IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Protected Mobile Banking Using Location of Users

Aishwarya Nair[1], Ankita Devrukhkar[2], Karthika M.Vinod[3], Pallavi Lanke[4]

Indira College of Engineering and Management, Parandwadi,Tal Maval Pune

Abstract- Mobile android applications often have access to sensitive data and resources on the user devices. Misuse of this data by malicious applications may result in privacy breaches and sensitive data leakage. An example would be a malicious application surreptitiously recording a confidential business conversation. The problem arises from the fact that android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. In many cases, however whether an application get a privilege depends on the specific user context and thus we need a context based access control mechanism by which privileges can be dynamically granted or revoked to applications based on the specific context of the user. As compare to current banking application which are location-independent, we are developing banking application which is location dependent. It means in Cryptography Cipher-text can only be decrypted at a specified location i.e. location-dependent approach. If an attempt to decrypt data at another location is made, the decryption process fails and reveals no information about the plaintext. This is important in real time application, example in military base application, Cinema Theater. But our system is flexible enough to provide access to customer to his/her account from any location. Our system also provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

Keywords- Location Based System, Global Positioning System, Tolerant Distance, And Dummy Server.

I. INTRODUCTION

The reason behind the location based services is to provide services to mobile users based on their knowledge of their locations. Services such as digital map services, real time traffic information which are delivered to Smartphone user's current location to reduce data transmission, providing dynamic guidance services according to the user's location and current traffic condition; user can request for nearest cinemas, ATMs, restaurants etc. Location based services offers lots of benefits to Smartphone user's. For the mobile users, the example of location based services is:

- Mobile Phone user can request for nearest business or service, such as banks, hotels, shopping malls etc.
- Provide alerts, such as notification of traffic jam on nearby location.
- Mobile user would be able to find the exact way to reach any particular place.
- Any user can find his/her friend at any location or receiving the location of the stolen phone.

II. SYSTEM ARCHITECTURE

The system architecture is divided into two parts:-
1. User / Client Side.
2. Server Side.

Module details:

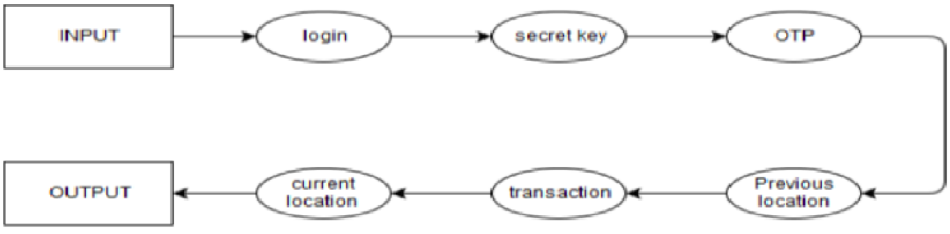
1. Location Based Encryption:

When the user goes to login there is must to input the encryption key. User location changed then the encryption key will also change.

2. Transaction:

There is Credit, Debit View Account Details operations which simply same as the Bank. In that the each operation is depends on the key and location and also on Tolerance Distance (TD) region.

Data Flow Diagram



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

3. Physical Attacks:

Physical Attack also work as same as main transaction. But it launches when the user types wrong credentials.

4. Encryption:

This module uses LDEA encryption algorithm to encrypt the easy-to-remember password. On the android application, this module decrypts the received password and displays it to the user.

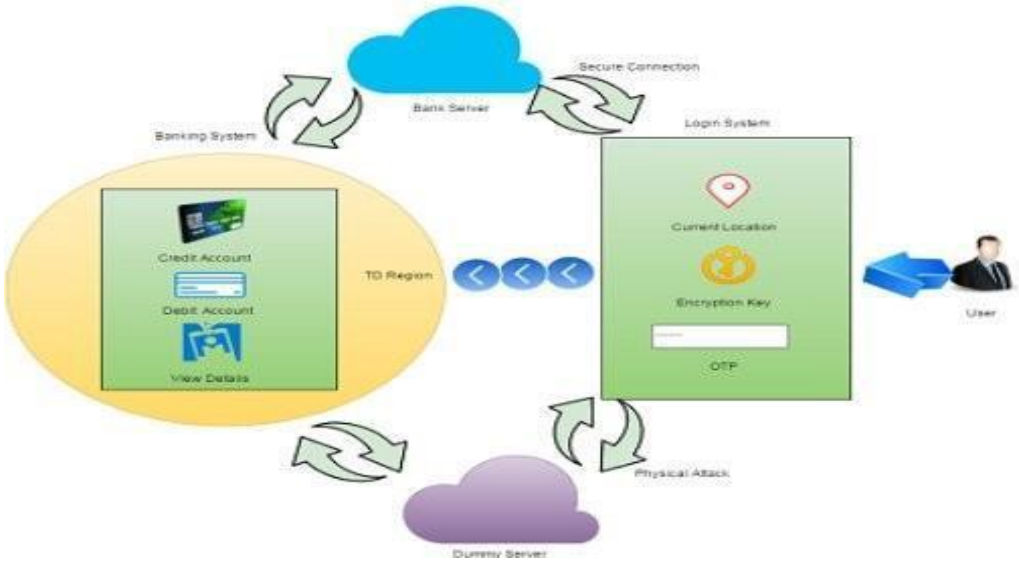
5. Android application:

