Scientific Journal of Impact Factor (SJIF): 5.71

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

International Journal of Advance Engineering and Research Development

Technophilia-2018.

Volume 5, Special Issue 04, Feb.-2018 (UGC Approved)

Provide Security To Mobile Banking Using Location Based Encryption

Chougule Nikhil S[1], Gatkal Anup N[2], Parave Sujay S[3] ,
Khaladkar Utkarsh R.[4] And Prof. Pokharkar S. R.[5]

Department of Computer Engineering, Jaihind Polytechnic ,Kuran

Abstract – *Location based encryption which we developing banking application. In Present finance request which is place in-dependent, so which is place dependent emerging finance appeal. Now that Cryptography Cipher-text decrypted at a measured place i.e. location-dependent method. In that decrypt documents at extra place, once the decryption method flops and tells there no data around the plaintext. This is main in actual time use, example in army base use, cinema acting. Our system is elastic which enough to deliver access to customer to his/her version from any place. For emotional round by virtualization in system also run end, in which client is allowed to make false industry for his/her physical security purpose.*

Keywords- *accurate GPS ,Cryptography, Geo-Encryption, Location Based, Security.*

I. INTRODUCTION

Using Place Based Encryption we are developing banking application. In Present finance request which is place in-dependent, so which is place dependent emerging finance appeal. Nowadays that Cryptography Cipher-text decrypted at a measured place i.e. location-dependent process. In that decrypt documents at extra place, once the decryption method flops and tells there no information about the plaintext. This is important in real time application ,example in military base application ,cinema theater. Our system is flexible which enough to deliver admission toward customer to his/her account from any location. Toward physical spasm by virtualization in scheme similarly deliver answer, in which client is certified to do false deal for his/her physical security purpose. In human life security is always needed and people have been looking for physical and financial security. With help of remote basic we encrypt the data after decrypt it. In that cryptography "identity" is important ,we can specify name, address, identification as individuality, but we can also give home (i.e. Physical presence at a particular location) as character. This place can be used in encryption.

II. PROPOSED SYSTEM

It is very important to provide security to online banking transactions. Users (individuals or companies) are concerned regarding the contact to the documents by unauthorized users. Currently information is some crucial and confidential information from a bank, or a corporation and etc. In data security actually the requirement of access data for banking application and is a very important . We have a tendency to use the user's location and geographical position and that we can add a security layer to the present security measures. Our resolution is additional acceptable for banks, big companies, establishments and examples like this. The only cause we need is compare to step Anti-Spoof and true GPS those businesses will give to workshop for. Also applying the location-dependent data encryption process (LDEA), on the fog and also the user's mobile (which is connected to the GPS) is necessary. We will tag the data. Tag holds name of the company or an specific who workings inside the company (for example the company's boss).These tags are located in secondary grade file chart that mentions to the customer's physical place and also the timeframe said of to contact data, in a storage. These tags and prices of the storage are often extra physically or automatically. For example, reason that a bank stores some information within the database and solely the controller will have access to that. The accountant's room is on the third surface of the bank's building and accountant's operating hours are from eight am to three pm. we will create the files within the cloud accessible solely among the accountant's room and his operating hours (in addition to the present security measures). As stated the new age group "Anti-Spoof" GPS is really right and force deal us the space, longitude and height correctly.

As a effect we will boundary the information access to the area place on a exact base of a shop and a stated timeframe. Additional sample: the data that may be available only in the head's area of several divisions of a set or a house. Within the traditional system, once users try to access the data, they use normal confidence actions and thus get contact to the cloud.

