I J C T A, 10(8), 2017, pp. 589-596 ISSN: 0974-5572

Design and Implementation of Secure Access to Mobile Banking Using Location Based Encryption

Pallavi V. Dhade*, Meghana Lokhande and Tushar S. Nikumbh*****

ABSTRACT

The focus of this paper is to build an Android platform based mobile application to provide secure access to critical and confidential information in banks using location based cryptography, Geo-Encryption algorithm, LDEA algorithm and anti-spoof GPS. With compare to existing banking application which are location-independent, the paper is proposing banking application which is location dependent means only at specified location Cipher-text from cryptography could get decrypted. Any other attempt to decrypt data at another location, the process cannot decrypt it and cannot identify information about the plaintext. This approach is important in real time applications like military, cinema theater etc. The proposed application is providing flexibility to customer in such a way that he/ she will access his/her account from any location for completing their tasks. Though the idea of building a mobile banking application is not totally new, there are some drawbacks of existing system to overcome those problems, the proposed solution is provided. This paper reviews the fundamental concepts of Location based cryptography. Further, the paper emphasizes on the system design and implementation which is essential to overall banking applications.

Keywords: Antispoof GPS, Cryptography, Geo-Encryption, Location Based Encryption, LDEA algorithm

1. INTRODUCTION

To improve the quality life of people, Security plays an important role. Security not in the sense with physical but with the other aspect for example security to mobile banking, security for online ticket booking etc. With this approach, to provide security with different aspects which adopts the enhancement in human knowledge, information security plays crucial role to provide the solution. In today's era, there is more demand to data security and information security as more improvements in the technology. Because the data and information is crucial and is in the confidential form, some solution will be the necessity. With this necessity , users need some competent system where he/she can process and transfer the data with less efforts.

To provide the solution to the mobile banking for secure access, the paper is proposing an application which is based on android platform. The application is using location based cryptography, Geo-encryption algorithm and anti-spoof GPS. Compare to existing banking applications which are location independent, the proposed application is location dependent where the cryptography cipher text related to banking transaction, only be decrypted at a specified location. If any attempt to decrypt the cipher text at any other location will expose no information about the plain text and results in fail attempt. The user can access his/ her account from any location and is also providing security to physical attack by executing the fake

* Assistant Professor, Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, *Email: pallavi.dhade@gmail.com*

** Assistant Professor, Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, *Email: meghna.ingole1983@gmail.com*

*** Lecturer, MAEER'S MIT Polytechnic, Pune, *Email: nikumbh.tushar1618@gmail.com*

transaction. Using location based encryption, a new security level is added to existing security depth. This application allow the users to access their account after changing or moving their location. The necessity of Location is required only in encryption and decryption process. It also uses Anti-spoof GPS to get accurate location using latitude and longitude.

In this paper, we have briefly elaborated and discussed some of security challenges of mobile banking. Then discussion continue with information about "location based cryptography" and "Geo-Encryption" algorithm and antispoof GPS for doing the banking transaction. Finally using "Geo-Encryption" we have proposed a model for improving the security of data access control in mobile banking.

2. CHALLENGES IN EXISTING SYSTEM

2.1. Challenges observed in cloud computing

Cloud computing is a model to access information and services using existing technology and Internet infrastructures that allows establishing communication between clients and the server [1, 2]. We can imagine cloud computing as the ability of sharing computational resources among many different users [3]. Customers do not have the actual physical infrastructure and they just pay a subscription fee to the cloud provider and gain access to resources and infrastructure clouds with minimal effort or interaction with the service provider. Few of the challenges are : Insider access, Access Control, Identity Management etc. The cloud service provider may gain an unauthorized access to the data as the data is available on cloud.

2.2. Challenges observed in tradition security techniques

In traditional cryptography algorithms (for example: asymmetric key algorithm) , the keys are generated. If the key is stolen by an unauthorized user, then it is easy for him to decrypt the data.

