ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Smart Technology: A Mobile Device using Context Management System

Prof.Minal Nerkar, Rohit Pardeshi, Dipak Rathod, Unati Salunke, Sushma Ugale

Department of Computer Engineering, AISSMS IOIT, Pune, Maharashtra, India

B.E Student, Department of Computer Engineering, AISSMS IOIT, Pune, Maharashtra, India

ABSTRACT: Location-dependent approach is planned for mobile system. This approach will meet the confidentiality, authentication, simplicity, and usefulness of security problems. Associate degree system that provides services for mobile shoppers is named mobile system. Encoding techniques are used for making certain the info transmission security between information server and mobile clients. The term “Context-based cryptography” is employed here to see any methodology of encryption wherever within the cipher text will solely be decrypted at a specified location. If a shot is formed to decode the info at another location, the decipherment method fails and divulges no info regarding the plaintext. The device playacting the we have a tendency to propose context-sensitive verification ways that allow checking the user’s claimed legitimacy in various ways in which and to various degrees. the result is a relatively strong, less intrusive and extra versatile access management methodology that mimics our natural means that of authentication and authorization among the physical world.

KEYWORDS: data encryption, GPS, mobile computing, location-based service

I. INTRODUCTION

Improve the protection of information access in cloud computing for a corporation or the opposite specific locations victimization the location-based secret writing. The wide unfold of nativespace network and additionallythe quality of mobile devices can increase the frequency of information transmission among mobile users. However, most of the knowledge secret writing technology is location-independent. Associate in Nursing encrypted informationaretypically decrypted anywhere. The cryptography technology cannot limit the locationof informationcryptography. so asto satisfy the demand of mobile users amongthe long run, a location-dependent approach, named as location-dependent encodingformula (LDEA), is projected throughout this paper. A target latitude/longitude coordinate is set foremost. The coordinate is incorporated with a random key for encoding. The receiver canexclusively rewrite the cipher text once the coordinate acquired from GPS, current GPS receiver is quality and inconsistent. the location of a mobile user is hardto exactly match with the target coordinate. A toleration distance (TD) is in addition designed in LDEA to increase its utility. The protection analysis shows that the possibility to interrupt LDEA is sort ofout of the question since the length of the random secret is adjustable. an example is in additionenforced for experimental study. The results show that the cipher text canexclusively be decrypted below the restriction of TD. It illustrates that LDEA is effective and smart for information transmission in mobile surroundings.

II .PROPOSED ALGORITHM

Data security within the cloud is therefore vital. Users (individuals or companies) are involved concerning the access to the data by unauthorized users. Currently suppose that information is a few vital and counselling from a bank, or an organization and etc. definitely the need of access management within the cloud computing is quite ever and could be a important part of information security in cloud. Several ways are planned for the safety of knowledge transmission. However, these ways are location-independent. The sender cannot limit the placement of the receiver for information decryption. If the information encoding algorithmic program will offer such operate, it's helpful for increasing the safety of mobile information transmission within the future. Therefore, a location-dependent data encryption algorithm (LDEA) is proposed during this paper. The latitude/longitude coordinate is employed because the key for encoding in

DOI: 10.15680/IJIRCCE.2017. 0502218

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 depending on how many satellite signals received. It's difficult for receiver to decrypt the cipher text at constant location exactly matched with the target coordinate. It is impractical by victimization the wrong GPS coordinate as key for encryption. Consequently, a toleration distance (TD) is intended in LDEA. The sender can also verify the TD and therefore the receiver can decipher the cipher text inside the region of TD.

In our technique 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 answer is a lot of acceptable for banks, massive corporations, establishments and examples like this. The sole factor we'd like is associate degree Anti-Spoof and correct GPS those corporations will afford to shop for. Conjointly implementing the location-dependent encoding algorithmic program (LDEA), on the cloud and therefore the user's pc (which is connected to the GPS) is needed. We will label the information. Label contains name of the corporate or an individual who works within the company (for example the company's boss).

These labels are placed in an index table that refers to the user's geographic location and therefore the timeframe thought-about to access information, in a very info. These labels and values of the info is additional manually or mechanically. As an example, suppose that a bank stores some info within the cloud and solely the accountant will have access to that. The accountant's area is on the third floor of the bank's building and accountant's operating hours are from eight am to three pm. we will create the data within the cloud offered solely inside the accountant's space and his operating hours (in addition to the existing security measures). As mentioned the new generation "Anti-Spoof" GPS is extremely correct and may offer us the latitude, meridian and altitude accurately. As a result we will limit the information access to the space placed on a selected floor of a building and a fixed timeframe. Another example: the data which will be offered solely within the chief's space of various branches of a bank or an organization. Within the usual technique, once users commit to access the information, they use commonplace security measures and so get access to the cloud.

III. LITRATURE SURVEY

1] Location Based Encryption Decryption Approach for Data Security
Published Year: 2014
AUTHORS:Borse Manoj V,Bhandure Harshad D.
Data security is an important task in today's life. Data security can be done using GPS device. Among computer user mostly use data in electronic format. How to provide a security for data is important. In this paper, we propose a Location Based Data Security System to secure data by applying Encryption Algorithm and coordinate using GPS device. Encryption means of efficient secure integer comparison. The encryption technology cannot restrict the location of data decryption.PS based encryption is an innovative technique that uses GPS technology to encode location information into the encryption keys to provide location based security.

2] Location based Encryption and Authentication of Cloud Data
Published Year: 2016
AUTHORS: Atul Kamble, Poonam Mantri
Cloud Computing is associate approach within the field of data technology that satisfies userneeds for computing resources like services and applications. Security of access to vital and tip in banks, institutionsetc. Arevery essential. we will improve security of knowledge access in cloud computing using location based mostlycoding and authentication

3]Location Based Encryption using Message Authentication Code in Mobile Networks
Published Year: 2014
AUTHORS: Swapna B Sasi, Betsy K Abraham

The popularity of mobile devices increases the frequency of data transmission among mobile users. How to provide a secure and convenient protocol for data transmission is important. Secure communication is possible through encryption of data. The concept of “geoencryption” or “location-based encryption” is developed to restrict the location and time of data decryption. Location-based encryption or geo-encryption refers to an encryption method in which cipher text can be decrypted only at a specified location. If someone attempts to decrypt the data at some other location, the decryption process fails ad reveals no details about the original plaintext information.

