ISSN 2395-1621

LOCATION BASED ENCRYPTION FOR ONLINE TRANSCATIONS

[#1]Suraj Mishra, [#2]Pradeep Satpute, [#3]Avinash Dangat, [#4]Kushal Roy,
[#5]Prof. Nilesh Pinjarkar

1,2,3,4Students and 5Asst. Prof. of Department of Computer Engineering,
Pune University, Pune

ABSTRACT

Banks are giving versatile application to their client. We are creating banking application utilizing Location Based Encryption. As contrast with current financial application which is area free, we are creating banking application which is area subordinate. Client can perform exchange just in the event that he/she is with in TD area. TD locale is territory of Toleration Distance (TD) where client can perform exchange. On the off chance that client leave TD area, at that point exchange will end consequently. We are giving additional security by OTP and mystery key.

Index Terms: K.4.1 [Computers and Society]: Public Policy Issues Privacy, K.6 [Management of Computing and Information Systems]: Security and Protection

ARTICLE INFO

Article History

Received: 8th March 2020

Received in revised form :

8th March 2020

Accepted: 10th March 2020

Published online :

11th March 2020

I. INTRODUCTION

Security has consistently been a basic piece of human life. Individuals have been searching for physical and money related security. With the headway of human learning and getting into the new time the need of data security were added to human security concerns. We are creating banking application utilizing Location Based Encryption. As contrast with current financial application which is area autonomous, we are creating banking application which is area subordinate. It implies User can perform exchange just on the off chance that he/she is with in TD district. TD locale is region of Toleration Distance (TD) where client can perform exchange. On the off chance that client leave TD area, at that point exchange will end automatically. In our framework client register himself/herself in our application. He/she give the individual subtleties like name, portable number, email id , mystery bit, and so forth then framework will send the encoded secret key to email. Scrambled secret word signifies "Mystery bit" is included into the secret key, this is done to shield secret key from perception. In the wake of entering right client name and secret key, client will login to framework and get the mystery key on enrolled email id. On the off chance that client entered key is right at that point OTP will get on versatile by SMS. Whenever entered OTP is right at that point the application will create TD district. This TD district indicate go in meters. After age TD area effectively client can view record subtleties and User can perform cash exchange operation. Our framework is adaptable enough to give access to client to his/her financial balance from any area. Our framework additionally give answer for physical assault utilizing virtualization, secret word send on email is scrambled by mystery bit.

II. MOTIVATION

All financial applications are area free. Client area could be utilized for better insurance. Since client area couldn't hack by programmer. There is nonattendance of security from representation, shoulder surfing in existing framework.

III. EXISTING SYSTEM

The current framework is having numerous issues, for example, security issues, progressively human association which is a tedious procedure with numerous manual computations. It even incorporates the machine harm and mark check process for verified exchanges which enables the clients and banks to burn through their significant time

and assets. The serious issue in web based financial framework is unapproved client access with phony passwords. The programmers are attempting to hack the client accounts and are performing distinctive unapproved exchanges.

IV. PROBLEM STATEMENT

To overcome the problem of the unauthorized user gaining access to genuine user's ac-counts and performing unauthorized transactions.

V. LITERATURE SURVEY

J. Kang, D. Steiert, D. Lin and Y. Fu, "MoveWithMe: Location Privacy Preservation for Smartphone Users," in 2019, has explained the risks related to location based servies. They have also presented a location privacy preservation mobile app, called MoveWithMe which automatically generates decoy queries to hide the real users' locations and intentions when they are using location-based mobile services. The uniqueness of the MoveWithMe app is that the generated decoys closely behave like real humans. Each decoy in the system has its own moving patterns, daily. It also guarantees the same level of user experience without affecting the response time or introducing extra control burdens. [1]

G. Sriram, B. Srikanth Reddy, K. V. Seshadri, K. H. Kumar and N. Suresh, "Location Based Encryption-Decryption System For Android," in 2018, has stated the importance of location based encryption that takes the information security to whole new level when implemented with mobile application. In this paper the author mainly focused on idea of location based encryption and decryption algorithm. They also stated that the location can be set as an additional security feature in which latitude and longitude coordinates are responsible for encryption and decryption of the data. [3]

I. Ahmad et al., "Current technologies and location based services," in 2017, has explained the advantages and disadvantages of location based services and other technologies like - Radio Frequency Identification, GSM, GPS, AGPS, Smart Antennas, Distributed Antenna Systems, Localization by Cell-ID, Localization by Prediction (Dead Reckoning method), Angle of Arrival (AOA), Localization by Finger Printing, Localization by Time of Arrival (TOA), Localization by Observed Time Difference of Arrival (TDOA), and Hybrid Localization-based AOA-TOA. They also differentiate them on basis of infrastructure, power requirements, sensing devices, and other factors. [4]

Sasikumar, D., "Mobile Banking and Security Challenges," in 2017, has made an effort to study the various security issue, challenges and solutions related to mobile banking services. He also stated that the cyber criminals are trying to find new techniques to get unauthorized access to finances of banking customers. He also said that security around the transfer of data through communication channels is a challenge for developers, pointing out that developers are placing too much confidence in secure end-user behavior and back-end server-side communications. [5]

L. Nosrati and A. M. Bidgoli, "A review of mobile banking security," in 2016, has discussed about the various mobile banking payment security challenges and security risks of mobile banking. He also compared different encryption algorithm. They have proposed a secure system for mobile banking which has 2 security layers i.e. Authentication and Authorization. The authors also prepared security of the network layer by authorizing the message format with check sum, which is encrypted with 'SHA-256' format. [6]

VI. PROJECT SCOPE

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. This protect from unauthorized access. Our system allows access of account from any location.