3. FEATURES OF LOCATION BASED CRYPTOGRAPHY

3.1. Location Based "Identity"

In cryptography "identity" Components are important to us. As a typical example we can mention the name and national ID card. So are scans of fingerprints or residential address, work address and so on. Data can be encrypted so that only the person who holds the private key can decrypt it (public key or private key). Here the question arises: can we have other forms of "identity"? What else can be used as an identity? Another question arises (in fact, it is the answer to the previous question): Can we use the place where we have a presence as our "identity"? Is it possible to use it in encryption? Physical presence in a particular location at a specific time, can be our "identity" in cryptography [5]. For example, we know the role of a bank-teller behind a bullet-proof bank window not because she shows us her credentials but by merely knowing her location. Another question arises: for what applications is this method is more suitable? For example, assume military base "A" wants to communicate with military base "B" (obviously military communications must be confidential). In the traditional approach the two bases can communicate by exchanging a secret key. One problem that arises is when an honest officer who carries the key is captured by enemy andhe's tortured and he finally reveals the secret key. As a result with the secret key the enemy can decrypt the messages[5].We trust physical security more. So maybe we're able to guarantee somehow through some physical means that those who were inside a particular geographical region are approved. As a result (in the previous example) those who have physical presence in the military base "B" or get into it, are approved. So the message that is encrypted and sent from military base "A" to military base "B" will only be decrypted by a person or persons who have physical presence in a particular geographical location (military base "B") and no one else can't decrypt it [5].

3.2. Location Based "Accsess Control"

Another usage for the "Location Based Cryptography" is "Access Control". A person who is physically present in a particular location can make use of the resources. For example, individuals who are physically present in a particular room are able to use the printer. If they leave the room, they will not be allowed to access printers anymore and many such examples[5].

3.3. Geo-Encryption Principles

"Geo-Encryption" is a method based on adding a new security layer on the available encryption protocols structure using the recipient's location information. Encrypted data can be decrypted and readout only on a particular geographical point at a specific time [6]. The particular point can be exactly where we want the information to be decrypted, even with a radius of a few centimeters. It can also be within the walls of a room on a particular floor. Next-generation GPS and highly accurate GPS like the military types that are "AntiSpoof",perform with an accuracy of 1cm. They have the ability to measure a specific location very accurately with latitude, longitude and height.

The idea of using "Geo-Encryption" was proposed and developed by "Logan cott" and "Dorothy E Denning" for the first time. They used Geo-Encryption to encode files related to films in the manufacturer studios and send them to the Cinema theaters through a wide network like the Internet. The sent files could be downloaded in all the areas which were covered. But they could be decrypted only on the location of the considered cinema theater at a specific time. The geographical information of the cinema theater must be matched with the information used in the sender's file [6,10]. As we know, using symmetric encryption (private key) in terms of computational and implementation is very fast. Asymmetric encryption (public key) method uses both the public and private keys and its security is very high. On the other hand due to the difficulty in computing its performing rate is low. Therefore in the "Geo-Encryption" algorithm a combination of symmetric and asymmetric encryption is used[11].

The public key algorithm is used to secure and distribute session keys and the symmetric encryption algorithm is used to encrypt the information (Fig. 1). The sender uses the session key (which is random) and a symmetric algorithm like "AES" to encrypt the desired data. Then using location information, time