4]A Generalized Study on Encryption Techniques for Location Based Services
Published Year: 2005
AUTHORS: Y. Lakshmi Prasanna, Prof. E. Madhusudhan Reddy

Location primarily based service (LBS) is that theconstruct that denotes applications integration geographic location (i.e., special coordinates) with the final notion of services. samples of such applications embody emergency services, automobile navigation systems, tourer tour designing etc. The increasing unfold of location primarily based services (LBSs) has semiconductor diode to a revivedanalysis interest within the security of services. to confirm the credibleness and convenience of LBSs, the requireddemand is to deal with access management, authentication and privacy problems with LBSs. during this paper a Study of the encoding techniques used for making certainthe safety of location primarily based services (LBSs) is completed. consistent with our discussion, the approach will meet the confidentiality, authentication, simplicity, and practicableness of security problems. As a result, the plannedencoding techniques also can meet the stress of mobile info systems

IV. METHODOLOGY

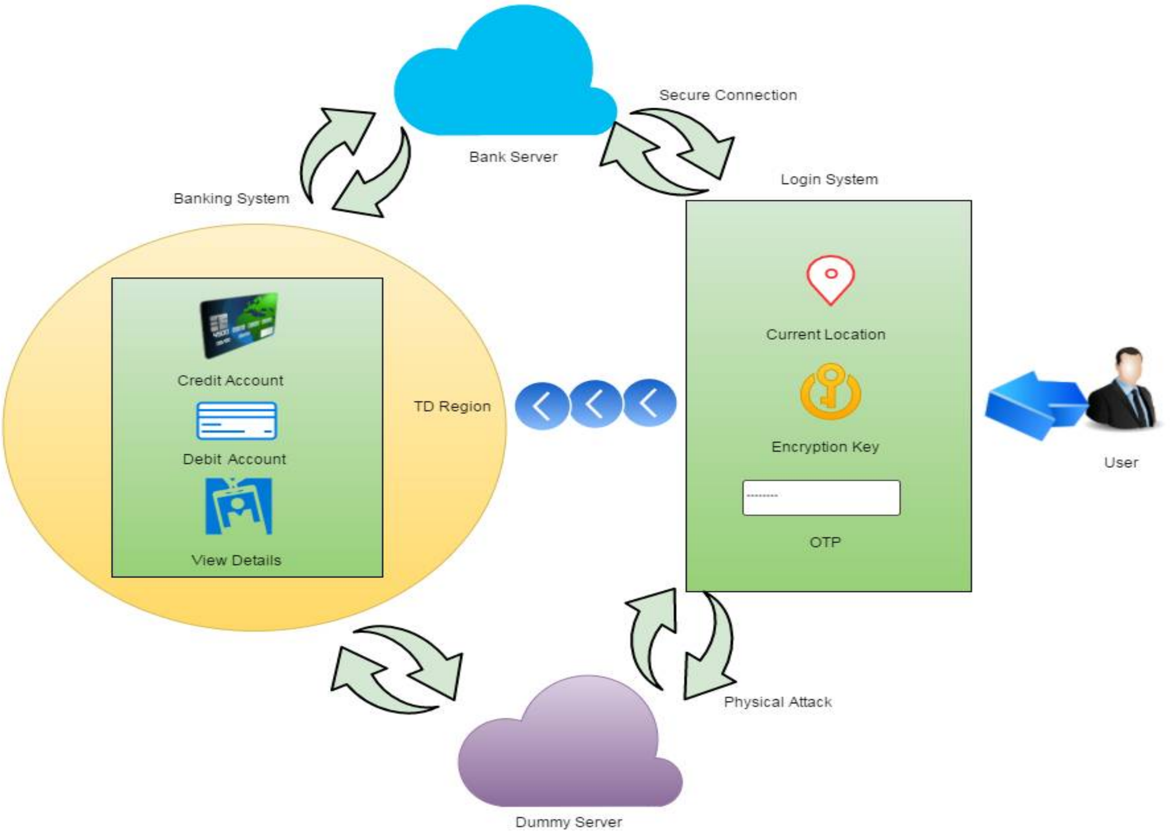


Fig 1: Architecture diagram of proposed system

DOI: 10.15680/IJIRCCE.2017. 0502218

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

A.1. Bank Server:

It is main server meant for saving the information of user throughout dealings. User will credit, debit and enquiry regarding his/her account details.

A.2. User:

The user must login to his/her account with the credentials provided throughout the registration method. User current location is fetched and cross examined with the registered location if its similar then user will proceed with any transaction else the dealings are going to be closed.

A.3. Dummy Server:

The dummy server is for providing security from physical attack. It additionally works same as main server however the transaction created here are pretend i.e. the transaction doesn't have an effect on the users main account.

.

B.Third-Party Provider Solutions

For last few years, a big range of third-parties providing to deliver alert messages (and different info services) via text electronic messaging services. The design of those systems is comparatively straightforward. Whether or not activated through an online interface, directly from a phone, or as software system running on a field administrator's laptop, these services act as SMS aggregators and inject text messages into the network. Within the event of Associate in Nursing emergency message is shipped to the service centre from the victim or footer mobile.

B.1. Short Message Service

Short Message Service (SMS) could be a text electronic communication service element of phone, web, or mobile communication systems, exploitation standardized communications protocols that enable the exchange of short text messages between fastened line and itinerant devices. SMS text electronic communication is that the most generally used knowledge application within the world, with 3.6 billion active users, or seventy eight of all itinerant subscribers. The term SMS is employed as an equivalent word for all sorts of short text electronic communication in addition because the user activity itself in several components of the globe. Straightforward user generated text message services - embrace news, sport, financial, language and placement primarily based services, in addition as several early samples of mobile commerce like stocks and share costs, mobile banking facilities and leisure booking services. SMS has used on fashionable handsets originated from radio telegraphy in radio memoranda pagers exploitation standardized phone protocols and later outlined as a part of the world System for Mobile Communications (GSM) series of standards in 1985] as a method of causing messages of up to one hundred sixty characters, to and from GSM mobile handsets. Since then, support for the service has dilated to incorporate alternative mobile technologies like ANSI CDMA networks and Digital AMPS, in addition as satellite and land line networks. Most SMS messages ar mobile-to-mobile text messages although the quality supports alternative styles of broadcast electronic communication in addition.

B.2. GSM Technology

GSM could be a cellular network, which implies that cell phones connect with it by checking out cells within the immediate neighbourhood. There square measure five completely different cell sizes in an exceedingly GSM network. The coverage space of every cell varies per the implementation atmosphere. Indoor coverage is additionally supported by GSM. GSM uses many crypto logical algorithms for security. A convenient facility of the GSM network is that the short message service. The Short Message Service – purpose to purpose (SMS-PP) was originally outlined in GSM recommendation that is currently maintained in 3GPP as TS twenty three.040. GSM 03.41 (now 3GPP TS twenty three.041) defines the Short Message Service – Cell Broadcast (SMS-CB), that permits messages (advertising, public data, etc.) to be broadcast to any or all mobile users in an exceedingly nominal geographic region. Messages square measure sent to a brief message service canter (SMSC) that provides a "store and forward" mechanism. It makes an attempt to send messages to the SMSC's recipients. If the subscriber's mobile unit is power-driven off or has left the coverage space, the message is hold on and offered back to the subscriber once the mobile is power-driven on or has re-entered the coverage space of the network. This operate ensures that the message are going to be received.