This module consists of two phases one is registration and other is login phase. In registration phase user need enter the email id and an initial password. This email id is then stored in the database (SQLite). In login phase user need to enter the email id and an initial password.

6. Database:

The database server contains several tables that store each user information and including the account details. On the android application, it stores only one email id and an initial
Password.

System Architecture



III. COMPONENTS AND TECHNIQUES USED

Mathematical Model:

System Description:

- Input: Providing input in terms of email id, mobile number, TD region.
- Output: Avoids hacking of account using location and easy transactions.

Mathematical formulation:

S= fs, x, y, e, fma, DD, NDD g s =Initial State : no user login
e =End State: Allow access to authenticated user
x =Input values i.e.Login id, password, user's personal info x = f X1, X2, X3

X1 = Login id
X2 = Password

X3 = user's personal info y =Secure Transaction
y = f Y1, Y2, Y3g
Y1 = Fake Transaction For Secure Purpose
Y2 = dummy server
Y3 = SMS

Fma =Geo encryption algorithm. NDD =Non deterministic data x1 = Location of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Customer

DD =Deterministic data x2 = Customer Information

∑ Identify the Process as P
P= {location fetch, Encryption, decryption, key value generation}

∑ Success Conditions: our system provide solution to physical attack using virtualization, in which customer is allowed to perform fake transaction for his/her physical security purpose.

∑ Failure Conditions: If the system doesnt activate required module i.e. profiling.

IV. ALGORITHM

Following two algorithms are used to generate a random login indicator / token.

1. **Location Dependent Encryption Algorithm (LDEA)**

The purpose of LDEA is mainly to include the latitude/ longitude coordinate in the data encryption and thus to restrict the location of data decryption. A LDEA. When a target coordinate is determined for data encryption, the at the expected location. Since the GPS receiver is inaccurate and inconsistent depending on how many satellite signals received.

It is difficult for receiver to decrypt the cipher text at the same location exactly matched with the target coordinate.

It is impractical by using the inaccurate GPS coordinate as key for data encryption. Consequently, a toleration distance (TD) is designed in LDEA.

The sender can also determine the TD and the receiver can decrypt the cipher text within the range of TD. In order to verify the performance of LDEA, a prototype tool is also implemented and tested in an outdoor experimental site.

The experimental result illustrates that LDEA is effective and practical for data transmission in mobile environment

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the project report on 'Protected Mobile Banking Using Location Of Users '.We would like to take this opportunity to thank Almighty God for being with us and giving us the knowledge and understanding to make this project. We are grateful to Principal Dr. Sunil Ingole and Vice Principal and HoD Dr. Poornashankar for their indispensable support and suggestions. We would like to thank our internal guide Prof. Diagambar Patil for giving us all the help and guidance we needed. We are really grateful for his kind support. His valuable suggestions were very helpful. In the end our special thanks to our parents for giving us the moral support and encouragement for our project.

REFERENCES

[1] F. D. r. Christian Becker, "On location models for ubiquitous computing." *2015.*
[2] W. L. Yanchao Zhang, Wei Liu and Y. Fang., "Securing sensor networks with location-based keys.," *IEEE/IFIP Network Operations and Management Symposium (NOMS 2016), pp. 375–382, 2016.*
[3] S. S. Dillip Mohapatra, "A survey on location based data encryption algorithms for mobile devices," *IEEE ICC 2014 - Communication and Information Systems Security Symposium, p. 1005, 2014.*
[4] A. G. Sandeep Kumar, Mohammed Abdul Qadeer, "Location based services using android," *IEEE ICC 2014 - Communication and Information Systems Security Symposium, p. 7760, 2015.*
[5] M. B. P. E. J. R.J. Hulsebosch, A.H. Salden, "Context sensitive access control.," *University of Toronto, p. 1*
[6] E. D. Claudio A. Ardagna, Marco Cremonini, "Supporting location-based conditions in access control policies." *15th International Conference on Network-Based Information Systems, p. 582, 2012.*
[7] B.-G. C.William Enck, Peter Gilbert, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones." *MobiSys10, 2010.*