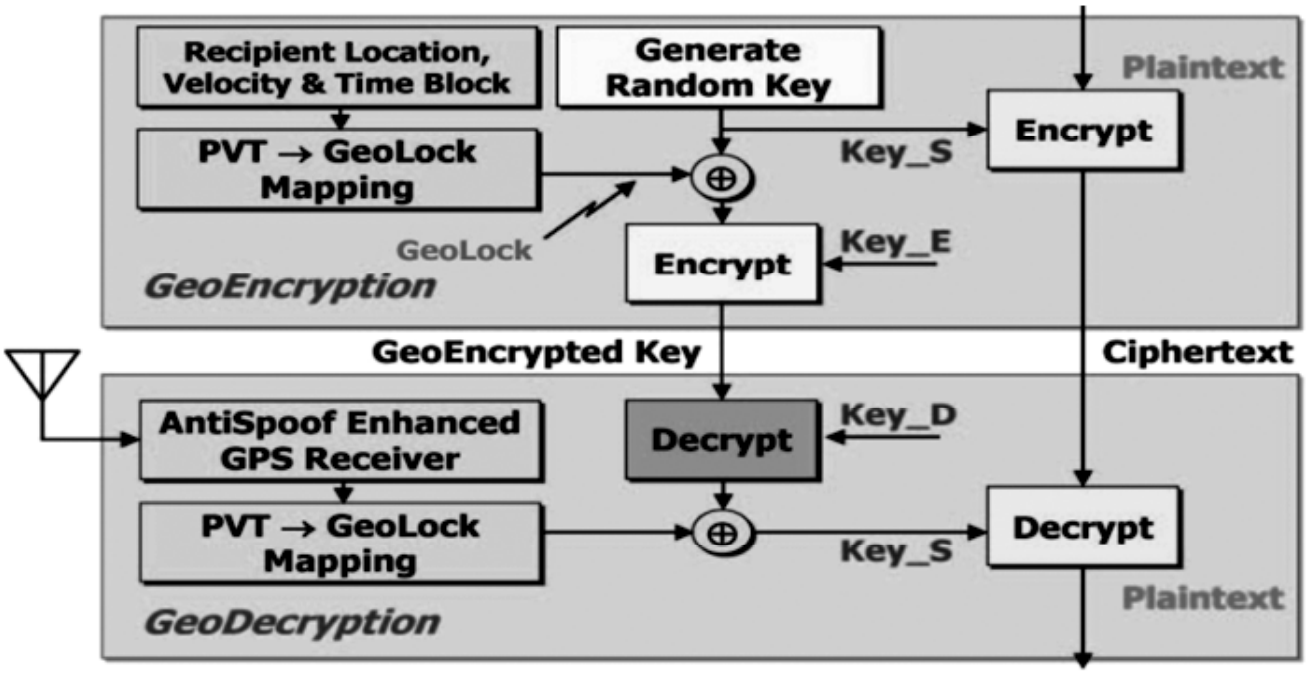


Figure 1: GeoCodex GeoEncryption algorithm [7].

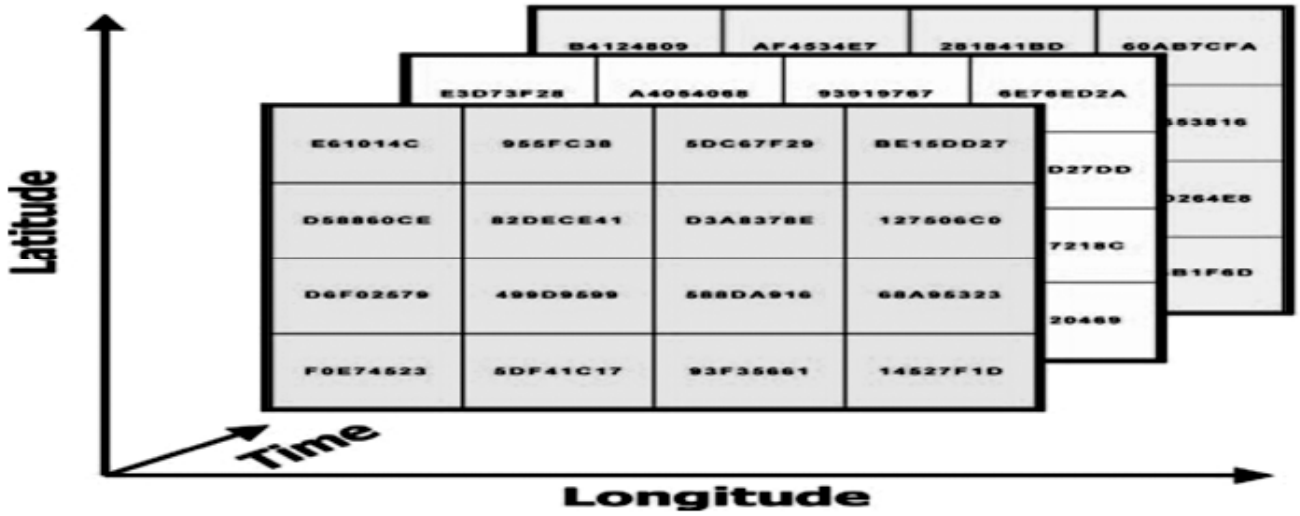


Figure2: PVTGeoLock mapping function [7].

