Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 5, May-2017

Data Security by Location Based Encryption for Banking Application

Waykar Rasika V[1], Naikodi Ravina J[2], Kadam Snehal M[3]

Department of Computer Engineering, Jaihind college of Engineering.

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. 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. However, most of the info encoding technology is location-independent. Associate degree encrypted knowledge is decrypted anyplace. The encoding technology cannot prohibit the situation of information cryptography. So as to satisfy the demand of mobile users within the future, a location-dependent approach, known as location-dependent encryption formula (LDEA), is planned during this paper. A target latitude/longitude coordinate is decided first off. The coordinate is incorporated with a random key for encryption. The receiver will solely decode the cipher text once the coordinate inheritable from GPS receiver is matched with the target coordinate. However, current GPS receiver is quality and inconsistent. The situation of a mobile user is troublesome to precisely match with the target coordinate. A toleration distance (TD) is additionally designed in LDEA to extend its usefulness. The protection analysis shows that the chance to interrupt LDEA is sort of not possible since the length of the random secret is adjustable. An image is additionally enforced for experimental study. The results show that the cipher text will solely be decrypted beneath the restriction of TD. It illustrates that LDEA is effective and sensible for knowledge transmission in mobile setting.

Keywords- data encryption, GPS, mobile computing, location-based service

INTRODUCTION

Security has always been an integral part of human life. People have been looking for physical and financial security. With the advancement of human knowledge and getting into the new era the need of information security were added to human security concerns. Data is encrypted only when person is having private key can decrypt it. In cryptography "identity" component is important ,we can specify name, address, id as identity, but we can also give place (i.e. Physical presence at a particular location) as identity. This place can be used in encryption.

Many ways are projected for the safety of information transmission. However, these ways are location-independent. The sender cannot prohibit the placement of the receiver for information cryptography. If the information secret writing formula will offer such operate, it's helpful for increasing the safety of mobile information transmission within the future. Therefore, a location-dependent encoding formula (LDEA) is projected in this paper. The latitude/longitude coordinate is employed as the key for encoding in LDEA. Once a target coordinate is set for encoding, the cipher text will solely be decrypted at the expected location. Since the GPS receiver is inaccurate and inconsistent looking on what percentage satellite signals received. It's tough for receiver to decode the cipher text at a similar location precisely matched with the target coordinate. It's impractical by exploitation the wrong GPS coordinate as key for encoding. Consequently, a toleration distance (TD) is intended in LDEA. The sender can also confirm the TD and also the receiver can decode the cipher text inside the region of TD. We are developing banking application exploitation Location primarily based secret writing, as compare to current banking application that is location-independent. It suggests that in Cryptography Cipher-text will solely be decrypted at a location i.e. location-dependent approach. If a shot to decode information at another location, the cryptography method fails and divulges no info regarding the plaintext. This is often necessary in real time application, example in military base application, Cinema Theater. However our system is versatile enough to supply access to client to his/her account from any location. Our system conjointly offer answer to physical attack exploitation virtualization, during which client is allowed to perform faux dealings for his/her physical security purpose.

PROBLEM STATEMENT

We are creating banking application using Location Based Encryption. As compare to current banking application which are location-independent, we are developing banking application which is location dependent. The

problem that is tangible and measurable is the financial fraud problem in online banking. Customers and banks lose money through illegitimate transactions. A less tangible and more difficult to quantify problem is the loss of privacy. Attackers that gain access to bank accounts have access to sensitive and incriminating information, such as account balances, transaction histories and information about debt. 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.

LITERATURE REVIEW

1. Technical report: Security of Online Banking Systems

AUTHORS: Sven Kiljan, Koen Simoens, Danny De Cock, Marko van Eekelen, Harald Vranken

This report discusses the security of today's online banking systems. this focus on both online banking using home and office computers, and mobile banking using devices such as smartphones and tablets. It compare our findings with a similar examination of a decade ago and present an overview of security issues in online and mobile banking that exist today.

2. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones

AUTHORS: William Enck, Peter Gilbert, Byung-Gon Chun

Today's smartphone operating systems frequently failto provide users with adequate control over and visibilityinto how third-party applications use their private data.We address these shortcomings with TaintDroid, an efficient,system-wide dynamic taint tracking and analysissystem capable of simultaneously tracking multiplesources of sensitive data. TaintDroid provides realtimeanalysis by leveraging Android's virtualized executionenvironment. TaintDroid incurs only 14% performanceoverhead on a CPU-bound micro-benchmark and imposesnegligible overhead on interactive third-party applications.Using TaintDroid to monitor the behavior of 30 popular third-party Android applications, we found68 instances of potential misuse of users' private informationacross 20 applications. Monitoring sensitive datawith TaintDroid provides informed use of third-party applicationsfor phone users and valuable input for smartphonesecurity service firms seeking to identify misbehavingapplications.

3. Location Based Services using Android MobileOperating System

AUTHORS: Amit Kushwaha1, VineetKushwaha

The motivation for every location based information system is: "To assist with the exact information, at rightplace in real time with personalized setup and location sensitiveness". In this era we are dealing withpalmtops and iPhones, which are going to replace the bulky desktops even for computational purposes. Wehave vast number of applications and usage where a person sitting in a roadside café needs to get relevantdata and information. Such needs can only be catered with the help of LBS. These applications include securityrelated jobs, general survey regarding traffic patterns, decision based on vehicular information for validity ofregistration and license numbers etc. A very appealing application includes surveillance where instantinformation is needed to decide if the people being monitored are any real threat or an erroneous target. Wehave been able to create a number of different applications where we provide the user with informationregarding a place he or she wants to visit. But these applications are limited to desktops only. We need to import them on mobile devices. We must ensure that a person when visiting places need not carry the travelguides with him. All the information must be available in his mobile device and also in user customized format

4. Location Based Services using Android

AUTHORS: Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta

Initially mobile phones were developed only forvoice communication but now days the scenario has changed,voice communication is just one aspect of a mobile phone.There are other aspects which are major focus of interest.Two such major factors are web browser and GPS services.Both of these functionalities are already implemented but areonly in the hands of manufacturers not in the hands of users
because of proprietary issues, the system does not allow theuser to access the mobile hardware directly. But now, afterthe release of android based open source mobile phone a usercan access the hardware directly and design customizednative applications to develop Web and GPS enabled servicesand can program the other hardware components like cameraetc. In this paper we will discuss the facilities available inandroid platform for implementing LBS services (geo-services)

5. On location models for ubiquitous computing

AUTHORS: Christian Becker AE Frank Du

Common queries regarding information processingin ubiquitous computing are based on the locationof physical objects. No matter whether it is the nextprinter, next restaurant, or a friend is searched for, anotion of distances between objects is required. A searchfor all objects in a certain geographic area requires thepossibility to define spatial ranges and spatial inclusionof locations. In this paper, we discuss general propertiesof symbolic and geometric coordinates. Based on that,we present an overview of existing location modelsallowing for position, range, and nearest neighbor queries.The location models are classified according to theirsuitability with respect to the query processing and theinvolved modeling effort along with other requirements.Besides an overview of existing location models andapproaches, the classification of location models withrespect to application requirements can assist developersin their design decisions.

MATHEMATICAL MODEL

Let 'S' be the system

Where

S= {I, O, P}

Where,
I = Set of input sensors
O = Set of output applications
P = Set of technical processes
Let 'S' is the system
S= {s, e, X, Y, Fma, DD, NDD}
s- Initial State: no user login
e- End state: Allow access to authenticated user
X- Input Login id, password, user's personal info.
Y- Secure Transaction.
Fma- Geo encryption algorithm.
DD- Deterministic Data
Customer information
NDD- Non Deterministic Data: Location of customer
Identify the Process as P
P= {location fetch, Encryption, decryption, key value generation}

SYSTEM ARCHITECTURE:

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 define TD region transaction would be secure even 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, his/her data will be secure. In this way we 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 secure.

