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 4, April 2017

Security of Data Access Using Location Based Encryption in Cloud Computing

Varsha Zaware[#1], Swapnali Thakur[#2], Akash Bharade[#3],Kalyan More[#4], Prof V.P.Tonde[#5]

Student, Dept. of Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India[#1]

Student, Dept. of Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India[#2]

Student, Dept. of Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India[#3]

Student, Dept. of Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India[#4]

Professor, Dept. of Information Technology, Sinhgad Institute of Technology, Lonavala, Pune, India[#5]

ABSTRACT: One of the most important challenge in cloud computing area is the security of cloud computing. On the other hand the security of access to critical and confidential information in banks, institutions etc. are extremely essential. Sometimes even with the enormous costs, it is not fully guaranteed and it is compromised by the attackers. 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. If an attempt to decrypt data at another location, the decryption process fails and reveals no information about the plaintext. 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. Data security in the cloud is so important. Now suppose that data is some critical and confidential information from a bank, or a company and etc. Unquestionably the need of get to control in the cloud computing is more than ever and is a very important part of data security in cloud. In our method we use the user's location and geographical position and we will add a security layer to the current safety efforts. Our answer is more suitable for banks, enormous organizations, establishments and cases this way. The only thing we need is an Anti-Spoof and accurate GPS that companies can afford to buy. Location based encryption and "Geo- Encryption" algorithm 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.

KEYWORDS: "Location-Based-Encryption" algorithm, Cryptography, Cipher-text, plaintext, virtualization.

I. INTRODUCTION

Security has dependably been a basic piece of human life. Individuals have been looking for physical and budgetary security. With the headway of human learning and getting into the new period the need of data security were added to human security concerns. As we know each and every companies, industries as well as people have their private and personal data which are very confidential. This all data are saving on private or public cloud. So now a day's hacker can hack this confidential data from cloud for misuse purpose and it is too dangerous. Mostly people don't know actually what will happen to their personal data and information on cloud and whetherother people can gain access to their data. To overcome all this problems as well as to provide more security we are going to implement security services.

We are creating saving money application utilizing Location Based Encryption. As contrast with current saving money application which are area autonomous. It means in Cryptography Cipher-text can only be decoded at a predefined area i.e. area subordinate approach.

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 4, April 2017

In the event that an endeavour to decode information at another location, the decryption process fails and reveals no information about the plaintext.Information is scrambled just when individual is having private key can decode it.
In cryptography “identity” segment is imperative, we can indicate name, address, id as personality, however we can likewise give put (i.e. Physical presence at a particular location) as identity. This place can be used in encryption process.
We investigate the useful possibility of utilizing setting data for controlling access to administrations. Construct exclusively in light of situational setting. we demonstrate that clients can be straightforwardly given unknown access to administrations and that specialist co-ops can in any case force different security levels. There to, we propose context-sensitive verification methods that allow checking the user’s claimed authenticity in various ways what's more, to different degrees. All the more accurately, customary data administration methodologies are utilized to compare historic contextual (service usage) data of an individual user or group. The result is relatively strong, less intrusive and more flexible access control process that mimics our natural way of authentication and authorization in the physical world.

II. RELATED WORK

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 allowsfake transactions. Our system allows access of account from any location.
There are four main modules in our project:
1. User.
2. Transaction.
3. Location Based Encryption Algorithm.
4. Dummy Server.