and speed of receiver (PVT) and a mapping table makes a certain code named "Geolock" (Fig. 2). Last the session key is encrypted by the certain code (Geolock) and by using an algorithm such as "RSA" the results are encrypted and sent [7]. The receiver using their PVT information obtained via positioning tools (Anti-spoof GPS) a nd the mapping table, calculates the Geolock and then: Geolock encrypted key = Session key. [7, 8]

4. OUR PROPOSED MODEL

In today's era, the most important thing along with physical security is data security. As we know, many times, there will have an unauthorized access to data, many of the users are concerend about this problem. For example, the confidential information from the bank, so that there is probability to have an access to this critical and confidential information by unauthorized users. So to provide the security we are prosposing this novel approch for mobile banking to get secure access through location based cryptography as the data of the bank is already stored on cloud.

In our method , the user's geographical position and location are the key parameter for implementation purpose. With the location and position as identity, we are adding a new security level to existing measures of mobile banking. Our proposed method is more valid for banks, institutions, companies, military and many more like this where transfer of data and security to the data is concerned. Only the constraint is that we require an Anti-Spoof and accurate GPS, Mobile and Geo-Encryption algorithm on cloud. We are assigning some tags to the data of every user who is using this application, so for different user different tags are created. These tags contains name of the person, and information about user's profile. These tags are then properly maintained in the table with the proper indexing. Then each of the tag in the given table will directly map to the user's geographic location and to access data from the database, the current time frame is used which is shown in fig. 3. Manually as well as automatically, these tags and values are added to sqlite user database. In this model, on the cloud, the whole information about the user is stored by banks and to access account, the user should be authorized to the bank. If the user is authenticated one, then he/ she is allowed to access accountant for doing the transaction through mobile banking.

We have considered tolerance distance in order to avoid inaccuracy and inconsistent problem of GPS receiver[9]. To calculate this tolerance distance, we have used LDEA algorithm.

The purpose of LDEA is mainly to include latitude/longitude coordinate in the data encryption to restrict the location of data decryption. A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver[9]. The mobile clients transmits a target latitude/longitude coordinate