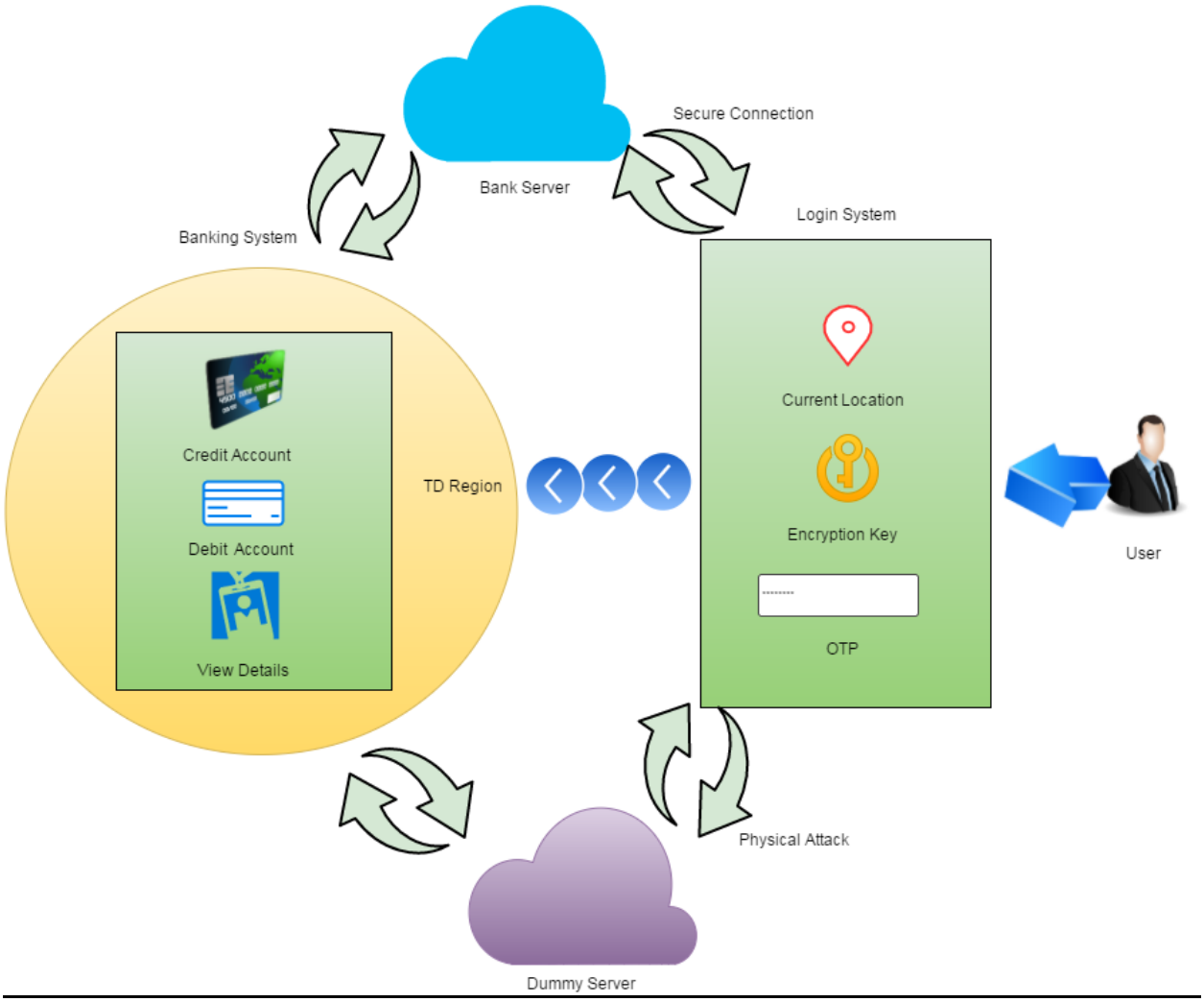


Fig:System Architecture

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : I3 processor 2.4 GHz.
- Hard Disk : 40 GB.
- Mobile : Android 4.4 onwards

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7/8.
- Coding Language : JAVA
- IDE : Android Eclipse
- Database : SQLite

