academy of Engineering, Pune
[2]Department of ComputerEngineering, Sinhgad Academy of Engineering, Pune
[3]Department of Computer Engineering, Sinhgad Academy of Engineering, Pune
[4]Department of Computer Engineering, Sinhgad Academy of Engineering, Pune
[5]Department of Computer Engineering, Sinhgad Academy of Engineering, Pune

Abstract — *Security has dependably been an essential piece of human life. Individuals have been searching for physical and monetary security. With the progression of human learning and getting into the new period the need of data security were added to human security concerns. Information is encoded just when individual is having private key can unscramble it. In cryptography "character" part is imperative, we can determine name, address, id as personality, yet we can likewise give put (i.e. Physical nearness at a specific area) as character. This place can be utilized as a part of encryption. We confide in physical security more. Those are inside (some portion of) specific topographical zone is endorsed for information decoding generally not permitted. Another utilization of "Location Based Cryptography" is get to control. (Ex-getting to printer in a room however can't access outside of room.). It is more suitable for banks, enormous organizations, Institutions.*

Keywords*-Authentication, Banking Application, GPS, LDEA, Shoulder surfing, Security*

I. INTRODUCTION

Nowadays, the use of wireless technology goes on increasing as an increase in the wireless applications. To give a higher layer of security to such applications, distinctive information encryption calculations are utilized. In any case, customary information encryption calculations are location free. Information encoded with such methods can be unscrambled anyplace. Independent location based cryptographic technique makes sure that after transferring encrypted information from sending end, decryption can takes place anywhere from receiving point of view. However, as indicated by need of portable clients on the off chance that we need greater security at the exchange of information in versatile communication for that we require location dependency [2]. They can't confine the area of versatile customers for information decryption. To beat the downsides of the current framework we outline our framework. In our proposed framework, it checks the authorized log in as well as checks the location of the user at the time of log in. In view of this client can't play out any exchanges from anyplace, he/she should be in the area which is given at the time of sign in [2]. We are utilizing android telephone as a GPS device in our framework. Finally, a new security level will be added to the existing security measures using location-based encryption.

Data security in the cloud is so important. Users (individuals, companies) are concerned about the access to the information by unauthorized users. Presently assume that information is some basic and secret data from a bank or an organization, and so forth. Surely, the need of access control in the distributed computing is like never before and is the critical piece of information security in cloud. In our strategy, we utilize the client's area and geological position and we will add the security layer to the current safety efforts. Our answers are more appropriate for banks, huge organizations, foundations and cases this way. The main thing we require is an Anti-Spoof and precise GPS that organizations can bear to purchase. Also implementing the location-dependant data encryption algorithm (LDEA), on the loud and uses computer (which is connected to the GPS) is required.

II. LITERATURE SURVEY

From paper “Protected Mobile Banking Using Location of Users” we learned, Mobile android application often has access to user personal data and other resources on the user device. Misuse of this data may result in data leakage. A control mechanism by which privileges can be dynamically granted or revoked to application based on a specific context of the user is needed. As compared to the current banking application which are location-independent, in this paper a banking application is developed which is location dependent [1]. The algorithm used only decrypts the cipher text in specified location. Each operation depends on the key, location and tolerance distance region. If a trail to decrypt data at another location is made, the decryption process fails and reveals no information. Our system also provides solution to physical attacks using virtualization, where the customer performs fake transactions for his/her physical security purpose.
In paper “Security scheme for geographic information databases in location based system” ,Mohammad Ahmdian, Jalal Khodabandeloo, Dan C. Marinescu, have discussed data structures for storing digital maps and matched encryption algorithms for mobile devices with limited computational resources. This paper proposes a solution of secure LBS,

systemthat is both accessible and scalable [3]. Inaddition, a new practical solution is suggested by applying cryptographic technics for building a reliable framework for all parties by preserving their digital rights. Although cryptographic algorithm, can overload CPUs, here a fast encryption algorithm is used which can be customized for LBS applications. Therefore the secured LBS system based on our cryptographic scheme is a new approach which is described and verified according to comparison between a plain map data and encrypted map data. The experiments show that the difference in the reading plain map data compared to encrypted map data is negligible, and a secure protocol is achieved between all parties and the digital assets in the LBS are well-protected. The suggested solution is very lightweight encryption schemes for building a reliable framework. By reading this paper we came to know that, several factors should be considered before selecting an encryption algorithm for each application. In this case, the final selection is made based on these characteristics:

1. Computational and memory efficiency
2. Flexibility, simplicity and ease of implementation
3. Compatibility with data format and hardware platform

The paper “Generalized Study on Encryption Techniques for Location Based Services”teaches there are four types of techniques used for mobile computing data encryption. The first technique is the geo-encryption technique, which considers the location of the device within a range of 1KM so the possible key generated values are approx. 1 billion [4]. The drawback of this system is that if a user goes out of the 1km he/she is unable to decrypt the message. The second technique in this paper is LDEA(Location Dependent Encryption Algorithm). This technique overcomes the drawback of geo-encryption algorithm, it specifies the TD region(Tolerant-Distance), the message is only decrypted in the tolerant distance otherwise the message is not visible at the receiver side. The third technique is self-encryption, which uses a ciphertext to encrypt the message. The same key is used for decryption of the ciphertext at receiver end. This is a lightweight encryption technique. The fourth technique is Mobile User Location Encryption (MULE) [4]. This technique encrypts and decrypts the message when the mobile is in sleep state.

From paper “Location based services using android mobile operating System” published by AmitKushwaha, VineetKushwaha we learnt that, the location based information system assists with the exact information, at the right place in real time and location sensitiveness They have utilized palmtops and iPhones, which supplant the cumbersome desktops [5]. We have huge number of utilizations and use where a man sitting in a roadside bistro needs to get applicable information and data. Such needs can only be catered with the help of LBS. These applications incorporate security related occupations, general overview with respect to activity designs. They have made various different applications where they have given the client's information regarding a place he or she needs to visit [5]. But these applications are limited to desktops. They have imported them on mobile devices. It guarantees that when a person goes for a tour or any tourist place there is no need of taking the travel guides with him because all guides work is done by these applications. In short all the information is available in his mobile device and also in user specified format.

In paper “Data encryption using the dynamic location and speed of mobile node” published by HamadHatem, ElkourdSouhir proposed a new solution to protect the mobile phone service like MMS and SMS attacked by spoofing, in which they have used one of the accessible administrations (GPS) by using the coordinate of receiver mobile phone.They have actualized this calculation utilizing J2ME programming and tried it for various locations and velocities [6].The plain content is scrambled utilizing the parameters sent in the asymmetric encryption.After the Encrypt catch is squeezed the plaintext document is scrambled. The cipher text is unscrambled utilizing the parameter calculated in the algorithm. The client picks the decoding choice. After the Decryption button is pressed the user detects the estimated coordinate and Dynamic Toleration Distance (DTD) [6]. Then by pressing the button next the ciphertext file decrypted. This means: "Open the folder to see the decryption file". If the acquired coordinate meets the constraint of target coordinate and DTD, the content of the decryption file is similar to the plaintext file which is stored in the folder. Otherwise, the content is indiscriminate and meaningless.

In [7]Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta says that, Mobile phones were developed only for voice communication but now a days , voice communication is just one service of a mobile phone. Other major factors are web browser and GPS services. Both of these servicesare handled by the manufacturers, the system doesn’t allow the user to access the mobile hardware directly. But now, after the launch of android based open source mobile a user can access the hardware directly and design customized native applications to develop Web and GPS enabled services. The facilities available in android platform for implementing LBS services (geo-services)are also discussed.

In [8] Hsien-Chou Leu& Yun-Hsiang Chou, proposed a location Data Encryption Algorithm LDEA, in which the coordinate is combined with a stray key for information encryption. We can only decrypt the text when the coordinate obtained from GPS is similar totarget coordinate. But, current GPS receiver is flawedand inconsistent. The exact location of mobile phone user is difficult to catch. A toleration distanceregion (TD) has been instigated in LDEA to grow its performance. The study shows that the odds to break LDEA is almost impossible. The results show that the text can only be decoded under the restriction of TD. It illustrates that LDEA is fruitfuland feasible for data transmission in mobile environment.