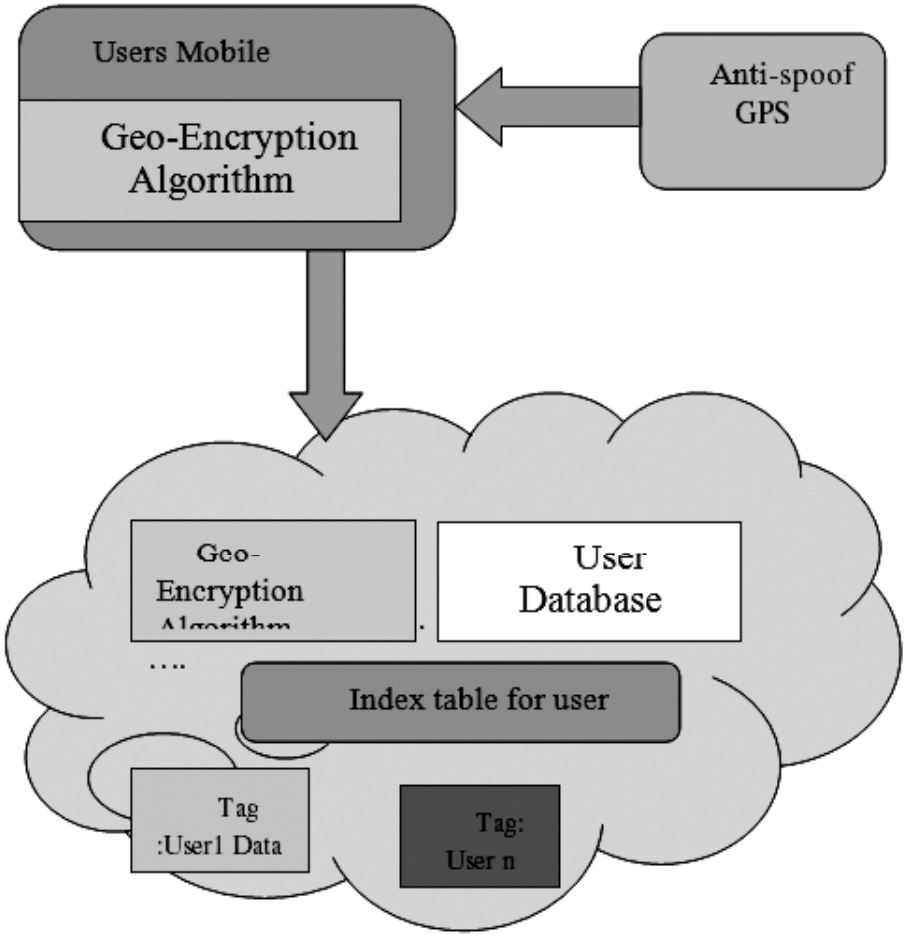


Figure 3: Outline of proposed model

and an LDEA key is obtained for data encryption to information server. The client can only decrypt the ciphertext when the coordinate acquired from GPS receiver matches with the target coordinate. They makes the use of random key (R-key) an addition to the LDEA key to improve security. LDEA protocol makes the use of static location. It is difûcult for a receiver to decrypt the cipher text at the same location which is exactly matched with the target coordinate. It is impractical by using the inaccurate GPS coordinate as a key for data encryption [9].

The below steps are follow for appropriate sequence of operation:

- First, For doing the transaction ,the user's tag is sent from the mobile to the bank cloud only after doing registration by entering userid and password.
- On the bank cloud the tag will be searched and retrieved.
- The retrieved tag checks database which is on the cloud.
- The information about the tag, will be retrieved.
- The data about transaction is encrypted using tag information and Geo-Encryption algorithm which is encryption key for the going transaction and sent it to the user.
- User's mobile gets location information from the GPS and the encrypted data about transaction.
- Then calculates the Geolockcode by using the mapping table
- Geolock key + encrypted key = Session key
- At last decrypts the data using the session key.

5. IMPLEMENTATION DETAILS

The proposed model consist of following modules:

1. Registration and Login
2. Encryption Key generation module
3. OTP Generation module
4. Location based encryption module.
5. Session key generation module using GPS Position
6. Location based decryption module.

The flow of the proposed model is shown in fig. 4.

1. User must have to register first for the mobile banking through an android app and then perform login by entering userid and password.
2. For making the transction, User need to enter the Encryption key which is already been send to E-mail.
3. For the current transaction OTP is is required and sent to respective mobile.
4. After submitting Encryption Key and OTP, User will login into the system successfully
5. In transaction user can credit or debit his account by setting current location by with the Tolerance Distance region.
6. If the user does not credit or debit the account within a Tolerance Distance region then it fails to process.