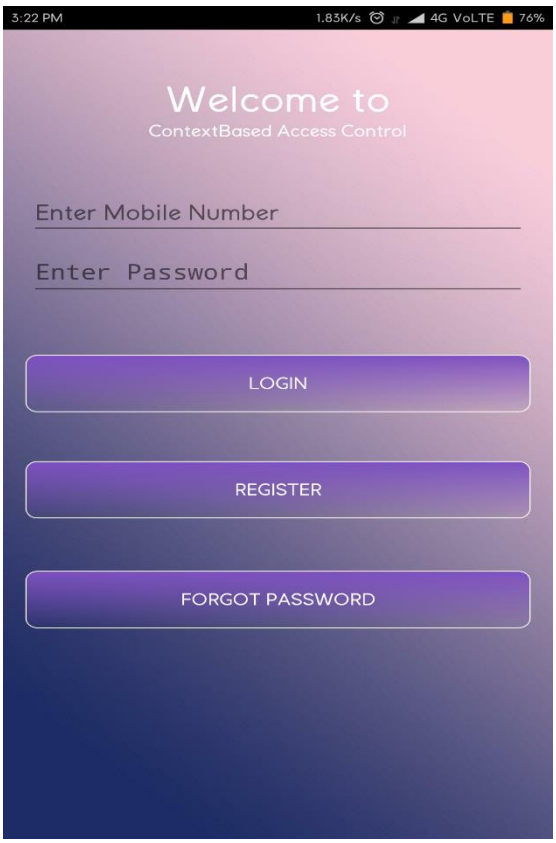
ADVANTAGES

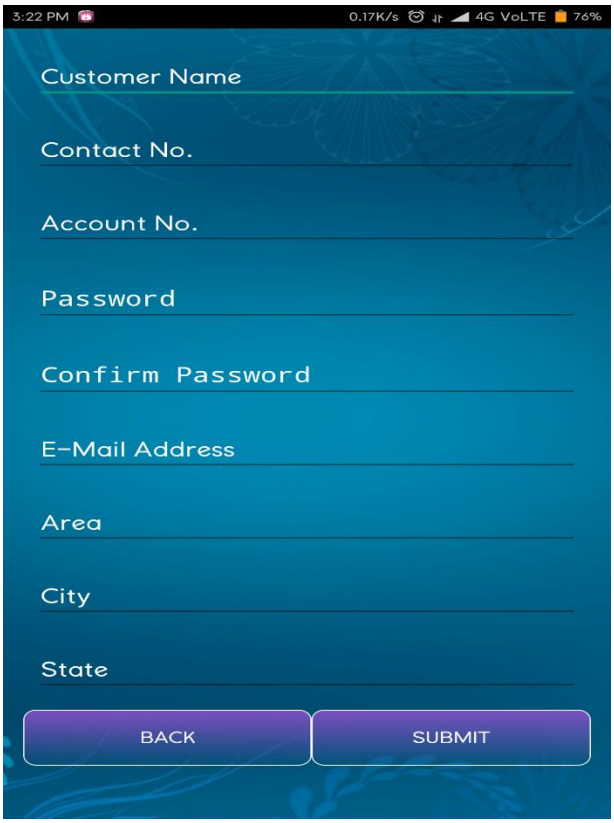
- Data security in cloud.
- It is more appropriate for banks, big companies, Institutions