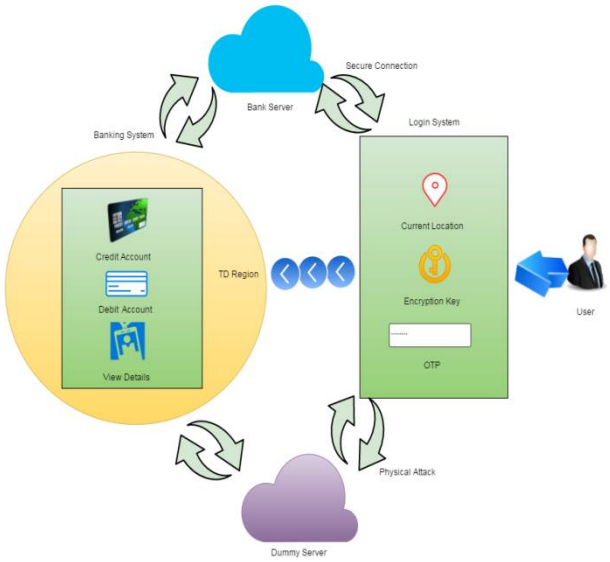


Fig. 1. Architecture diagram

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 4, April 2017

1. User

After installation of application in android device the user can register by giving valid username password, phone number.

Further the user can Login with the username and password after verifying username and password the he/she can get the Encryption key which is based on the users current location after successfully confirmation of that key by user the OTP(one time password) will be generated which will sent to user mobile.

Further by using the OTP user can access his/her account and make transaction.

2. Transaction

The transaction is based on credit, debit. After the user done with successful registration and login process he/she can access his/her account and make the transaction based upon their need.

The Transaction is also based on the user's current location and the TD region which is provided by user.

If the user gets out from the area of TD region then he/she can't get access the account.

3. Dummy Server

To overcome from physical attacks we have implemented dummy server. Its working is same as main server like it shows account details, balance etc.

But doesn't make any transaction in real-time i.e. it doesn't make any changes in main account which will be accessed by main server. If user access his account with main server than he/she can make transaction if he/she use dummy server than it will not affect to his/her main account.

Dummy server works when the wrong password is input to the system by the user.

III. PROPOSED ALGORITHM

Location based encryption algorithm:-

To provide security from attackers we go for location based encryption. During registration, once the user submits the details regarding username, password, mail-id, phone number. After user done with successful transaction user get username and password. After verifying username and password user can login successfully. After login user location will track through GPS and encrypted key will generated which will be send to user mail-id. After entering encrypted key user request for OTP. Now user can make transaction securely.

After successful login the user will be asked for TD (tolerance distance) which is of integer type the user can mention the range (for example: 1m) from registered location so that within the mentionedrange from his/her registered location he/she can access his/her account successfully.

Step 1 -The target coordinate at the centre is acquired from the GPS receiver.

Step 2- For each TD, a source record is scrambled by utilizing the objective facilitate and TD firstly.

2a. For every circle, the tester moves randomly along the curve of the circle and tries to decode the information consistency.

2b.There are absolutely ten circumstances of information decoding. The destination file is checked whether the content is the same as the original file. The number of successful decryption is recorded.

Step 3-Repeat Step 2 until finishing the testing of all TDs.

The successful rate is computed for every combination of TD and testing distance.

