An Android Bank Application: Location-Based Encryption

[1]Kiran P. Somase, [2]Nikita S. Patil, [3]Ruchita R. Gadiya, [4]Shubham U. Dhake, [5]Kushagra Anand.
[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Computer Engineering,
[1]Dr D. Y. Patil Institute of Technology, Pune, India

Abstract: A bank is providing a mobile application to their customer. We are developing a Location-based Encryption System which is a banking application. As compared to current banking application which is location independent, we are developing banking application which is location dependent. The user can perform transaction only if he/she is within TD region. TD region is an area of Toleration Distance (TD) where the user can perform the transaction. If the user goes out of TD region then the transaction will terminate automatically. We are providing extra security by OTP and secret key.

Index Terms **- Location Privacy, Mobile Networks, AES, GPS, Toleration Distance**

I. INTRODUCTION

Security has always been an important 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 was added to human security concerns. We are developing banking application using Location Based Encryption. As compared to current banking application which is location-independent, we are developing banking application which is location dependent. It means User can perform transaction only if he/she is within TD region. TD region is an area of Toleration Distance (TD) where the user can perform the transaction. If the user goes out of TD region then the transaction will terminate automatically. In our system user register himself/ herself in our application. He/she provide the personal details like name, mobile number, email id, secret bit, etc. then the system will send the encrypted password to email. Encrypted password means " Secret bit" is added to the password, this is done to protect password from visualization. After entering correct username and password user will login to the system and get the secret key on registered email id. If the 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 specifies a range in meters. After the generation of TD region, the user can successfully log in and perform the bank transactions. Our system is flexible enough to provide access to the customer to his/her bank account from any location. Our system also provides the solution to physical attack using virtualization, password send on email is encrypted by secret bit.

II. SYSTEM ARCHITECTURE

In our system user register himself/ herself in our application. He/she provide the personal details like name, mobile number email id, secret bit, etc. then the system will send the encrypted password to email. Encrypted password means Secret bit is added to the password, this is done to protect password from visualization. After entering correct username and password user will login to the system and get the secret key on registered email id. If the 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 specifies the range in meters. After generation TD region successfully, user can view account details and User can perform money transaction operation.

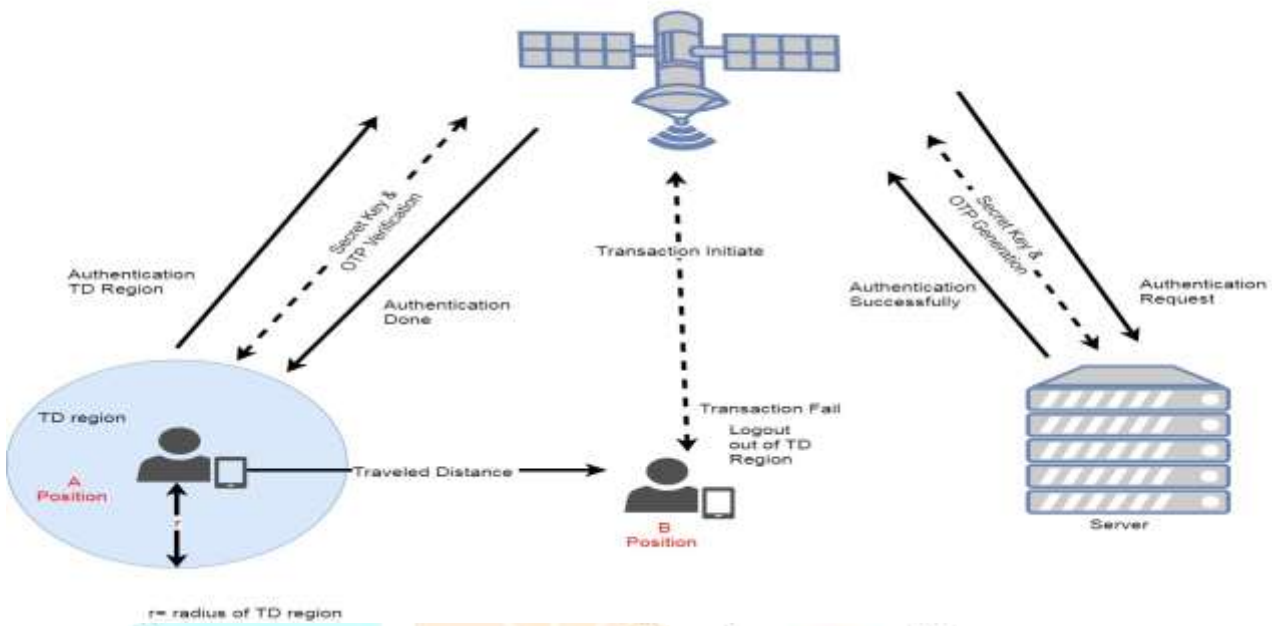

Fig.1 Software Architecture

III. METHODOLOGIES

3.1. Haversine Algorithm

This algorithm is used to calculate the distance from target point to origin point.