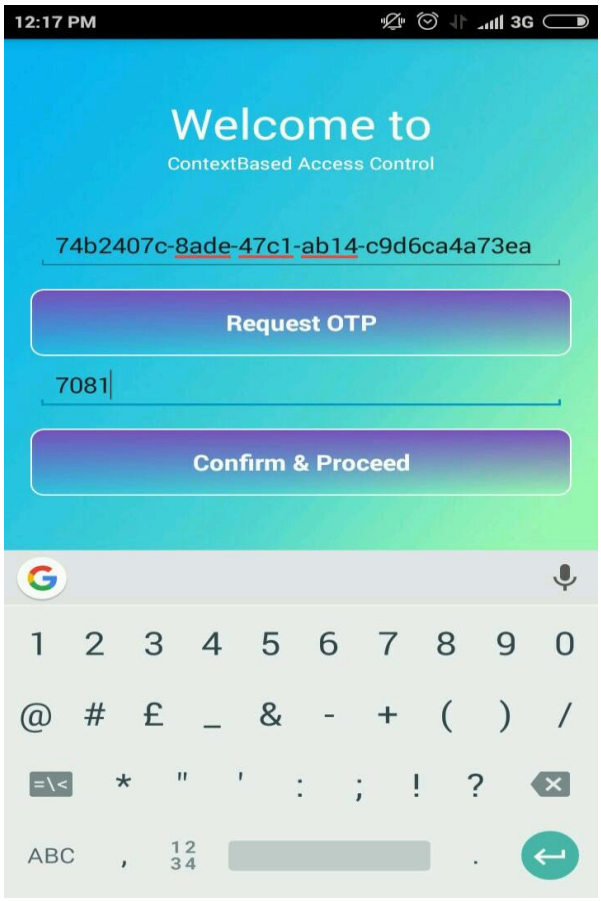
APPLICATION

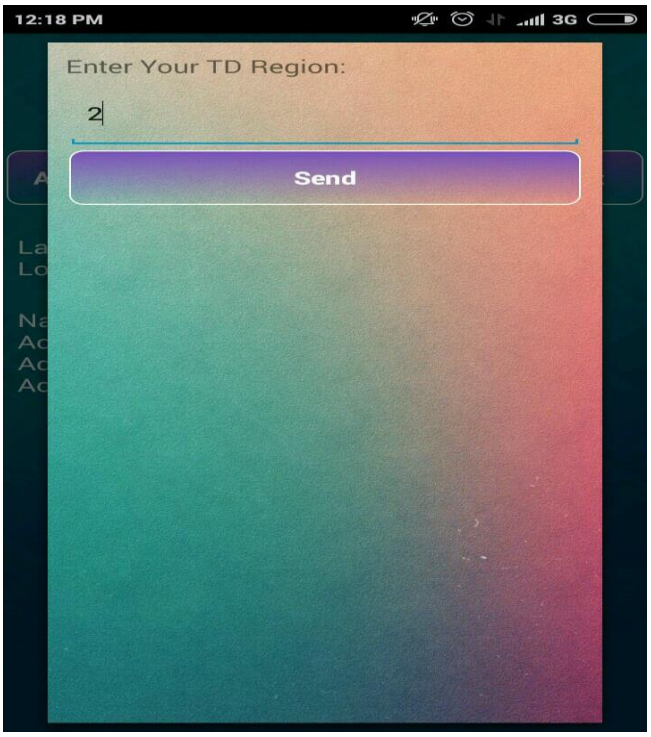
- Military-In military this technology can be used to keep the data secured from the attackers during wars.
- Banks-This technology can also be used in banking for the purpose of money transaction.
- Individual use-It can also be used to store one's confidential data. For e.g.: for business purpose.
- Multinational Industries-In Industries important data can be secure by using this technology.
- College-In college's important data can be secure by using this technology. For e.g. Question paper