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 4, April 2017

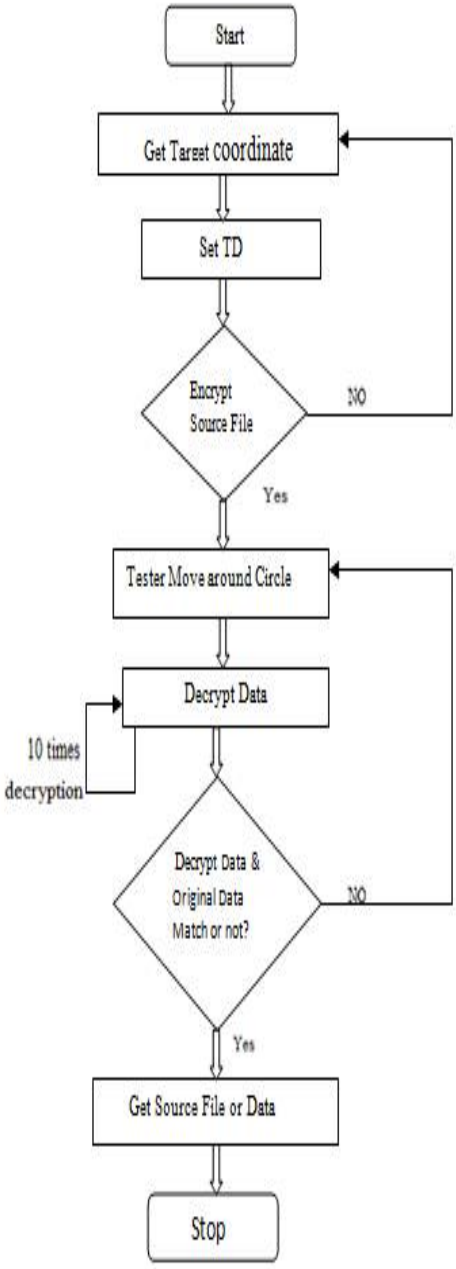


Fig. 2. Algorithm Flow Diagram

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 4, April 2017

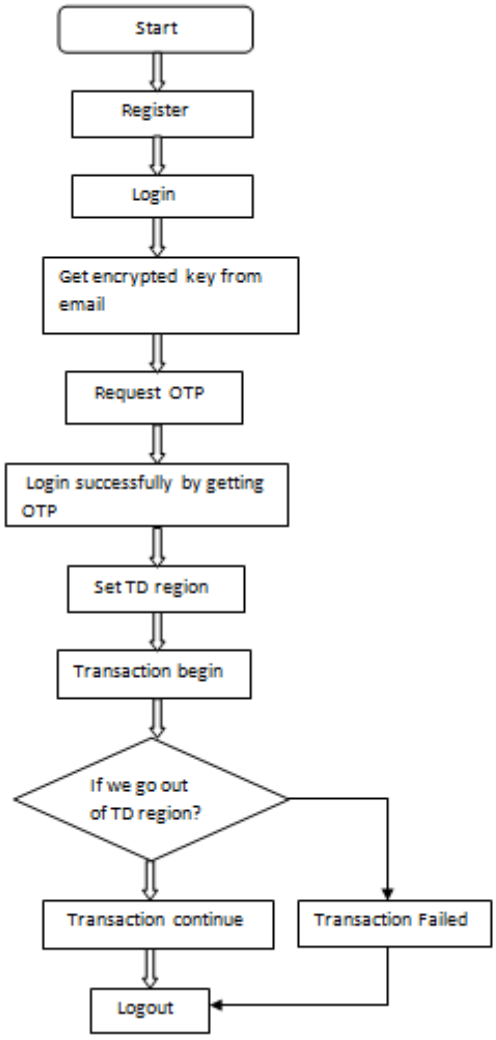


Fig. 3. Overview of Project System

Advantages of our system are as follows:

- Our system is advantageous for data security in cloud.
- It is more appropriate for banks, big companies, Institutions, etc.
- This technology is Location Dependent.

There are several applications of our system are as follows:

- Secure online money transaction.
- Online shopping.