In paper “Securing sensor networks with location-based keys”, Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang explained, Wireless sensor networks are often deployed in unattended and hostile environments, leaving individual sensors vulnerable to security compromise. They proposed the novel notion of location-based keys for designing compromise tolerant security mechanisms for sensor networks [9]. In light of location based keys, we build up a hub to-hub verification conspire, which isn't just ready to limit the effect of bargained hubs inside their region, but also to make way for the establishment of pair wise keys between neighboring nodes. Compared with previous proposals, our plan has idealize strength against hub trade off, low stockpiling overhead, and great system versatility. We likewise show the utilization of location based keys in battling a couple of infamous assaults against sensor network routing protocols.

Christian Becker, Frank Durr have given that the information processing in ubiquitous computing is based on the location of physical objects in their paper “On location models for ubiquitous computing”.A notion of distances between objects is required. A search for all objects in a certain geographic area requires the possibility to define the special ranges and the special inclusion of locations. They have talked about general properties of geometric directions. In light of that, they introduced an outline of existing area models taking into consideration position and range. The area models are arranged by their prerequisites [10]. Other than an outline of existing area models and methodologies, the characterization of area models as for application necessities can help engineers in their plan choices.

William Enck, Peter Gilbert, Byung-Gon Chun in the paper “Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones” clarified that today’s smart phone operating systems frequently fail to give clients sufficient control over and perceivability into how outsider applications utilize their private information. We address these deficiencies with TaintDroid, a productive, system-wide dynamic taint tracking and analysis system capable of simultaneously tracking multiple sources of sensitive data [11]. TaintDroid gives continuous investigation by utilizing Androids virtualized execution condition. TaintDroid causes just 14% execution overhead on a CPU-bound micro benchmark and and forces insignificant over-head on intuitive outsider applications. Utilizing TaintDroid to screen the conduct of 30 well known outsider Android applications, we found68 occasions of potential abuse of clients private data crosswise over 20 applications. Checking delicate information with TaintDroid provides informed use of third-party applications-for phone users and valuable input for smart phone security service firms seeking to identify misbehaving applications.

Tomas Sander Christian, F. Tschudin produced the idea of converting the message into a program in paper “Towards Mobile Cryptography”. In current system, there is leakage of information because of the message which is encrypted uses a key. But in this paper the key itself is a program. The paper mainly focuses on encryption and decryption of text by not entering key but instead using a direct program [12]. This reduces the threat of spying any other user to the key. As there is no key, but a program to convert the data. It uses the EEF algorithm (Evaluation of Encrypted Functions) to encrypt the data in a public environment [12]. The other system used is crypto systems which also encrypts and decrypts the data using a set of keys which is available at the sender’s as well as receiver’s end.

III. PROPOSED SYSTEM

In our technique we utilize the client's area and geological position and we will add a security layer to the current safety efforts. Our answer is more proper for banks, huge organizations, foundations and so on. The main thing we require is an Anti-Spoof and exact GPS that organizations can bear to purchase. Also implementing the LDEA algorithm on the server and the user’s mobile (which is connected to GPS) is required.