1. R is the radius of the earth in meters.
   Lat_o= latitude of origin point, $Long_o$ = longitude of origin point

   Lat_T= latitude of target point, $Long_T$= longitude of target point
2. Difference in latitude = Lat_o-Lat_T
   Difference in longitude = $Long_o$-$Long_T$
3. Φ =Difference in latitude in radians
   Λ =Difference in longitude in radians
   O= Lat_o in radians
   T= Lat_T in radians
4. A= sin(Φ/2) * sin(Φ/2) + cos(O) *cos(T)*sin(Λ/2) *sin(Λ/2)
   B= min (1, sqrt(A))
5. Distance = 2*R*B

3.2. KNN Algorithm

1. Determine parameter K = number of nearest neighbors.
2. Calculations are done based on the distance between the query-instance and all the trainings samples.
3. Sort the distance and determine nearest neighbors based on the K-th minimum distance.
4. The nearest neighbors of category y are to be gathered.
5. Use the simple majority of the category of nearest neighbors as the prediction value of the query Instance.

3.3. AES Algorithm

The following are AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. The block data (plain text) is initialized to state array.
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

3.4 Block Diagram

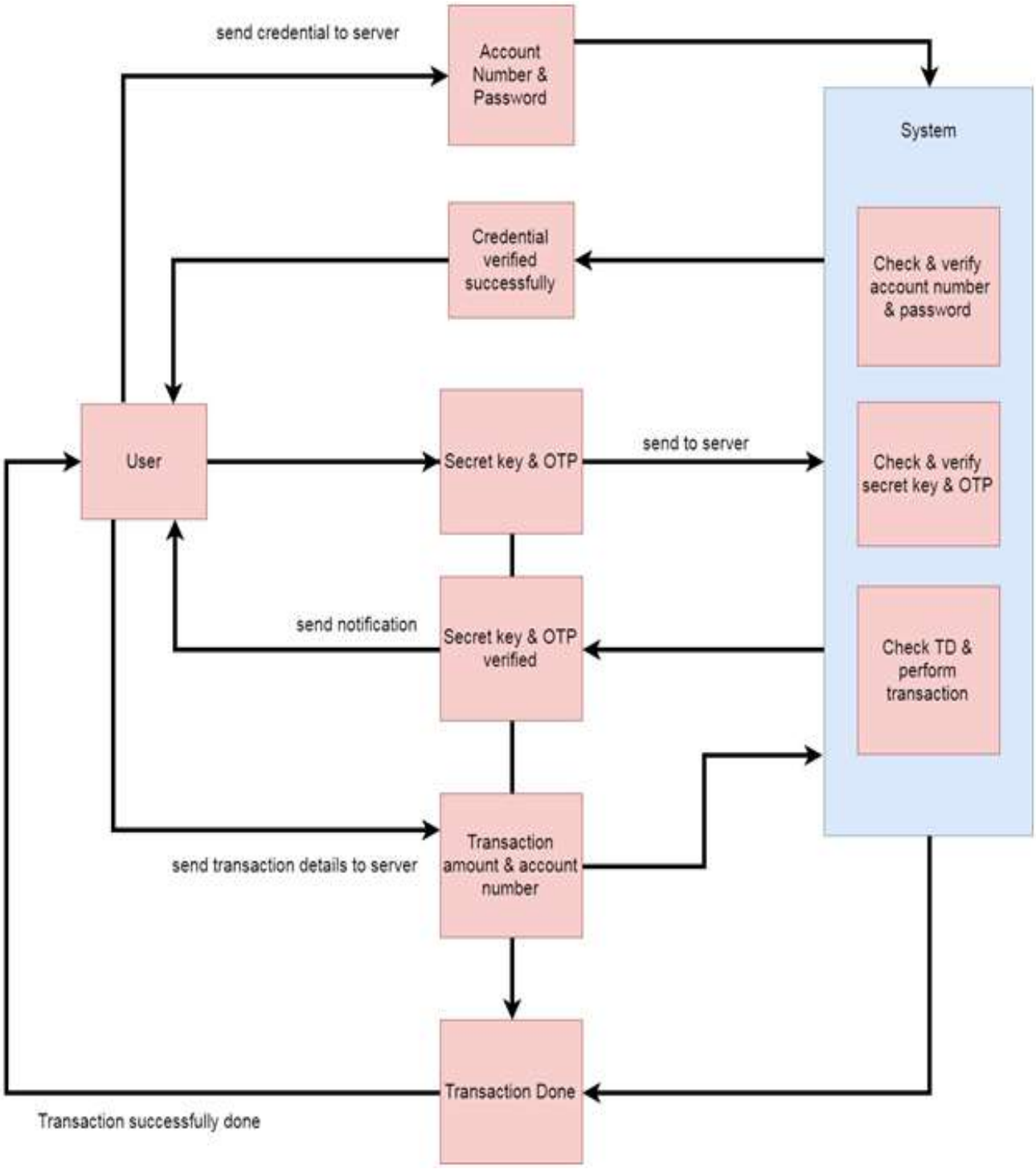

Fig.2 Block Diagram

IV. FLOWCHART

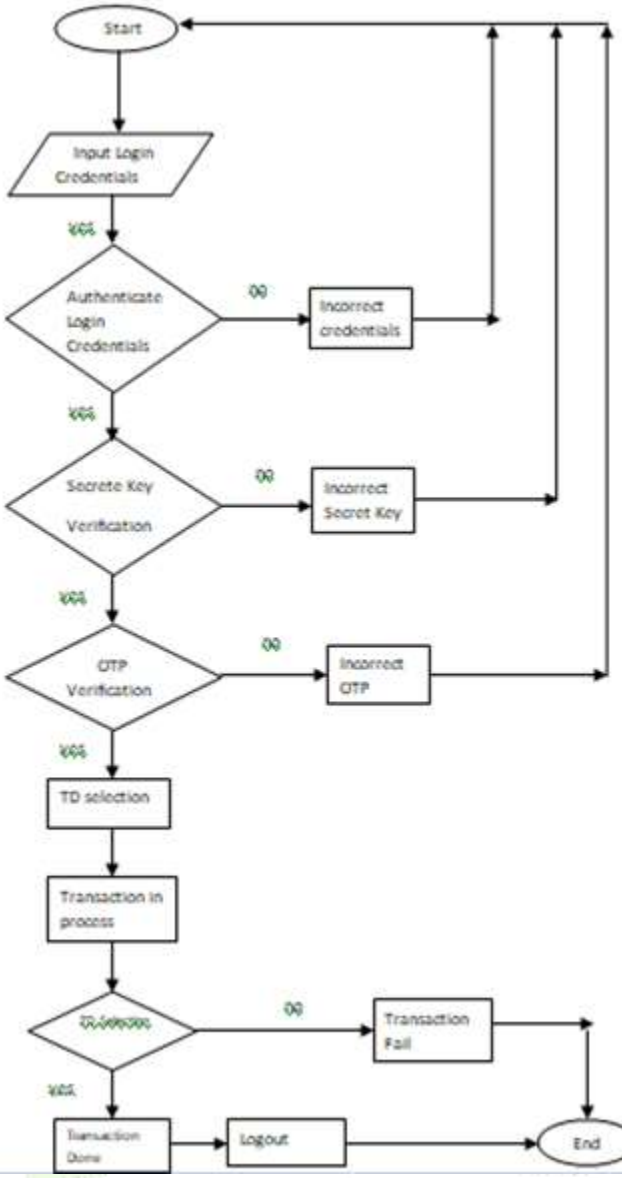

Fig.3 Flow Chart

IV. RESULTS

4.1 Results and Snapshots

1. The given below Figure.4 is a transaction page. When the user is within in TD region he will perform the transaction.

Fig.4 Transaction Page

2. The given below Figure.5 is when user forgets the password. When a user forgets password, he will receive an OTP on his phone number and he can reset the password.

Fig.5 Forget Password Page

3. The given below Figure.6 is for the transaction. The user actually performs transaction here.