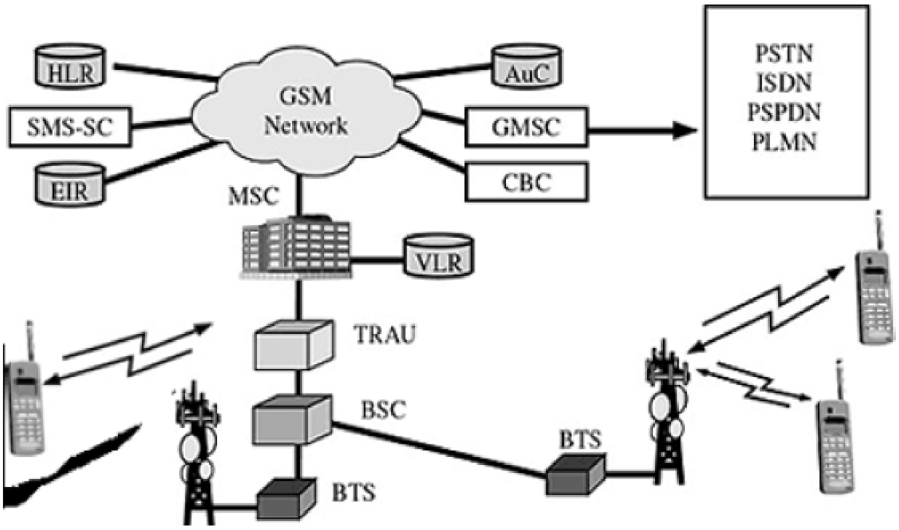


Fig 2: GSM Network along with SMSC

Both mobile terminated (MT, for messages sent to a mobile handset) and mobile originating (MO, for those sent from the mobile handset) operations are supported. In Message delivery, delay or complete loss of a message is uncommon, typically affecting less than 5% of messages.

B.3. GPS Technology

The Global Positioning System (GPS), additionally referred to as Navistar, could be a world navigation satellite system (GNSS) that has location and time data altogether climatic conditions, anyplace on or close to the planet wherever there's associate degree unobstructed line of sight to four or a lot of GPS satellites. The GPS system operates severally of any telecommunication or web reception, though' these technologies will enhance the utility of the GPS positioning data. The GPS system provides essential positioning capabilities to military, civil, and industrial users round the world. The US government created the system, maintains it, and makes it freely accessible to anyone with a GPS receiver. The GPS conception is predicated on time and also the celebrated position of specialized satellites. The satellites carry terribly stable atomic clocks that square measure synchronized with each other and to ground clocks. Any drift from true time maintained on the bottom is corrected daily. Likewise, the satellite locations square measure celebrated with nice exactness. GPS receivers have clocks as well; but, they're typically not synchronized with true time, and square measure less stable. GPS satellites ceaselessly transmit their current time and position. A GPS receiver monitors multiple satellites and solves equations to see the precise position of the receiver and its deviation from true time. At a minimum, four satellites should be visible of the receiver for it to work out four unknown quantities (three position coordinates and clock deviation from satellite time).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

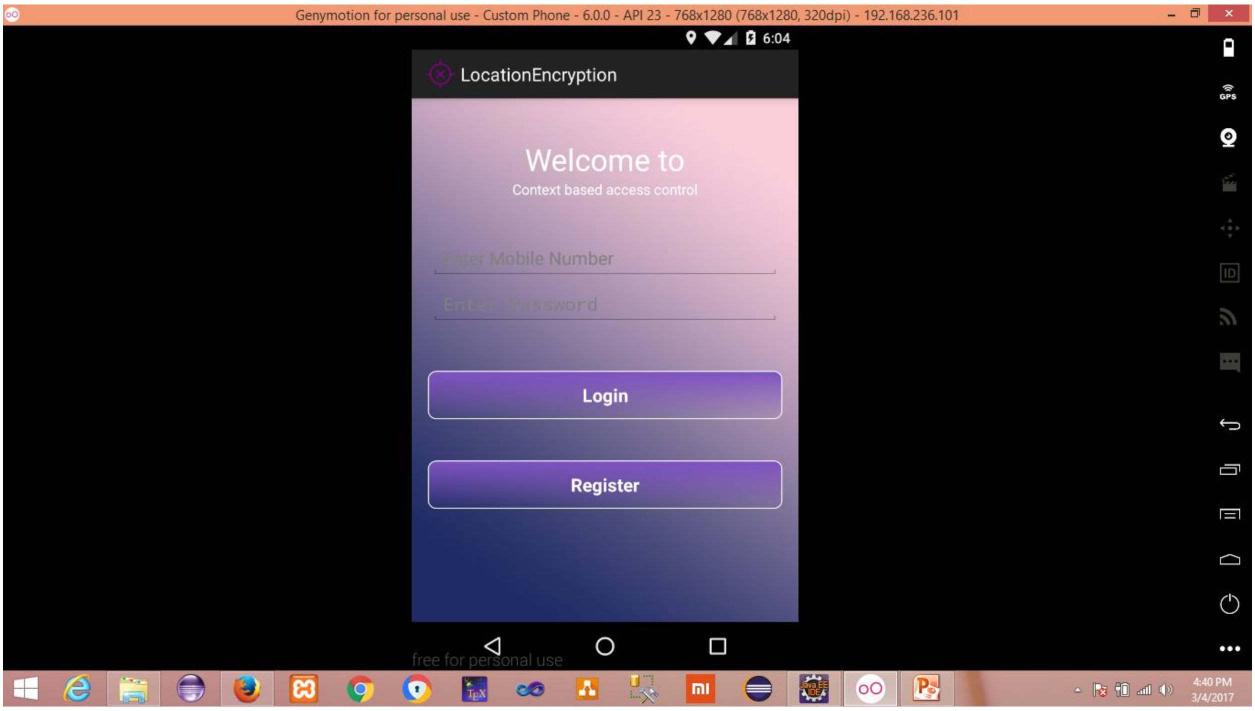
International Journal of Innovative Research in Computer and Communication Engineering