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

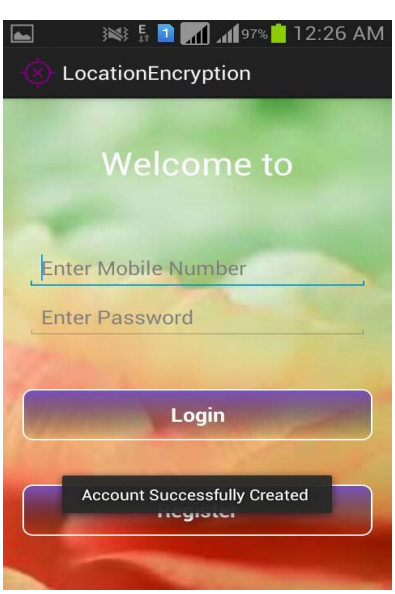
Vol. 5, Issue 4, April 2017

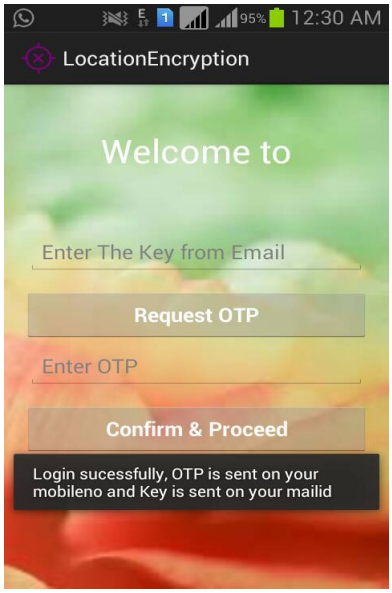
- Ticket booking

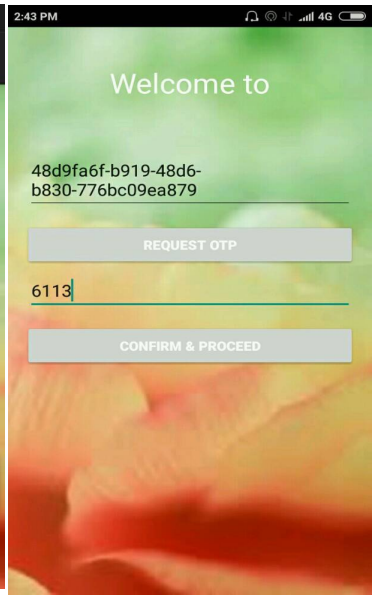
IV. SIMULATION RESULTS

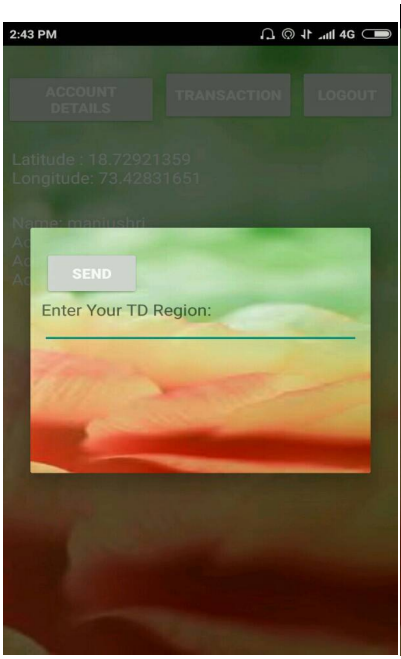
Successfully done the transaction by user when he/she is in authorized area. The transaction is secured from the external/ un-authorized person or from hackers.

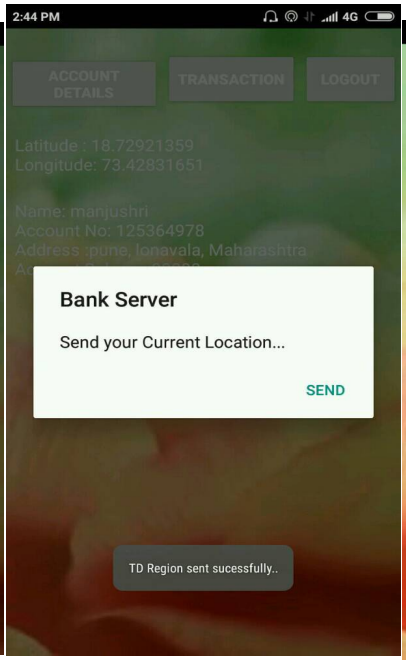
It also provides the security or safety from the Physical attack.