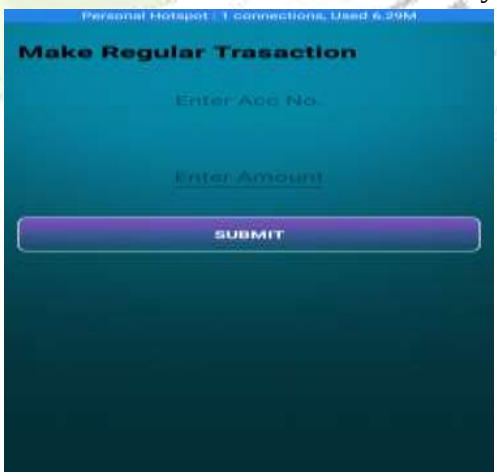

Fig.6 Regular Transaction

4.1 Testcases

Table 4.1: Testcases

Test Case Id	Test case	Test case I/p	Actual result	Expected Result	Test case criteria
1	send secret key to email	secret key	secret key send to email	secret key should send to email	Pass
2	send OTP to mobile	OTP	OTP send to mobile	OTP should send to mobile	Pass
3	Generate TD region	Range in meters	TD region generated successfully	TD region should generated successfully	Fail
4	Out of TD region	Range in meters	TD region terminates	TD region should terminate successfully	Pass

V. CONCLUSION

We are developing a Location-based Encryption System which is a banking application. As compared to current banking application which is location-independent, we are developing banking application which is location dependent. It means User can perform transaction only if he/she is within TD region. TD region is the area of Toleration Distance (TD) where the user can perform the transaction. If the user goes out of TD region then the transaction will terminate automatically.

We are providing extra security by using the secret key and OTP. The study shows that location could increase the security of the banking application.

REFERENCES

[1] Hui Zhu, Member, IEEE, Rongxing Lu, Senior Member, IEEE, Cheng Huang, Le Chen, and Hui Li, Member, IEEE. An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud, 65(9),11 November 2015.

[2] 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.

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

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

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

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

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

[8] 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.