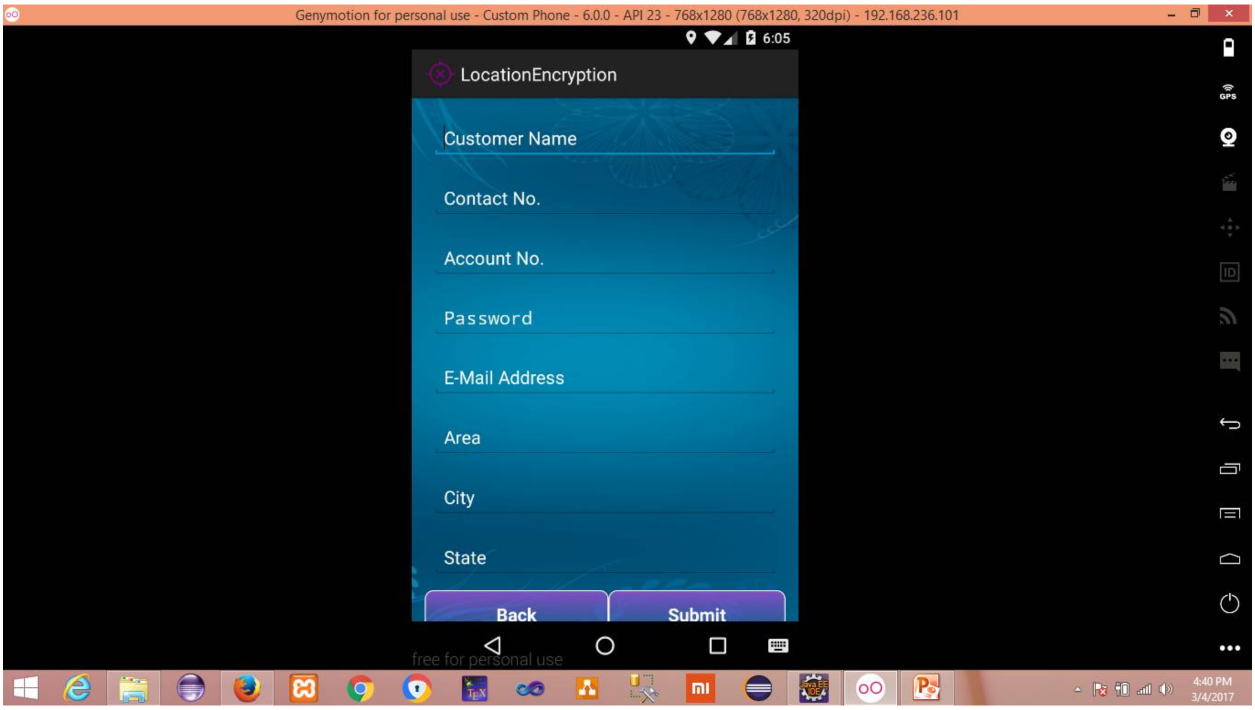
(An ISO 3297: 2007 Certified Organization)

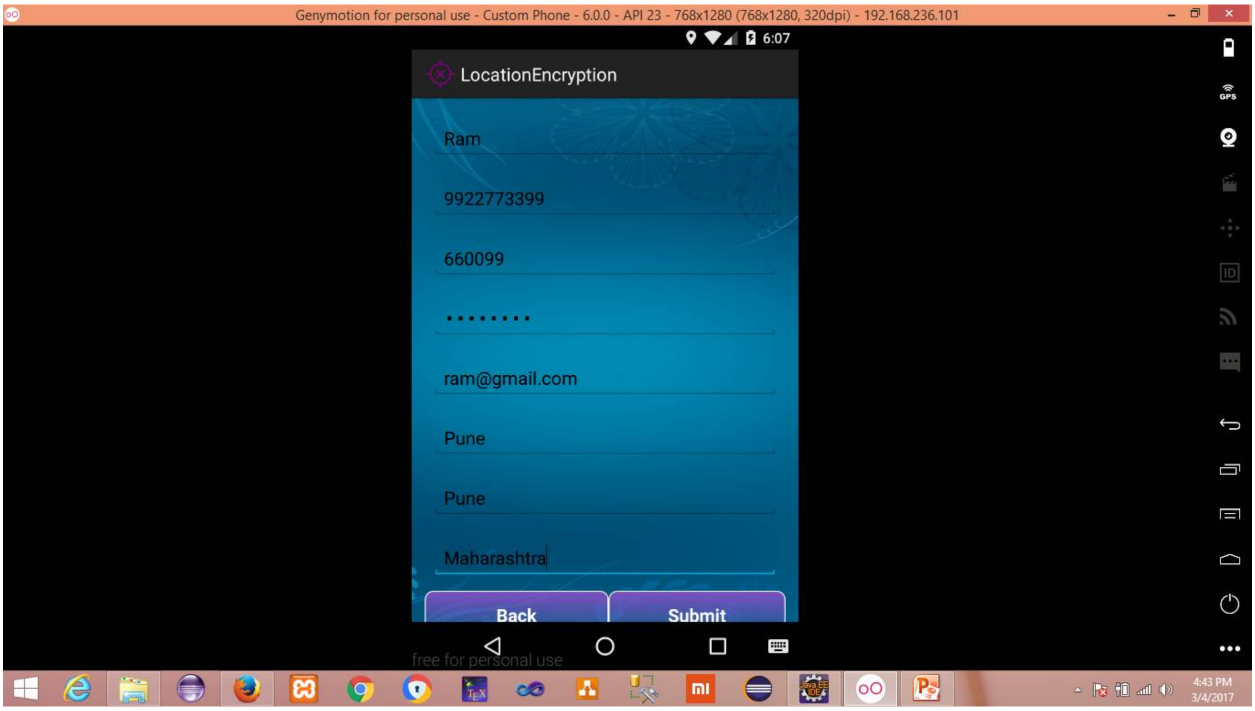
Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

V. SIMULATION RESULTS


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101
6:04
LocationEncryption
Welcome to
Context based access control
Enter Mobile Number
Enter Password
Login
Register
free for personal use
4:40 PM
3/4/2017





Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101

LocationEncryption

Ram

9922773399

660099

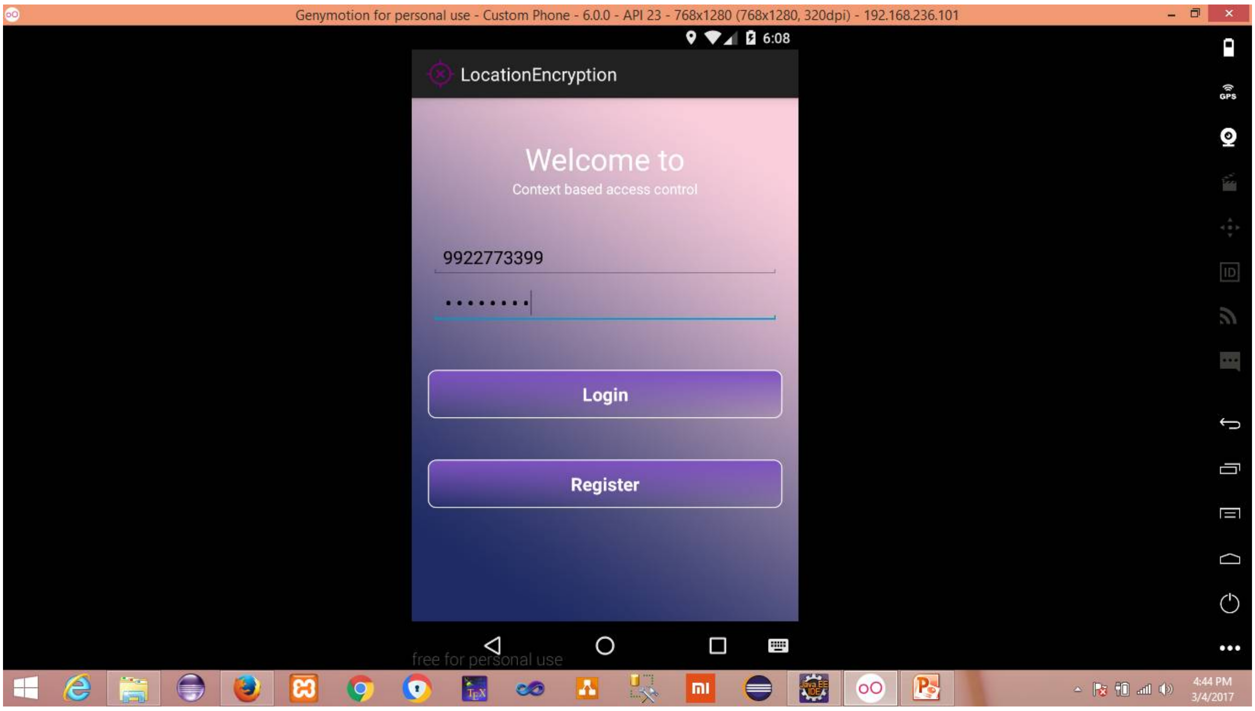
••••••••

ram@gmail.com

Pune

Pune

Maharashtra



Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101

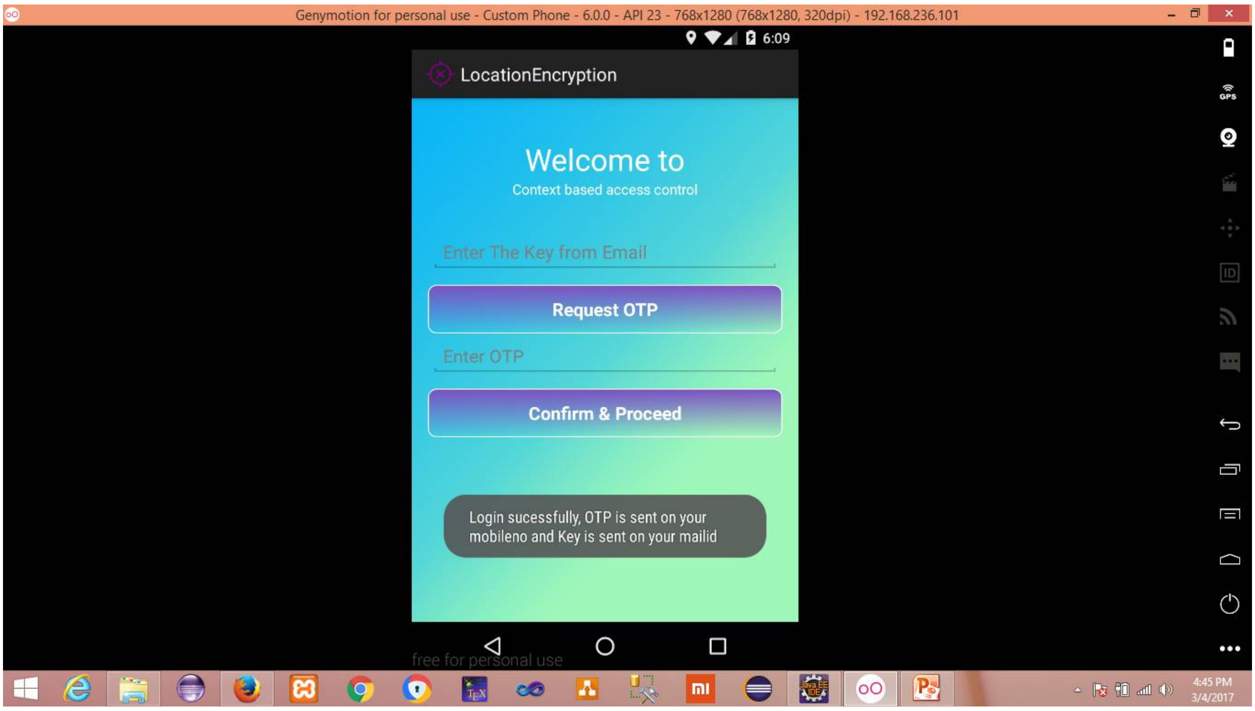
LocationEncryption

Welcome to

Context based access control

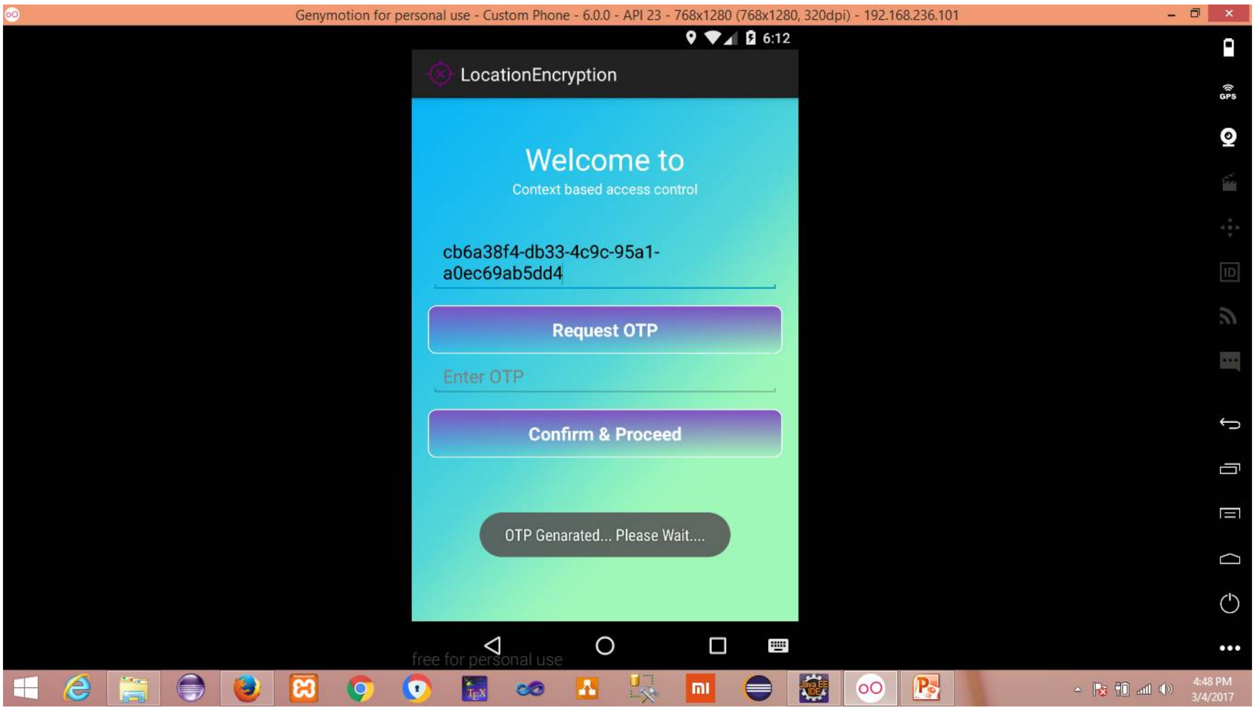
9922773399

••••••••



Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101

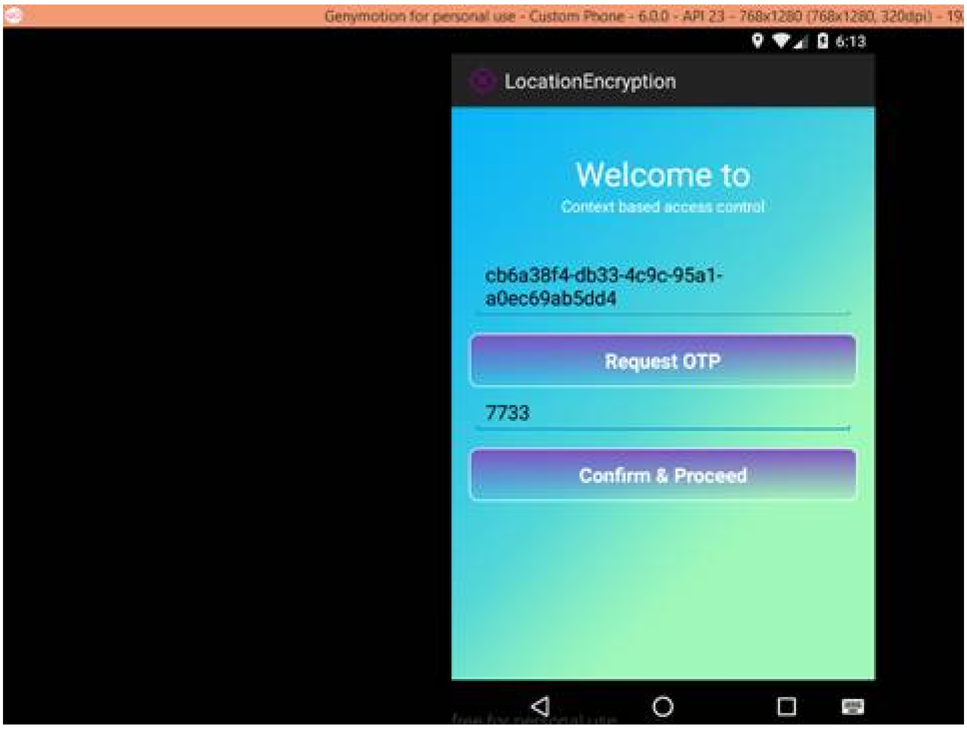