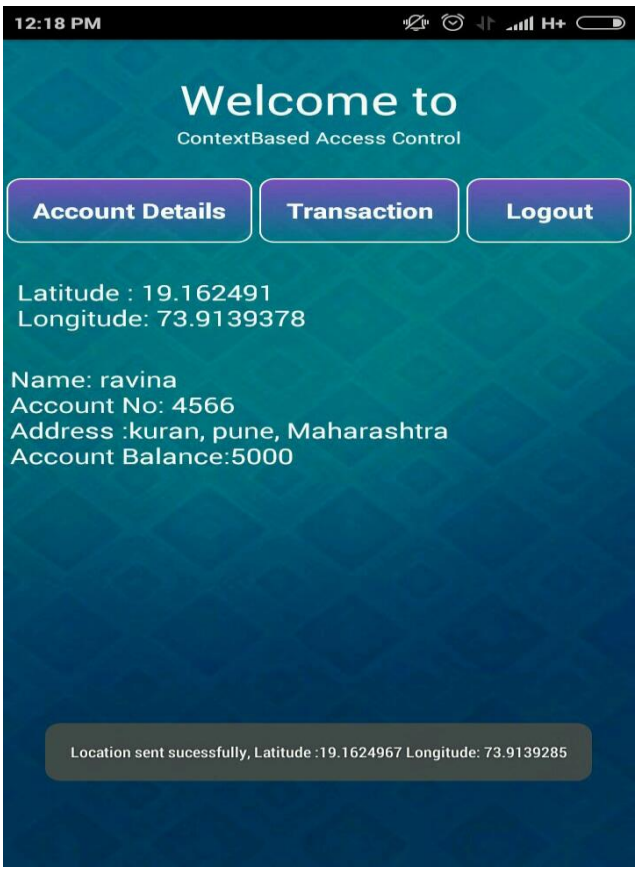
RESULT ANALYSIS

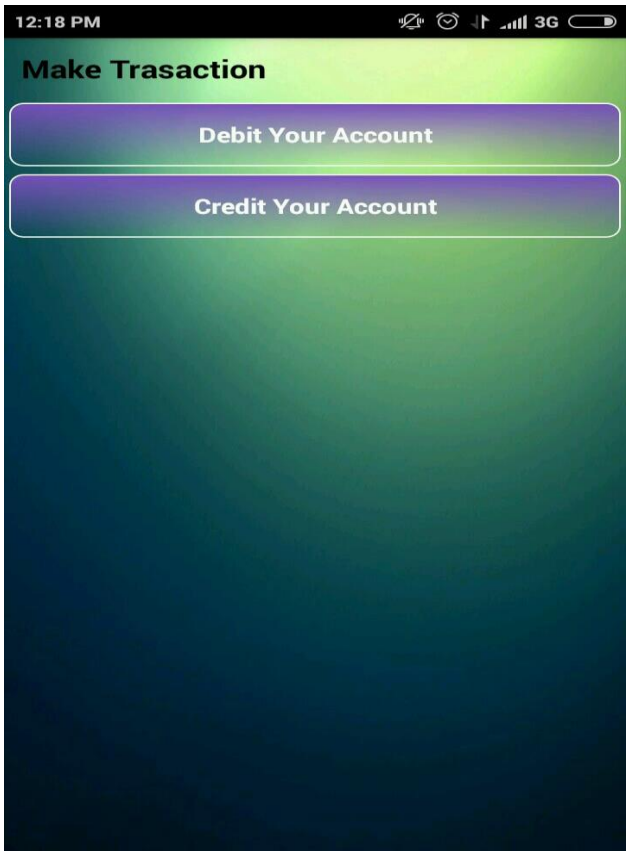


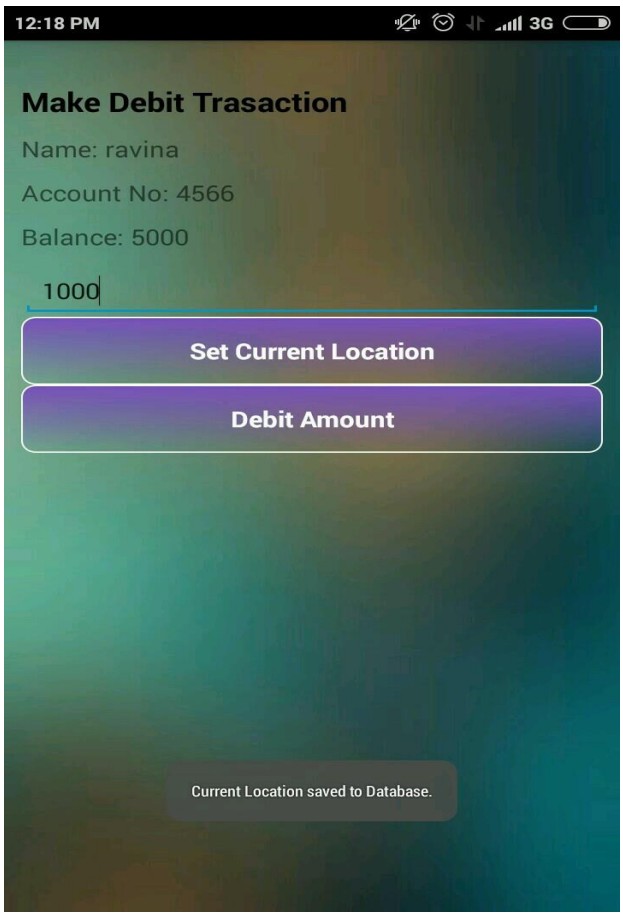


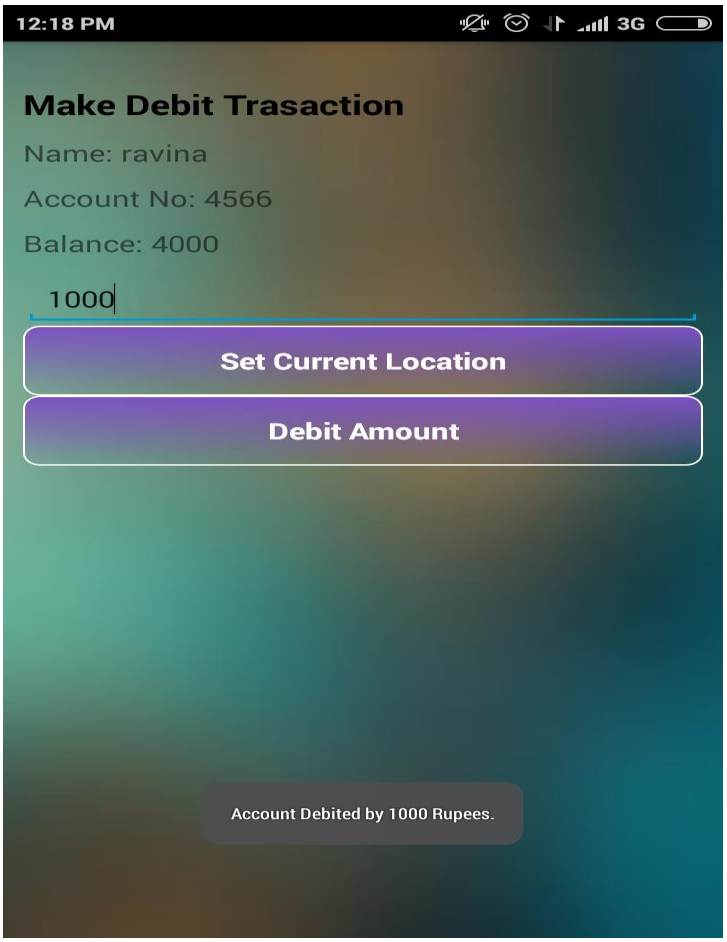












CONCLUSION AND FUTURE SCOPE

Hence we are implementing new security level to existing security measures, using location based encryption. We also provide solution to physical attack. Location based encryption and location-dependent data encryption algorithm (LDEA), were also reviewed. Finally a new security level was added to the existing security measures using location-based encryption. This method can be used in several places such as banks, big companies, institutions and have the desired performance.

Our system uses location based encryption technique for providing security to the banking application. Our system only allows authenticated people for doing transaction. Authentication is based on location based encryption. In case of physical attack, our system creates a virtual environment with extra key in password and allows fake transactions. Our system allows access of account from any location.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

REFERENCES

[1]R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, “Placeraider: Virtual theft in physical spaces with smartphones, ” in Proc. 20th Annual Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2013.
[2] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, “Soundcomber: A stealthy and context-aware sound trojan for smartphones,” in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp., Feb. 2011, pp. 17–33.
