Three Tier OTP Generation for Secure Banking Applications

Pranjal Rajendra Hole [1], Renuka Rajendra Mhetre[2] , Manali Pravin Gujar[3] , Mayawati Ashok Kalewar[4]

Prof. M.D. Ingle (Asst. Prof.)

Department Of computer Engineering, JSPM's Jayawantrao Sawant College Of Engineering

Abstract

New method describe the methods of how the two stage authentication is implemented using Message OTP or mail OTP generated by phone One Time Password to make secure user of customer accounts during various transactions. The proposed process gives the us the guarantees of authenticating online banking features are secured and also this method can be useful for various e-shopping scenarios as well as ATMs. Authentication and private key generation securely over insecure channel is a big factor. If One time password(OTP) is generated from the server and it get to the user but if OTP get hacked over network then that transaction may be done by the hacker so as a banker or application owner we have to send secure OTP to banking customer or user. Our system explains three level security for the OTP while doing transactions. The whole transaction is based on public key and private key as well as with advanced encryption standard (AES).

Keywords: *Encryption, Decryption, OTP, AES Algorithm, Security, Application, Division.*

1.INTRODUCTION

Now-a-days e-Banking application has increased more frequently because of use of bank from customers in terms of time, space, and synchronization. Banks draw information into the pub/sub system, and customers specify the events of interest by means of subscriptions. Published actions are navigated to their relevant bank user of customers, without the bank knowing the relevant user of customers or vice versa. This separation is traditionally not secure by intermediate navigation over a any network.

Secured bank login need to consider and include some factors which can secure the bank account login process. So what is that we are going to do here, encrypt the passwords? Yes that could be the only thing we can do to save our lives from the hackers who try hacking our bank accounts. So now the question is how, how exactly and appropriately are we going to do this?

This application provide a security for the customer OTP over network. Every time when customer wants to do any banking transaction in the application a new OTP is generated for him/her and that OTP is secured or encrypted and sends to the customers registered mobile number. Customer has to convert that OTP with the help of a private key owned by user. Then that converted password is checked into to user mobile app provided by bank (this is done in application). Now user can login using his decrypted password.

2.PROBLEM STATEMENT

To overcome problem of Man-In-Middle attack and enhancing authentication for online transaction using mobile one-time -password using encryption and decryption algorithm.

3.EXISTING SYSTEM

3.1Related Work:

Encrypted key share to the network can be hacked by the hackers but that key is encrypted so no hacker can decrypt that key as he don't know whether it is encrypted or not. Even anyone can open that received OTP into customers inbox, that OTP is also in the encrypted format. The system going to provide android application which will be useful to decrypt that encrypted OTP. Our proposed system provides three level security to the bank customers. Different encryption techniques are used in proposed system to decrypt the one time password.

In previous systems generated OTP was either in number format or in string format but in proposed system the generated OTP is combination of number as well as alphabets therefore, the security level enhances.

4.PROPOSED SYSTEM:

4.1Features of proposed system:

- Dynamically generating OTP
- Encryption of OTP using AES algorithm, OTP division technique and RSA algorithm.
- Asymmetric key encryption technique
- Secure login task(OTP send to only registered mobile)
- High Secure logged out process(used OTP deactivated)