Login sucessfully, OTP is sent on your mobileno and Key is sent on your mailid



Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101

cb6a38f4-db33-4c9c-95a1-a0ec69ab5dd4

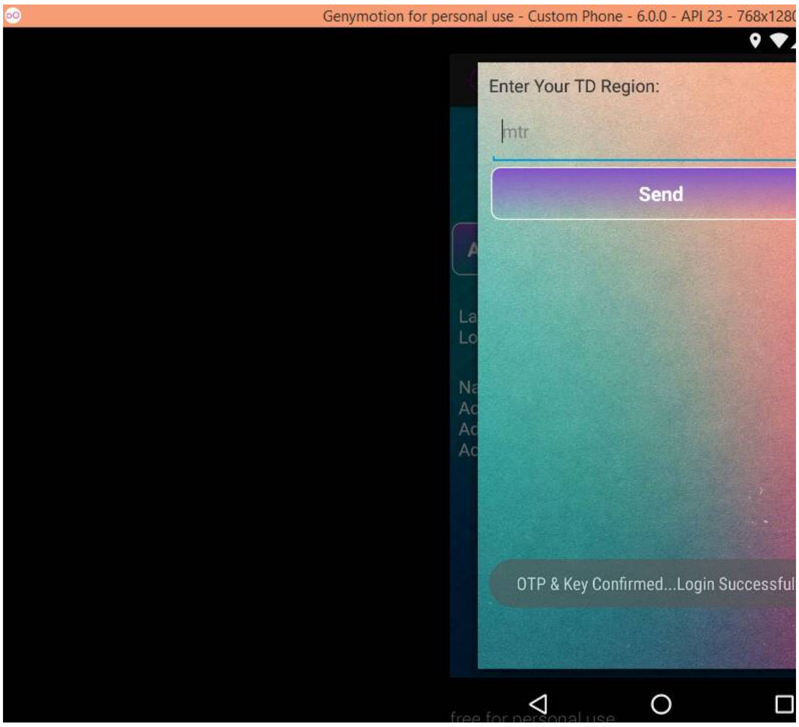
OTP Genarated... Please Wait....


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 19
6:13
LocationEncryption
Request OTP
Confirm & Proceed
free for personal use

Welcome to
Context based access control

cb6a38f4-db33-4c9c-95a1-a0ec69ab5dd4

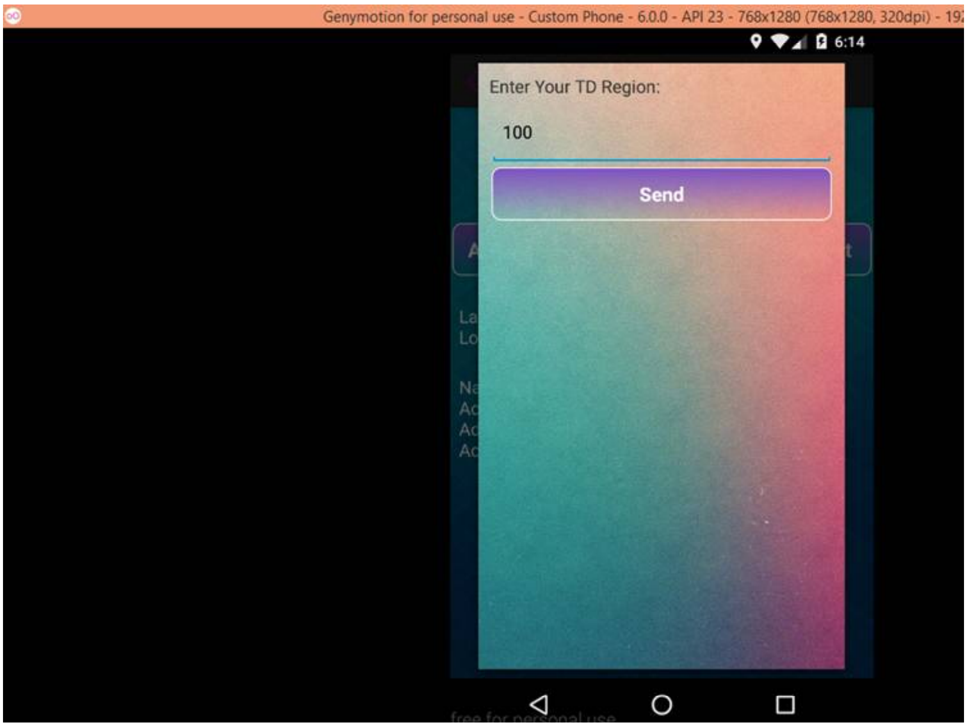
7733


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x128
Send
free for personal use