III. METHODOLOGY

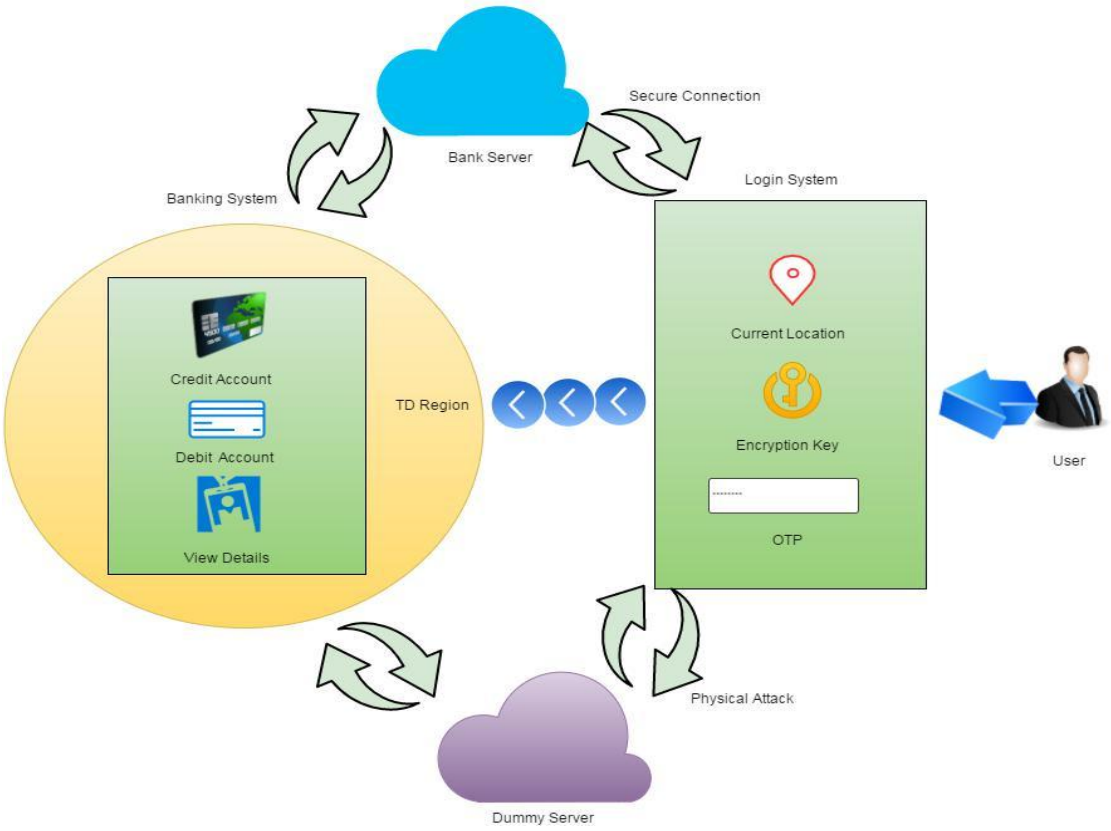


Fig 1: Architecture diagram of proposed system

In this system, first user need to do registration for that he/she needs to enter his/her valid email Id and password. It will generate secret key which would send to user's email id and OTP (on time password) on mobile as a text message in inbox. After that while login user need enter the secrete key and OTP from email account and mobile respectively. Then user need to enter TD (Tolerance distance) region (i.e within how much distance user could do his/her transaction that would be beyond 10km). Then user would able to do some activity like credit, debit etc. So within if user were not able do to transaction within define TD region then message will pop out i.e no coverage. That means transaction will stop. So even if user's transaction go beyond TD are securing data by location based encryption as data will be secure within TD and beyond TD also. System will also give solution to physical attack using virtualisation, allow user to perform fake transaction for his/her security purpose. In this case, if attacker ask user to do transaction forcefully, he/she need to enter valid email id and while entering password required to enter password with one additional digit or alphabet etc. Then transaction would go to dummy server. It will show pop out message i.e transaction successful but actually it will perform fake transaction and user data will be

