

Implementation of Location Based Encryption for Secure Banking Transactions in Mobile Data Environment

Aishwarya Rathod, Bhagyalaxmi Kodre, Nida Sayyed, Ronak Sayta, Lata Sankpal

Abstract: Security has constantly been a fundamental bit of human life. People have been hunting down 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. In cryptography "character" part is imperative, we can utilize this part as encryption. Those are inside specific topographical zone is endorsed for information decoding, otherwise 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 take 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 and a router as a GPS system for other than android users. At long last, another security level will be added to the current safety measures utilizing location-based encryption.

Revised Version Manuscript Received on 04 June 2018.

Aishwarya Rathod, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune (Maharashtra)-411048, India.

Bhagyalaxmi Kodre, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune (Maharashtra)-411048, India.

Nida Sayyed, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune (Maharashtra)-411048, India.

Ronak Sayta, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune (Maharashtra)-411048, India.

Prof. Lata Sankpal, Department of Computer Engineering, Sinhgad Academy of Engineering, Pune (Maharashtra)-411048, India.

Information security in the cloud is so critical. Clients (people, organizations) are worried about the access to the data by unauthorized clients. 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 primary concern we require is an Anti-Spoof and exact GPS that associations can stand to buy. 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 Khodabandelloo, Dan C. Marinescu, have discussed information structures for putting away computerized maps and coordinated encryption calculations for cell phones with restricted computational assets. This paper proposes an answer of secure LBS, framework that is both available and adaptable [3]. In addition, another handy arrangement is proposed by applying cryptographic methods for building a solid structure for all gatherings by protecting their computerized rights. Though cryptographic calculation, can over-burden CPUs, here a quick encryption calculation is utilized which can be redone for LBS applications.

Implementation of Location Based Encryption for Secure Banking Transactions in Mobile Data Environment

Consequently the secured LBS framework in view of our cryptographic plan is another approach which is portrayed and confirmed by correlation between a plain guide information and encrypted information. 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 proposed arrangement is extremely lightweight encryption plans for building a solid structure. By perusing this paper we came to realize that, few components ought to be considered before choosing an encryption calculation for every 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 Amit Kushwaha, Vineet Kushwaha 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 Hamad Hatem, Elkourd Souhir 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 services are 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 to target coordinate. But, current GPS receiver is flawed and inconsistent. The exact location of mobile phone user is difficult to catch. A toleration distance region (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 fruitful and 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 found 68 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 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.

We are using Geo Encryption 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.

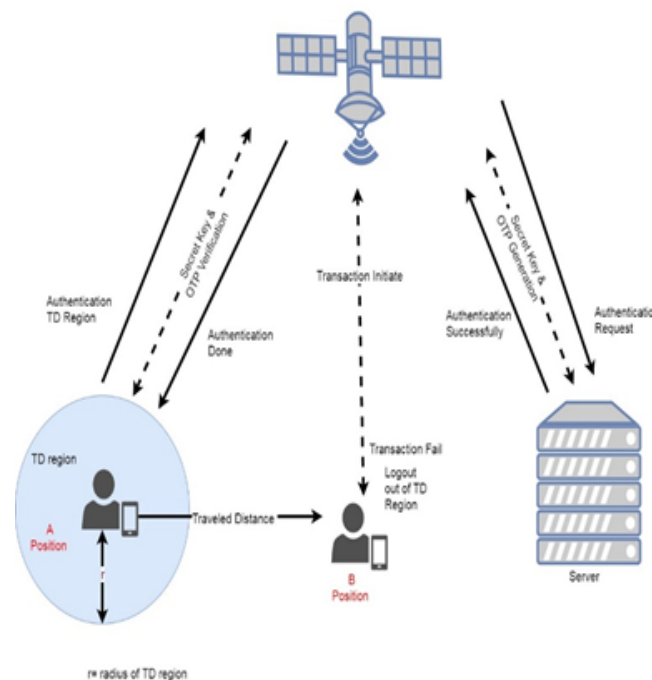


Fig. 1. Design of the Proposed System

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)
- AES (Advanced Encryption Standard) Algorithm
- Haversine Algorithm

IV. METHODOLOGY

In hardware requirements we require system consisting of Intel I3 Processor and above, 40 GB Hard Disk, 15 VGA Color Monitor, 4GB Ram, Android operating system for Mobile devices for implementation of our project.

In software requirements we require PC which contains Windows 7 and above Operating system, Java 1.8 Coding Language, Android 2.3 and above Tool Kit, Android Studio IDE.

Algorithms:

A. Purpose of LDEA

The purpose of this algorithm i.e. LDEA is primarily to embrace the latitude/longitude coordinate in the information encryption and to limit the area of information decryption. LDEA give another capacity by utilizing the latitude /longitude facilitate as the key of information encryption.

The steps of LDEA algorithm are:

1. Transform latitude/longitude coordinate into float values.
 - The organization of arrange gained from the GPS collector is WGS84 (world geodetic framework 1984) characterized 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 scope.
2. Combine and hash
 - The transformation results of the above step are combined by performing a bitwise exclusive-OR operation.
 - Then, AES calculation is used and it creates a 128-bit key for the joined outcome.
 - Then, the key is part into two 64-bit values , called LDEA-keys.

B. Purpose of AES Algorithm

AES is based on a design principle known as a substitution - permutation network, a combination of both substitution and permutation, and is fast in both software and hardware. AES operates on a 4×4 column-major order matrix of bytes. The steps involved in AES algorithm are as follows:

Step 1: InitialRound

- AddRoundKey - each byte of the state is combined with a block of the round key using bitwise xor.