Enter Your TD Region:

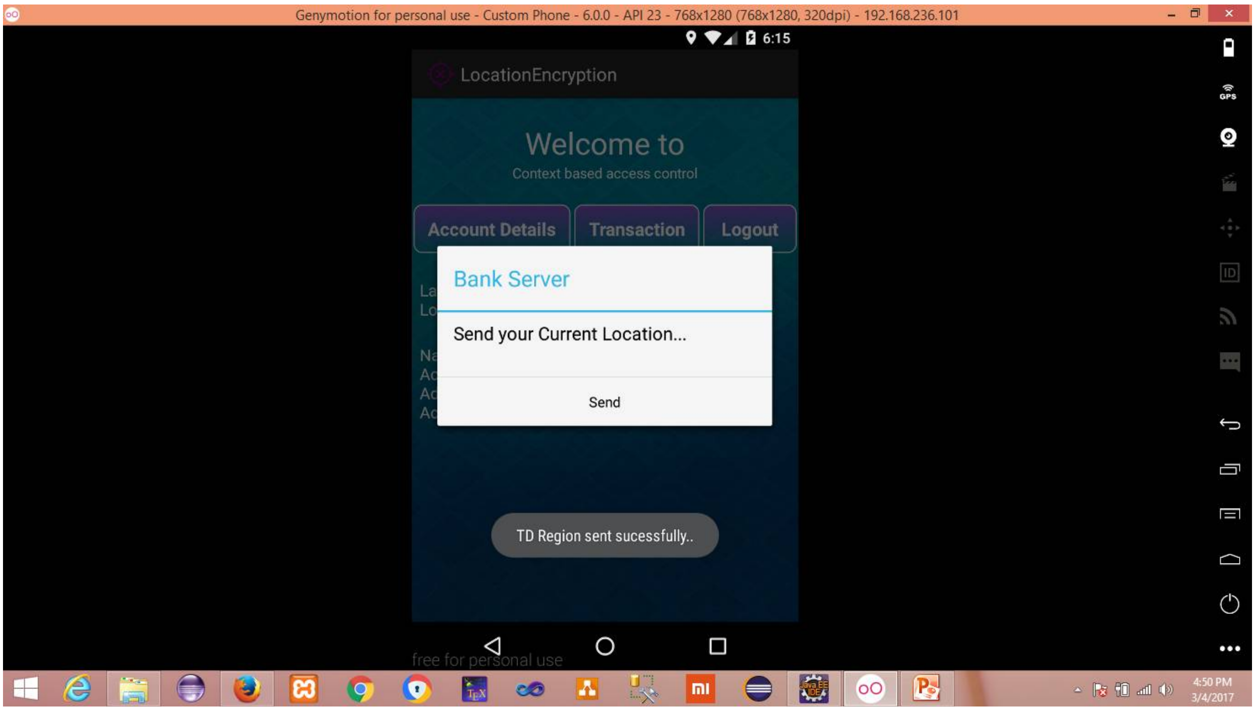
mtr

OTP & Key Confirmed...Login Successful


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192
6:14
Send
free for personal use

Enter Your TD Region:

100


Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101
6:15
LocationEncryption
Account Details
Transaction
Logout
Send
free for personal use
4:50 PM
3/4/2017

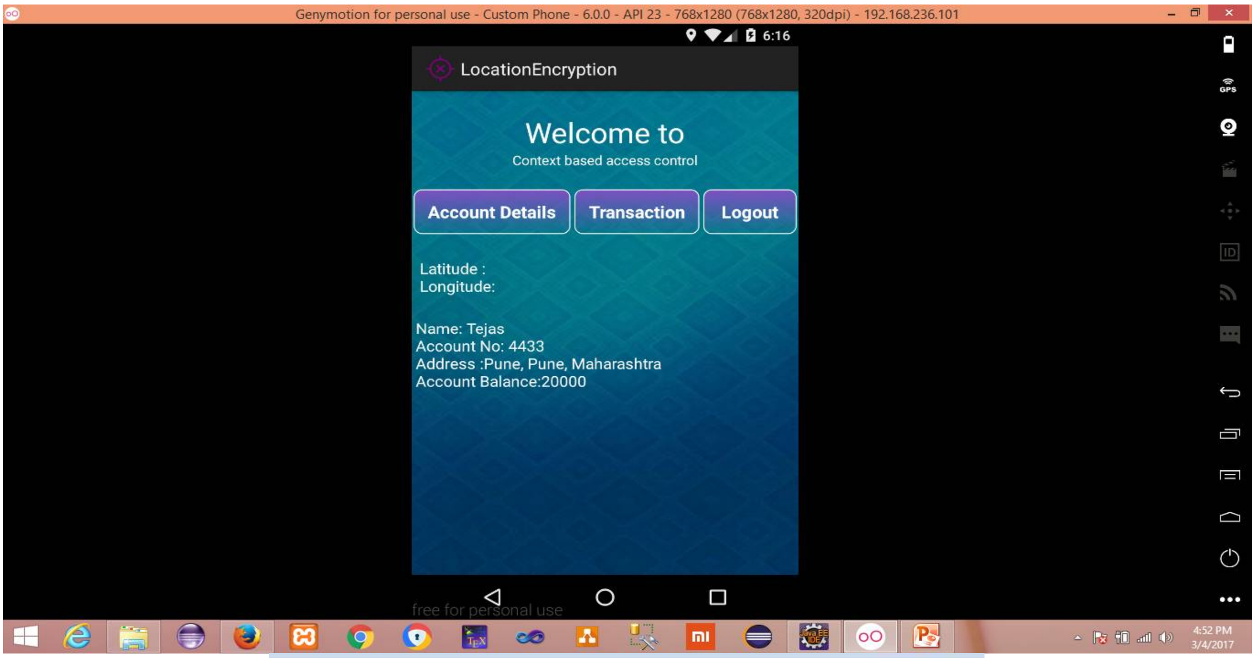
Welcome to

Context based access control

Bank Server

Send your Current Location...

TD Region sent sucessfully..