[3] L. L. N. Laboratory, Controlled items that are prohibited on llnlproporty. (2013). [Online]. Available: https://www.llnl.gov/ about/controlleditems.html

[4] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: Context-related policy enforcement for android," in Proc. 13th Int. Conf. Inf. Security, 2011, pp. 331–345.
[5] A. Kushwaha and V. Kushwaha, "Location based services using android mobile operating system," Int. J. Adv. Eng. Technol., vol. 1, no. 1, pp. 14–20, 2011.
[6] S. Kumar, M. A. Qadeer, and A. Gupta, "Location based services using android," in Proc. 3rd IEEE Int. Conf. Internet Multimedia Serv. Archit. Appl., pp. 335–339.
[7] M. S. Kirkpatrick and E. Bertino, "Enforcing spatial constraints for mobile RBAC systems," in P roc. 15th ACM Symp. Access Control Models Technol., 2010, pp. 99–108.
[8] A. Gupta, M. Miettinen, N. Asokan, and M. Nagy, "Intuitive security policy configuration in mobile devices using context profiling," in Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471–480.
[9] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," IEEE Security Privacy, vol. 7, no. 1, pp. 50–57, Jan. 2009.
[10] E. Trevisani and A. Vitaletti, "Cell-id location technique, limits and benefits: An experimental study," in Proc. 6th IEEE Workshop Mobile Comput. Syst. Appl., 2004, pp. 51–60.
[11] J. LaMance, J. DeSalas, and J. Jarvinen, AGPS: A low-infrastructure approach. (2002). [Online]. Available: http://www.gpsworld. com/innovation-assisted-gps-a-low-infrastructure-approach/.