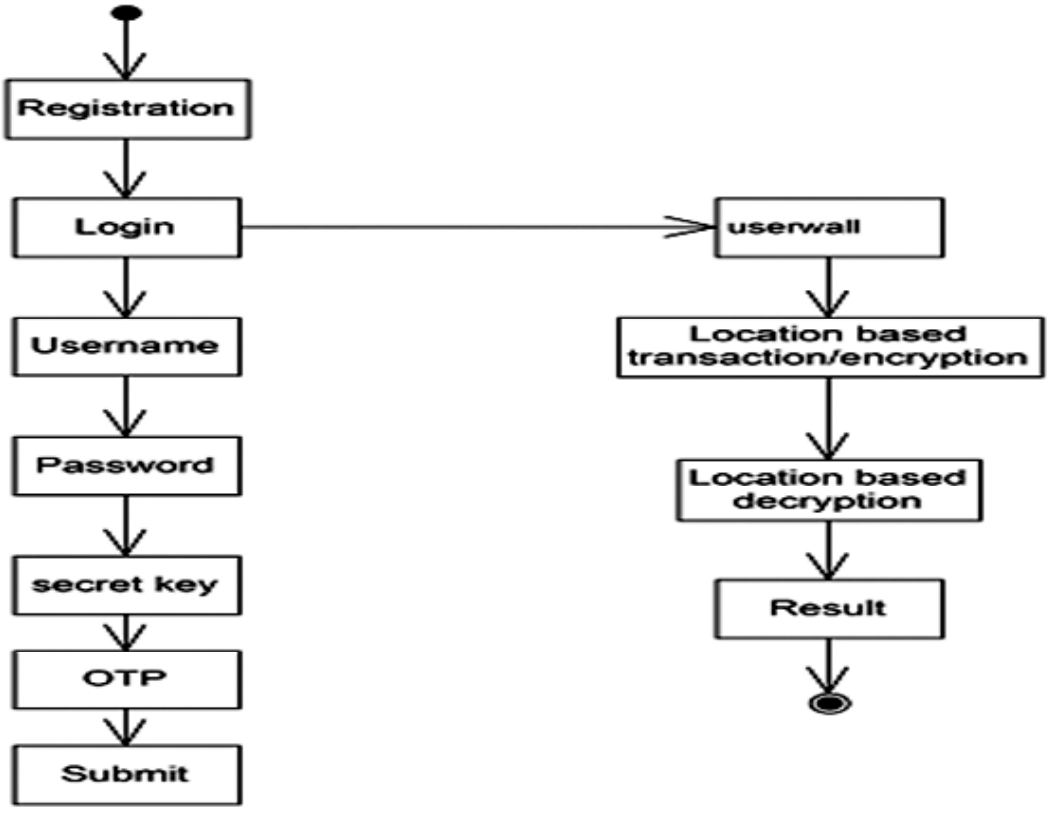


Figure 4: Flow of the proposed model

6. RESULT

A prototype was implemented to illustrate and evaluate the used algorithm. Seven screen shots of the prototype are shown in Fig. 5.

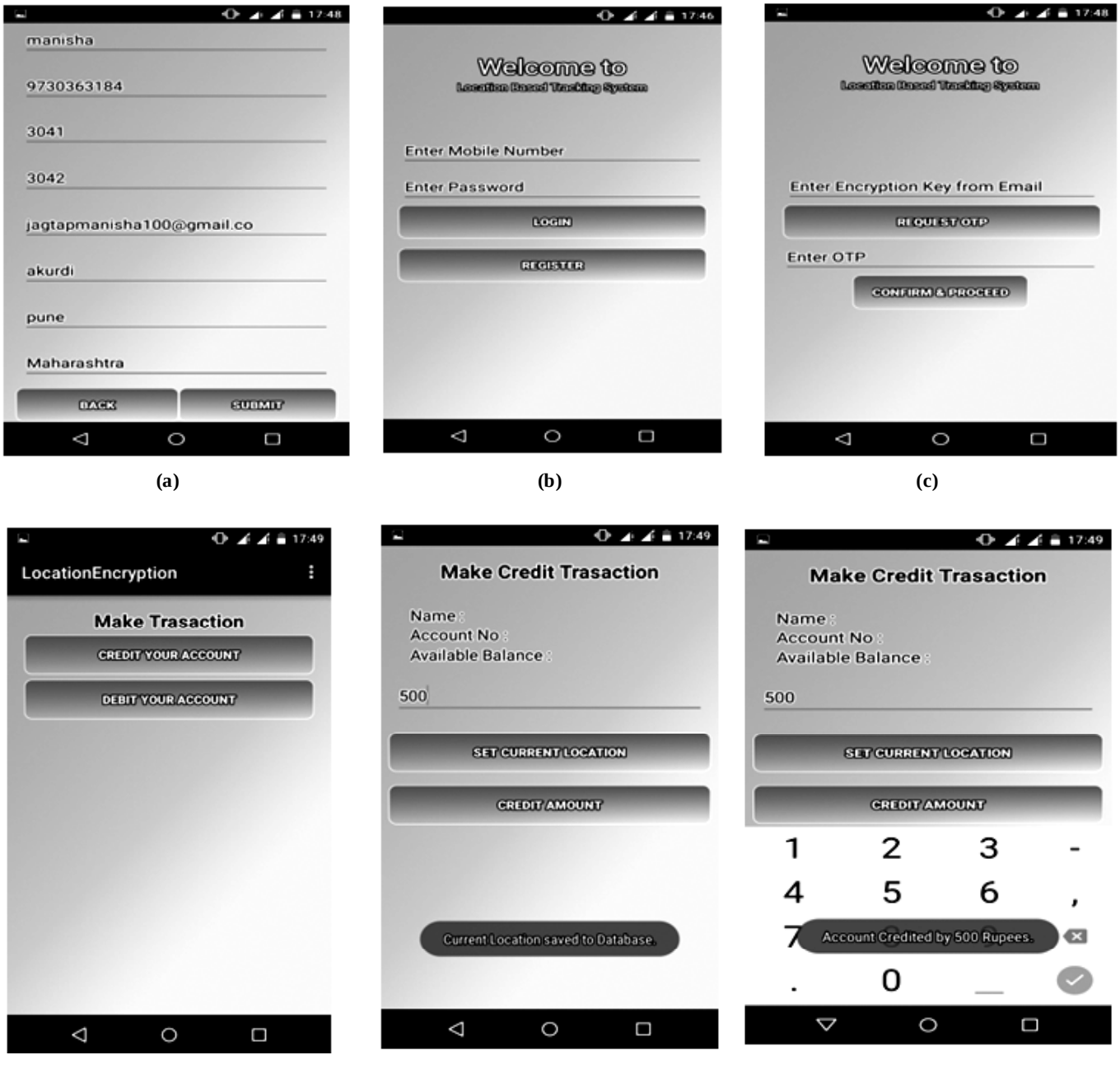
In Figure 5(a), the user have to register first for the mobile banking android app. In Figure 5(b), the user will login successfully to the system by using registered mobile number and password