3.1. The proposed system consists of the Bank server, Dummy server, User.

3.1.1. User:

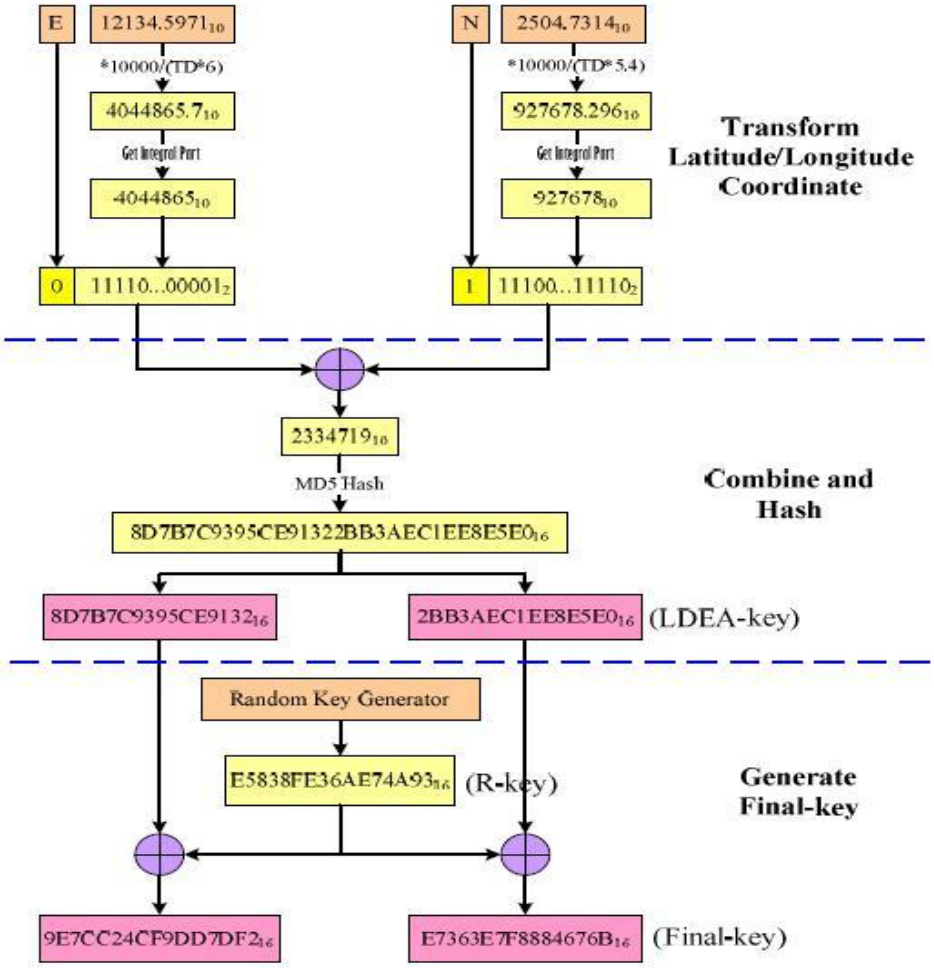
First user login his/her account which is registered then user current location is fetched then after cross examined with the registered location which is similar then user will proceed with additional transaction else the transaction are going to be closed.

3.1.2. Bank Server:

It is main server in that saving the information of user transaction. User will credit, debit and enquiry regarding his/her account details.

3.3.Algorithm

LDEA(Location dependant Data Encryption Algorithm) Algorithm:



LDEA Algorithm

1. Transform latitude/longitude coordinates:

   The directs attained from GPS phone are increased by 10000 to be an number. Then, number is divided by a value parallel to the TD. In progress, one bit is put in opposite of the basic part of the above result. The bit is zero for east and south and one for west and north.

2. Combine and hash:

   The change grades are mutual by acting a bitwise exclusive-OR operation. Then, MD5 hash process is used and makes a 128-bit abstract for the mutual result. Then, abstract is divided into two 64-bit prices, called LDEA-keys.

3. Generate final-key:

   A meeting key (R-key) is made accidentally with the same distance of LDEA-key. LDEA -keys are exclusive-OR with the R-key individually to produce the final-keys. Then these two final-keys are used as the secret key.

IV.CONCLUSION

The largest risk to online banking is still malicious code executed not carefully on the end-user's computer. The enemies try to target the weakest link. Once the attacker has control over a user's computer, he or she can modify the information flow to his or her advantage. For example we near a culture where automatic material means are better and cryptography will last to rise in status as a safety tool. Automatic networks for banking, shop, account device, profit and deal transfer, data loading and recovery, thin handling, and rule submissions will essential better ways for access device and data security. The info safety can be simply done by using Cryptography method. DES is now careful to be unconfident for Certain request like banking

REFERENCES

1. Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino, Fellow, Context-Based Access Control System for Mobile Devices IEEE,2015.

2. Hsien-Chou Liao and Yun-Hsiang Chao, LDEA : Data Encryption Algorithm Based on Location of Mobile Users IEEE Transaction on Cyber Security

3. Becker, C. and F. Durr, 2005. On Location Models for Ubiquitous Computing. Personal and Ubiquitous Computing, 9 (1): 20-31, Jan. 2005.

4. Eagle, N. and A. Pentland, 2005. Social Serendipity: Mobilizing Social Software. IEEE Pervasive Computing, 4 (2), Jan.-March 2005.

5. Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location-Tracking Applications. IEEE Security & Privacy Magazine, 2 (2): 28-34, March-April 2004.

6. Liao, H.C., P.C. Lee, Y.H. Chao and C.L. Chen, 2007. A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. In: Proc. the 9th International Conference on Advanced Communication Technology (ICACT 2007), 1: 625-628, Feb. 2007.