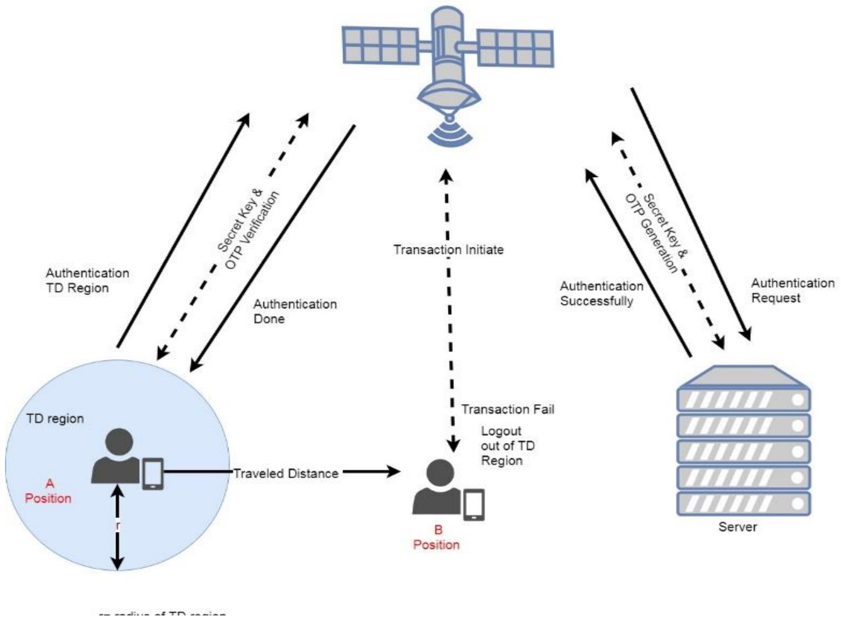

Figure. 1. Design of the Proposed System

We are using GeoEncryption Algorithm, location based cryptography, positioning tools (Anti-spoof GPS). That means our system provide solution to physical assault utilizing virtualization, in which client isn't permitted to perform fake transaction for his/her physical security purpose.

In above architecture user register himself/ herself in our application. For registration he/she should provide personal details. After successful registration user can login to the system. Then the system will send the encrypted password to registered email so that password is prevented from visualization.

After successful login, user will be asked to enter his/her preferred TD region. This TD region specify range in meters. A toleration distance (TD) is also designed to overcome the inaccuracy and inconsistent of GPS receiver. Then user is supposed to enter the secret key sent on registered email id. If user entered key is correct then OTP will be received on mobile by SMS. If entered OTP is correct and is in the specified TD region, then user can view account details and/or perform money transaction operation.

This technology empowers individuals, companies, etc. to store their data and information on the server and they can access their own data at any time, from any place. Our system utilizes location based encryption technique for providing security to the banking application. Our framework just permits validated individuals for doing exchange. Confirmation depends on location based encryption. If there should be an occurrence of physical assault, our system creates a virtual domain with additional key in secret word and stops counterfeit exchanges. Our framework prevents access of record from any area. To achieve it we require following three algorithms :

- LDEA (Location Dependent Encryption Algorithm)
- MD5 (Message Digest 5) Algorithm
- Haversine Algorithm

A. *Purpose of LDEA*

The purpose of this algorithm i.e. LDEA is mainly to include the latitude/longitude coordinate in the data encryption and to restrict the location of data decryption.LDEA provide a new function by using the latitude/longitude coordinate as the key of data encryption.

The steps of LDEA algorithm are:

1. Transform latitude/longitude coordinate into float values.
   - The format of coordinate acquired from the GPS receiver is WGS84 (world geodetic system 1984) defined in NMEA (National Marine Electronics Association) specification.For example, “E 12134.5971” means 121 degrees and 34.5971 minutes east longitude. “N 2504.7314” means 25 degrees and 4.7314 minutes north latitude.
2. Combine and hash
   - The transformation results of the above step are combined by performing a bitwise exclusive-OR operation.
   - Then, MD5 hash algorithm is utilized and it generates a 128-bit key for the combined result.
   - Then, the key is split into two 64-bit values, called LDEA-keys.
   - This step causes that the target coordinate is unable to be derived from the LDEA-keys.
3. Generate final-key
   - A session key (R-key) Is generated randomly with the same length of LDEA-key, i.e., 64 bits in the example.
   - LEDA-keys are exclusive-ORed with the R-key separately to generate the final-keys.
   - These final-keys are used as the secret key and initial value of DES symmetric encryption algorithm.
   - These steps should be redesigned when necessary.

B. *Purpose of MD5 algorithm*

The MD5 algorithm is widely used hash function producing a 128-bit hash value. It can be used as a checksum to verify data integrity. The steps involved in MD5 algorithm are as follows:

Step 1: Append padded bits

- The message is padded so that its length iscongruent to 448, modulo 512.
- Means extended to just 64 bits shy of being of512 bits long.
- A single “1” bit is appended to the message,and then “0” bits are appended so that thelength in bits equals 448 modulo512.

Step 2: Append length

- A 64-bit representation of b is appended to the result of the previous step.
- The resulting message has a length that is an exact multiple of 512 bits.

Step 3: Initialize MD buffer

A four-word buffer (A,B,C,D) is used to compute the message digest.

- Here each of A, B, C, D, is a 32-bit register.
- These registers are initialized to the following values in hexadecimal:
  word A: 01 23 45 67
  word B: 89 ab cd ef
  word C: fe dc ba 98
  word D: 76 54 32 10

Step 4: Process message in 16-word blocks

- Four auxiliary functions that take as input three 32-bit words and produce as output one 32-bit word.