Genymotion for personal use - Custom Phone - 6.0.0 - API 23 - 768x1280 (768x1280, 320dpi) - 192.168.236.101

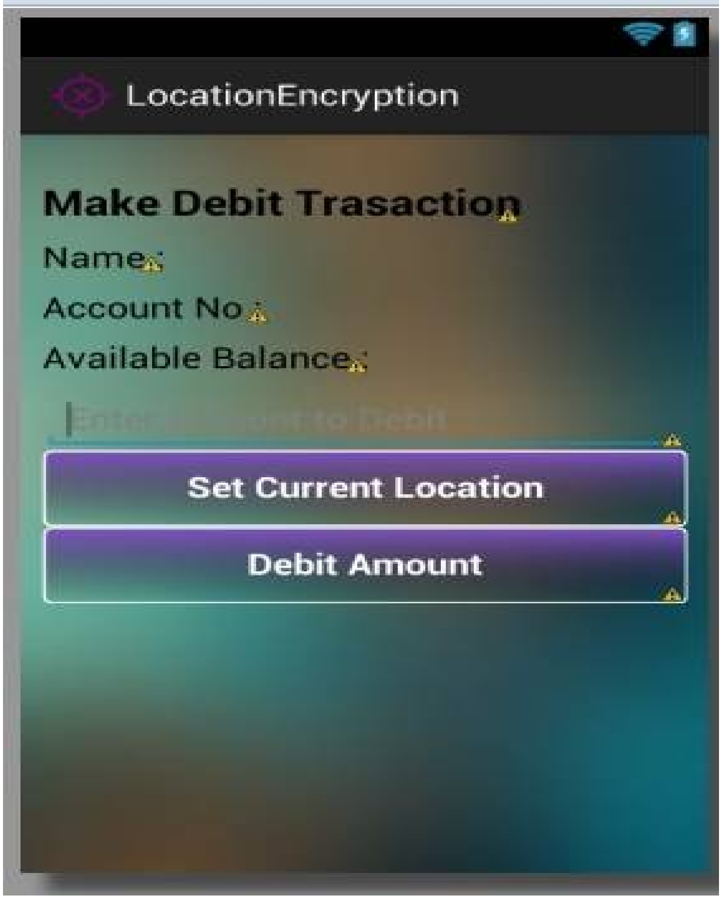
LocationEncryption

Welcome to
Context based access control

Account Details | Transaction | Logout

Latitude :
Longitude:

Name: Tejas
Account No: 4433
Address :Pune, Pune, Maharashtra
Account Balance:20000



LocationEncryption

Make Debit Trasaction

Name:

Account No:

Available Balance:

Enter amount to Debit

Set Current Location

Debit Amount

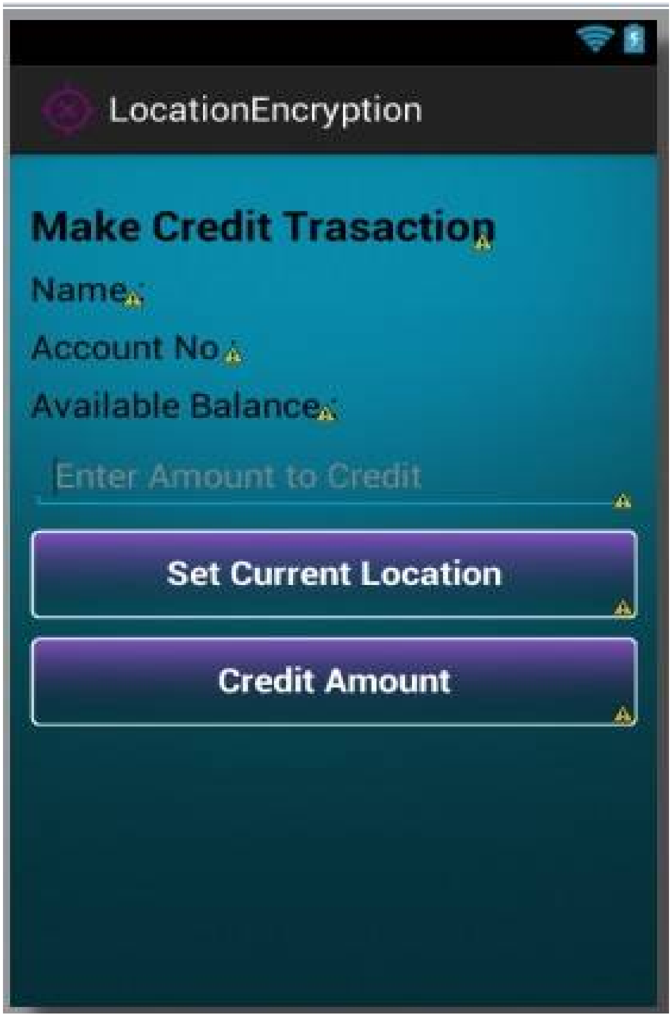
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017



LocationEncryption

Make Credit Trasaction

Name :

Account No :

Available Balance :

Enter Amount to Credit

VI. CONCLUSION

. Security in context aware environments would force solutions terribly different from those of today’s systems that are predicated on comparatively stable, well-defined, consistent configurations, static contexts, and participants of security arrangements. For example, historically a user authentication mechanism is taken into account secure if it's a mixture of one thing the user has, one thing the user is aware of, or one thing the user is. what's required will be characterized by the term ‘conformable security’, within which the degree and nature of security related to any specific sort of action can amendment over time, with dynamical circumstances and with changing obtainable information therefore on suit the context .

We have additional context awareness as a fourth dimension to security. Context sensitive security exploits the power to sense and use discourse information to enhance or replace ancient user attributes like username/password for the aim of authentication and access management by creating security less intrusive and adaptable to situational or discourse changes. We’ve got incontestable this by concerning the access management method as a context aware service, whose objective is to grant or deny the access of a supplicant to a resource (e.g., a service) supported context information. The code will be executed only if the user is at intervals the approved area. Besides, the distribution of multimedia system content is also utilized the LDEA algorithm for advanced access management except the username/password. The planned LDEA algorithm provides a brand new means for information security. It’s additionally meeting the trend of mobile computing. Several doable applications are developed within the future to demonstrate and promote the thought of LDEA algorithmic program. The planned methodology will be employed in many places like banks, huge companies, and institutions to fulfil the required performance.

REFERENCES

[1] Aikawa, M., K. Takaragi, S. Furuya and M. Sasamoto, 1998. A Lightweight Encryption Method Suitable for Copyright Protection. IEEE Trans.on Consumer Electronics, 44 (3): 902-910.

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

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

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

[5] Jamil, T., 2004. The Rijndael Algorithm. IEEE Potentials, 23 (2): 36-38.

[6] Jiang, J., 1996. Pipeline Algorithms of RSA Data Encryption and Data Compression, In: Proc. IEEE International Conference on Communication Technology (ICCT'96), 2:1088-1091, 5-7 May 1996.

[7] Lian, S., J. Sun, Z. Wang and Y. Dai, 2004. A Fast Video Encryption Scheme Based-on Chaos. In: Proc. the 8th IEEE International Conference on Control, Automation, Robotics, and Vision (ICARCV 2004), 1: 126-131, 6-9 Dec. 2004.

[8] 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.