Step 2: Rounds

- SubBytes - a non-linear substitution step where each byte is replaced with another according to a [lookup table](#).
- ShiftRows - a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

- MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
 - AddRoundKey
- Step 3: Final Round
- SubBytes
 - ShiftRows
 - AddRoundKey.

C. Purpose of Haversine Algorithm

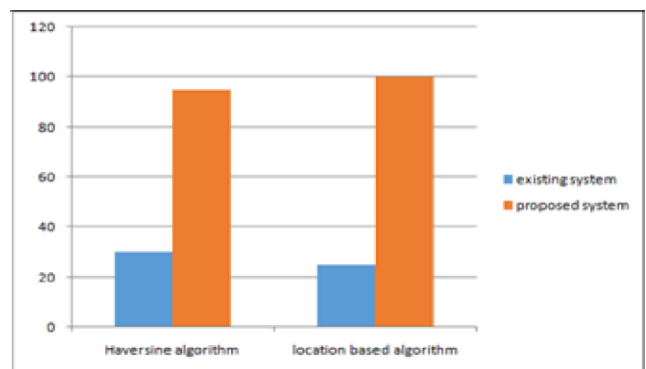
Haversine algorithm is used to calculate the TD (Tolerant Distance) region from target point to origin point. The origin point is the extreme point in the region. The steps are given below:

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. $A = \sin(\Phi/2) * \sin(\Phi/2) + \cos(O)*\cos(T)*\sin(\Lambda/2)*\sin(\Lambda/2)$
5. $B = \min(1,\sqrt{A})$
6. Distance = $2*R*B$

V. RESULTS

We carried out various operations and on the basis of positive and negative results generated we have jotted down some graphs . These are drawn keeping in mind the existing and the proposed system. The aim is to show estimate effects of the application on online banking environment.

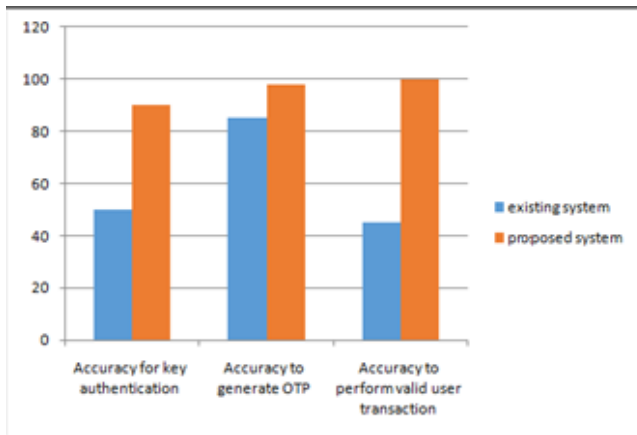
The below graph depicts the usage of have sine algorithm and location based algorithm . As it is clearly seen the use of haversine algorithm in the existing is every less (around 35%) as compared to our proposed system (around 95%) . Similarly the use of location based algorithm is 30% in existing system and 100% in proposed system.



The below graph shows the various operations carried out in the application. The accuracy achieved in key authentication is higher in proposed system (95%) than the existing system (50%).



The operation of generating and obtaining OTP has more promising results in the proposed system (97%). It can be clearly seen performing transaction for a valid user has better security and exactness in the proposed system (98%) as equated to existing system (45%) since our system provides a added security feature in the form of geographical position of the user.



VI. DISSCUSION / CONCLUSION

Our framework utilizes location based encryption technique for providing security to the banking application. The framework just permits verified individuals for doing exchange. Verification depends on location based encryption. Earlier geo-encryption had many drawbacks but the use of LDEA (Location Dependent Encryption Algorithm) in our system overcomes this drawback, it specifies the TD region (Tolerant-Distance), the secret key is only decrypted in the tolerant distance otherwise the message is not visible at the receiver side. This shields from unauthorized access. Also our system permits access of record/account from any area. All banking applications are location subordinate. Client location is being utilized for better insurance. Thus, Location based encryption and location-dependent data encryption algorithm (LDEA), were revised. Finally another security level was added to the present wellbeing endeavors utilizing location based encryption. This strategy can be utilized as a part of a few spots, for instance, banks, colossal associations, foundations and have the coveted execution.

REFERENCES

1. Aishwarya Rathod, Bhagyaxmi Kodre, Nida Sayyed, Ronak Sayta and Prof. Lata Sankpal, "Location Based Encryption for Secure Banking Transactions in mobile data environment" IJAERD, e-ISSN (O): 2348-4470, p-ISSN (P): 2348-6406, Volume 4, Issue 11, November -2017.
2. Aishwarya Nair, Ankita Devrukar, Karthika M. Vinod, Pallavi Lanke, "Protected Mobile Banking Using Location of Users", IJARCC, ISO 3297:2007 Certified, Vol. 6, Issue 4, April 2017.
3. Sourish Mitra, Avijit Chakraborty, 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.
4. Mohammad Ahmdian, Jalal Khodabandeloo, Dan C. Marinescu, "A security scheme for geographic information databases in location based system", IEEE southeast conference, 2015, Florida.
5. 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-

6. Amit Kushwaha, Vineet Kushwaha, "Location based services using android mobile operating System", Int. J. Adv. Eng. Technol., vol. 1,no. 1, pp. 1420, 2011.
7. 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.
8. Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta, "Location based services using Android", Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471480,2009.
9. 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.
10. 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.
11. Christian Becker, Frank Durr, "On location models for ubiquitous computing", 2005 9: 20-31, DOI: 10.1007/s00779-004-0270-2,2003.
12. 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.
13. Tomas Sander Christian, F. Tschudin, "Towards Mobile Cryptography", International Computer Science Institute, Berkeley, icisi.berkeley.edu