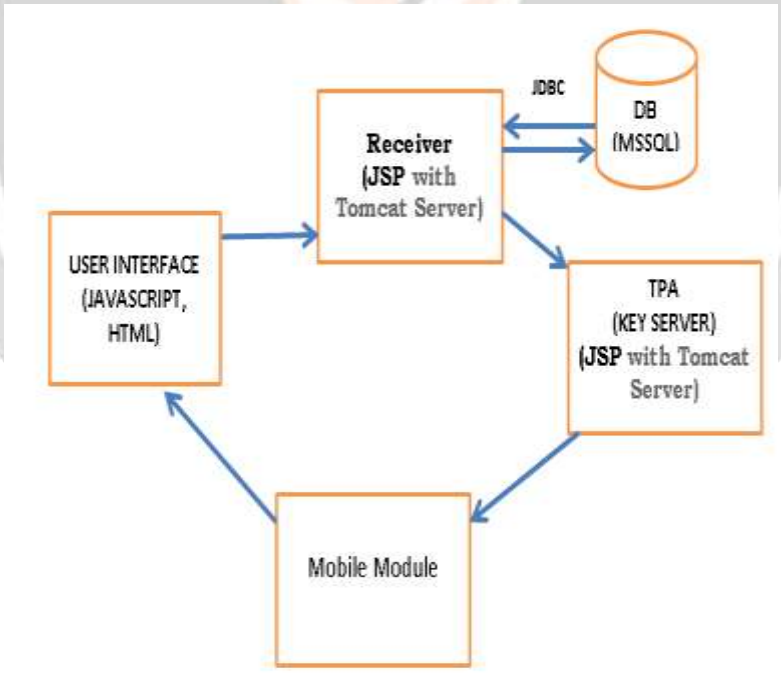

Figure 1: Block Diagram of System

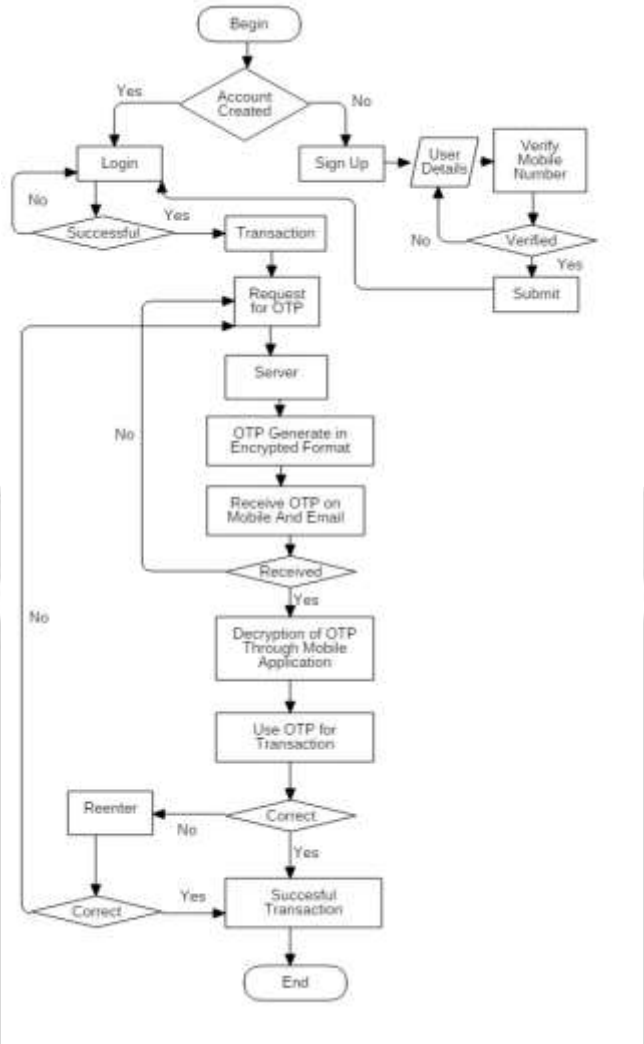

Figure 2: Flowchart of System

5.DESCRIPTION

In proposed system we are going to use android application for OTP decryption. when customer login after entering login id and password then one OTP will be received on the customer mobile in the encrypted format. Here, to encrypt that OTP using AES Algorithm and OTP division algorithm. AES Algorithm will convert public key into private key[2] and OTP division algorithm[5] will divide the OTP into two parts and encrypt them individually, the divided OTP also get reversed before encryption of OTP. We are using different pattern for encryption of OTP. Public key is the key before encryption and private key is the key after encryption. when that private key (encrypted OTP) reach to the customer mobile then with the help of android application we can convert that private key into original public key.

To open android application customer has to enter password. After entering correct password application will be unlocked then customer will get an option to select any message from the inbox for decryption purpose. Once customer select the message for decryption that message OTP will display into android application interface then customer will use that OTP to complete login process.

After logged in customer will get option for various transactions such as withdraw money, deposit money, transfer money, balance enquiry etc .After login for every transaction same way OTP will be encrypted and will send to the customer mobile.

6.FEASIBILITY STUDY

Feasibility has following dimensions and here is a brief description in context to our project.