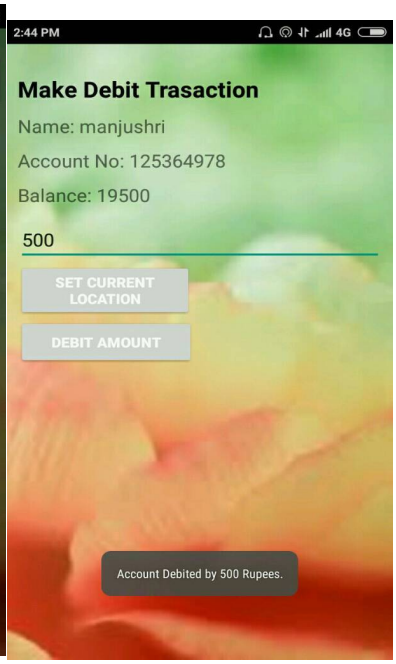












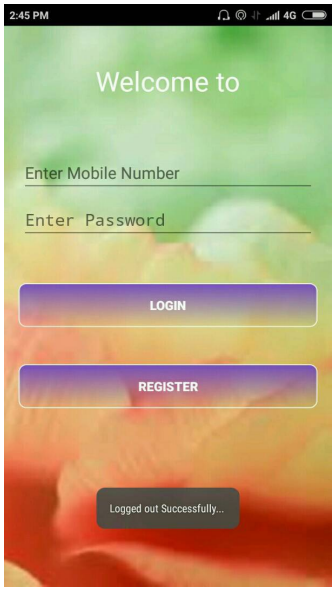
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017



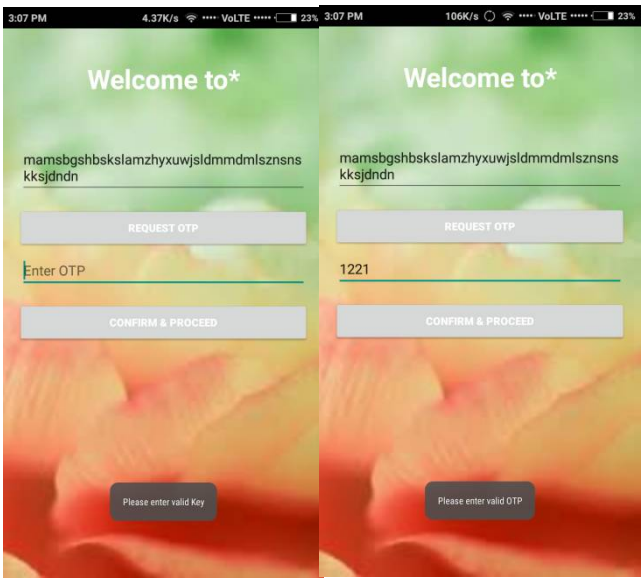
Success condition:

Transaction is successfully done by user. No matter whether it is credit or debit.

Fail condition:

Login fails due to the wrong key or OTP.

Transaction fail if the user out of the TD region



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 4, April 2017

V. FUTURE WORK AND CONCLUSION

In proposed system the person is performing transaction only within 40 m. TD region. But in future we can increase TD region i.e. above 40 m. so that person can able to perform transaction while he/she will travelling.

Location based encryption and "Geo- Encryption" algorithm 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.

REFERENCES

1] Hsien-Chou Liao and Yun-Hsiang Chao Department of Computer Science and Information Engineering, Chaoyang University of Technology, 168 Jifong E. Rd., Wufeng Township Taichung County, 41349, Taiwan (R.O.C.). "LDEA: Data Encryption Algorithm Based on Location of Mobile Users", IEEE Transaction on Cyber Security, Volume 5, No. 2, April 2016.
2] Bilal Shebaro, OyindamolaOluwatimi, and Elisa Bertino, Fellow, IEEE, 2015. "Context-Based Access Control Systems for Mobile Devices". IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 2, MARCH/APRIL 2015.
3] Amit Kushwaha1, VineetKushwaha, "Location Based Services using Android Mobile Operating System," 2011.
4]Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta, "Location Based Services using Android," March 2009.