Step 5: Output

- The message digest produced as output is A, B, C, D.
- That is, output begins with the low-order byte of A, and end with the high-order byte of D.

C. Purpose of Haversine algorithm

Haversine algorithm is used to calculate the TD (Tolerant Distance) region from target point to origin point. The origin point is the extreme point in the region. The steps are given below:

1. R is the radius of earth in meters.
   LatO= latitude of origin point.
   LongO = longitude of origin point.
   LatT= latitude of target point.
   LongT= longitude of target point.
2. Difference in latitude = LatO-LatT
   Difference in longitude = LongO -LongT
3. Φ =Difference in latitude in radians
   Λ =Difference in longitude in radians
   O= LatO in radians.
   T= LatT in radians.
4. A = sin(Φ/2) * sin(Φ/2) + cos(O)*cos(T)*sin(Λ/2)*sin(Λ/2)
5. B = min(1,sqrt(A))
6. Distance = 2*R*B

IV. SCOPE OF PROJECT

Our framework utilizes location based encryption technique for providing security to the banking application.Our framework just permits verified individuals for doing exchange. Verification depends on location based encryption. This shields from unauthorized access. Our framework permits access of record/account from any area. All banking applications are location subordinate. Client location could be utilized for better insurance. Because user location could not be hacked by hacker.

V. CONCLUSION

Location based encryption and location-dependent data encryption algorithm (LDEA), were reviewed. At last another security level was added to the current safety efforts using location-based encryption. This technique can be used in several places, for example, banks, huge organizations, establishments and have the coveted execution.

VI. REFERENCES

[1] Aishwarya Nair, Ankita Devrukhar, Karthika M. Vinod, Pallavi Lanke, “Protected Mobile Banking Using Location of Users”, IJARCCE, ISO 3297:2007 Certified, Vol. 6, Issue 4, April 2017.

[2] Sourish Mitra, Avijit Chakrabotry, Arunabha Bhaumik, Joy Devanjee, Mainak Maulik, “A location dependent cryptographic approach based on target coordinate from distanc tolarant key transfer for GPS mobile reciever”, IOSR-JCe, e-ISSN: 2278-0661, p-ISSn:2278-8727, Volume 17, Issue 1, Ver.VI 2015, pp 56-63.

[3] Mohammad Ahmdian, Jalal Khodabandeloo, Dan C. Marinescu, “A security scheme for geographic information databases in location based system”,IEEE southeast conference, 2015, Florida.

[4] Y. Lakshmi Prasanna, Prof. E. Madhusudhan Reddy, “A Generalized Study on Encryption Techniques for Location Based Services”,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 19-26,2014.

[5] Amit Kushwaha, Vineet Kushwaha, “Location based services using android mobile operating System”, Int. J. Adv. Eng. Technol., vol. 1,no. 1, pp. 1420, 2011.

[6] Hamad Hatem, Elkourd Souhir, “Data encryption using the dynamic location and speed of mobile node”, European, Mediterranean & MiddleEastern Conference on Information Systems 2010 (EMCIS2010) April 12-13 2010, Abu Dhabi, UAE.

[7] Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta, “Location based services using Android”, Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471480,2009.

[8] Hsien-Chou Liao and Yun-Hsiang Chao, “LDEA: Data encryption algorithm based on location of mobile users",Taiwan(R.O.C.), Journal 2008, Vol. 7, No. 1, p. 63-69.

[9] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, “Securing sensor networks with location-based keys”, IEEE communication society/WCNC 2005, 0-7803-8966-2/05/$20.00 2005 IEEE.

[10] Christian Becker, Frank Durr, “On location models for ubiquitous computing”, 2005 9: 20-31, DOI: 10.1007/s00779-004-0270-2,2003.

[11] William Enck, Peter Gilbert, Byung-Gon Chun, “Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones”, Proc. 9th USENIX Conf. Oper. Syst.Des. Implementation, 2010, pp. 1–6.

[12] Tomas Sander Christian, F. Tschudin, “Towards Mobile Cryptography”, International Computer Science Institute, Berkeley, icsi.berkley.edu.