Figure 5(c), the user has to enter encryption key and OTP for making transaction

Figure 5(d) For making transaction, user will either credit or debit through account

Figure 5(e) For crediting or debiting operation user has to set current location

Figure 5(f) transaction get completed.



(a) **(b)** **(c)**

(d) **(e)** **(f)**

Figure 5: Experimental Result

7. CONCLUSION

One of the most challenging issues in mobile banking is to provide the security to data access control as it is available on cloud . Everyday new challenges come in security and many technologies are working to resolve the issues and challenges. We have proposed the security to mobile banking through location based encryption, where the whole approach is based on location. In this paper, security to mobile banking is briefly discussed. The features of Location based encryption ,Geo-Encryption, Anti-spoof GPS and LDEA algorithm were also considered. Finally, with location based encryption , a new security level is added to the existing security . Through this paper we have designed and implemented a secure access to mobile banking using above discussed algorithms with the expected performance.

REFERENCES

[1] Barrie Sosinsky: “Cloud Computing Bible,” 1th ed, January 11, 2011.

[2] Weiss, A. (2007): “Computing in the Clouds”. Networker, Vol. 11, No.4, pp: 16-25, December 2007.

[3] David S. Linthicum: “Cloud Computing and SOA Convergence in your Enterprise”, Pearson, 2010.

[4] Meer Soheil Abolghasemi, Mahdi Mokarrami Sefidab, Reza Ebrahimi Atani: Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing, 978-1-4673-6217-7/13/$31.00 c 2013 IEEE, 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)

[5] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky: “Advances in Cryptology”, CRYPTO 2009 Lecture Notes in Computer Science Volume 5677, pp. 391-407, 2009.

[6] Logan Scott & Dorothy E. Denning: “Location Based Encryption & Its Role in Digital Cinema Distribution”, Proceedings of ION GPS/GNSS 2003, pp 288-297.

[7] D. Qiu, “Security Analysis of Geoencryption: A Case Study using Loran”, proceeding of ION GNSS 2007.

[8] D. Qiu & Sherman Lo & Per Enge & Dan Boneh, “Geoencryption Using Loran”, Proceeding of ION NTM 2007.

[9] 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, 2008 Asian Network for Scientific Information

[10] Logan Scott & Dorothy E. Denning: “Location Based Encryption & Its Role in Digital Cinema Distribution”, Proceedings of ION GPS/GNSS 2003, pp 288-297

[11] D. Qiu & Sherman Lo & Per Enge & Dan Boneh, “Geoencryption Using Loran”, Proceeding of ION NTM 2007.