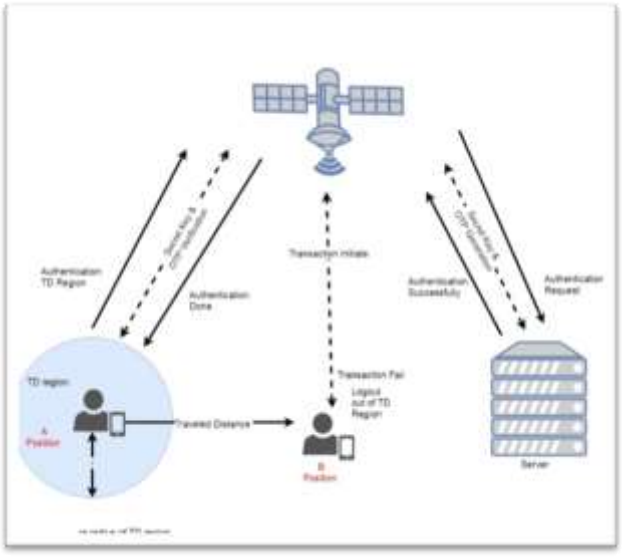
VII. SYSTEM REQUIREMENT

Database Requirements
- o Server: Apache Tomcat
- o Database: SQLite and Xampp

Software Requirements
- o Operating system: Windows 7 and above.
- o Coding Language: Java 1.8
- o Tool Kit: Android 2.3 and above.
- o IDE: Android Studio.

Hardware Requirements
- o System: Intel I3 Processor and above.
- o Hard Disk: 40 GB.
- o Monitor: 15 VGA Color.
- o Ram: 4 GB.
- o Mobile: ANDROID

VIII. SYSTEM ARCHITECTURE



In above architecture user register himself/ herself in our application. He/she provide the personal details like name, mobile number, email id, secret bit, etc., then system will send the encrypted password to email. Encrypted password means "Secret bit" is added into the password, this is done to protect password from visualization. After entering correct user name and password user will login to system and get the secretkey on registered email id. If user entered key is correct then OTP will receive on mobile by SMS. If entered OTP is correct then generate TD region. This TD region specify range in meters. After generation TD region successfully, user can view account detail and user can perform money transaction operation. In GPS there are two techniques are used, first is the latitudes and second is longitude to the get the correct position of the user to determine the new key for the encryption. This key is made by using the combining of the AES and GPS location with the TD. Using latitude, longitude to find the exact location of the user on the map we need to determine which latitude line and which longitude line meets, where user is standing. In this, TD is Tolerance distance which is used to create a geographical area to the user in which all the transaction process will done inside this area. This tolerance distance is calculated as the actual position of user and the provided distance. Such as in equation TD = User current position + Provided distance, this Tolerance distance is calculated and then this area is provided to the user to complete the transaction for the security purpose. If user goes out of this area then this process will be performed again and new TD is generated and new secret key is generated to the encryption and decryption.

IX. ALGORITHM USED

- Advanced Encryption Standard (AES).
- Haversine

X. MODULES

User Module

o User register himself/herself into system then login into application.
o Enter Secret Key receive from email. If key is correct then OTP will receive on mobile.
o Enter OTP receive on mobile. If OTP is correct then generate TD region.
o Enter TD region range in meters to generate TD region.
o After generation TD region successfully user view account details.
o User perform money transaction operation.

User module contains:
Register
Login
View details
Money Transfer

Server Module

o After user successfully register into system, system send "encrypted password" to email. Encrypted password means "Secret bit" is added into the password, this secret bit is provided by user at the time of registration. (all these operations are performed to secure the password)
o After successfully login, system will generate "secret key" and send to the registered email id
o If user enter correct secret key then system will generate OTP and send it to the registered mobile number.
o "Haversine" Distance calculation algorithm is used to calculate TD region. It utilizes user current location.
o If user is within TD region then transaction are allowed. If user out of TD region transaction will be terminated.

Server module contains:
Authenticate user information
Password
Secret key
OTP
Generate TD Region
Transaction

XI. CONCLUSION

Using this system user can be able to do secure transaction from mobile with the help of location and anti-spoof GPS. In case of physical attack, our system creates a virtual environment with extra bit in password.

XII. REFERENCES

1. J. Kang, D. Steiert, D. Lin and Y. Fu, "MoveWithMe: Location Privacy Preservation for Smartphone Users," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 711-724, 2020.
2.J. Kwak, J. Kim and S. Chong, "Proximity-Aware Location Based Collaborative Sensing for Energy-Efficient Mobile Devices," in IEEE Transactions on Mobile Computing, vol. 18, no. 2, pp. 417-430, 1 Feb. 2019.
3. G. SRIRAM, B. SRIKANTHREDDY, K. V. SESHADRI, K. H. KUMAR and N. SURESH, "Location Based Encryption-Decryption System For Android," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 590-593.
4.I. Ahmad et al., "Current technologies and location based services," 2017 Internet Technologies and Applications (ITA), Wrexham, 2017, pp. 299-304.
5.Sasikumar, D., "Mobile Banking and Security Challenges," in International Journal of Scientific Research and Management (IJSRM), 2017, pp 6014-6018
6. T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation l based on a fog structure for cloud location services," IEEE Access, vol. 5, pp. 7692–7701, 2017.
7. L. Nosrati and A. M. Bidgoli, "A review of mobile banking security," 2016 IEEE Canadian Conference on

Electrical and Computer Engineering (CCECE), Vancouver, BC, 2016, pp. 1-5.
8. T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," IEEE Access, vol. 4, pp. 673–687, 2016.