- Technical

Technical analysis starts with an assessment of the technical viability of the proposed system. In this study we made an analysis on what technologies can be used to accomplish system function and performance. We have come to the conclusion that netbeans and JSP are most suitable for the project as netbeans open source software. Moreover netbean is the most widely used O.S on most of the handsets available

- **Financial**

The financial investment is feasible for creating this application. For MOTP application development, android plug in can be used in netbeans which is an open source package. The database will be built using Oracle which has a better concurrency control. JSP will be used for accessing the database.

- **Operational**

The project being developed is very useful as the searching of ads is based on the user's preferences and feedback; hence it saves user's time.

7. ALGORITHMS

I. OTP generator algorithm

OTP Generator algorithm is the hashing algorithm other than converting into encryption or authentication algorithm. The main purpose of this algorithm is to send a set of bytes into another set of bytes. Moreover, this is not able to be undone or altered algorithm, which means that the output can't be used to get the source.

This algorithm uses a private key to send one byte array into another byte array. This secure key must be minimum 20 bytes , which conclude that the algorithm take 20 bytes secret key with 8 bytes counter to create an 8 digit number. This OTP will be valid for a next few minutes.

II. AES Algorithm

It stands for **Advanced Encryption Standard.** Basically this Algorithm is a symmetrical key algorithm, it means that the similar key is key is used at both the scenarios i.e. encrypting and decrypting the data. Besides, it is depends on the design principle.

This paper is applying AES Algorithm for the protection or securing of the sensitive, important and the confidential data of the bank customer or user. In this paper, we are developing an application where the hacker or any anonymous even if hacks the customers OTP or data somehow, he/she will get permission to the customer's data but in an secured or encrypted form. Moreover, the android app developed by bank , can have facility to convert the encrypted OTP into decrypted format. But even if he/she tries to access the customer OTP over network, he/she will get the data in the encrypted form only, which will be only be decrypted or converted into original form by following the procedure of the OTP generation. This algorithm uses matrix i.e. 4*4 column-major order matrix of bytes.

OTP Algorithm:
To secure any banking system, the created OTP must be difficult to fetch, guess or trace by hackers. Therefore, it is important to generate a robust secure OTP generating algorithm. OTP algorithm can be used some factors to generate a tough-to-guess password. Customers or Users seem to be willing to refer easy factors such as their phone number and a Personal Identification Number (PIN) for services i.e. authorizing mobile micro payments, so we develop a Secured Cryptographic algorithm [9]. The distinct OTP is created by the mobile app offline, without server connectivity. The mobile will use some unique/distinct info in order to generate the OTP. The server will use the same unique information and validate the OTP. In order for the system to be secure, the unique OTP must be hard to predict by hackers. The following factors will be used to generate the OTP:

ATM PIN: Needed for verifying the authenticity of the client. If the phone is stolen, a valid OTP can't be generated without knowing the user's PIN. The PIN isn't stored in the phone's memory. It is only being used only to generate the OTP and destroyed immediately after that. *Two Factor Authentication Using Smartphone Generated One Time Password* www.iosrjournals.org 87 | Page

Timestamp: It can be used to generate distinct OTP, which is valid for a less time. The time duration on the mobile should be cyclic with the one from the backend[4].

IMSI number: It for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the (SIM) card in the mobile phone. This number will also be stored in the server's database for each client.

DOB: Birth date of customer whose going to use the application.

Username: Username of customer provided by bank.

How OTP Generated: The Username, password, birthdate of customer is taken from the customer and then concatenated with the current date, time and the time stamp for which the OTP is valid. This concatenated string is then given as input to Secured Hash Algorith (SHA1) algorithim. SHA- 1 algorithm returns its message digest which is 20 bytes value. These 20 bytes are reduced to 5 bytes by XORing a group of 4 bytes , i.e byte no. 1, 4, 8, 12 are XORed ; 2, 5, 9, 13; 3, 6, 10, 14; 4, 7, 11, 15; 5, 8, 12, 16; 17, 18, 19, 20 are Xored. Then from this 5 byte value, every byte is right shifted with 4 digits and then is converted to hexadecimal. Finally by converting the ASCII values to a character string, it is displayed as a onetime password to the user.

8.AES ALGORITHM MATHEMATICAL MODULE

Sr. No Algorithm Strategy

1. Customer (C) this is actor handles system functionality.
   SET OF U = {1.....N}
2. Enter the msg for Encryption (Ec) & Decryption(Dc). For example "hello" &"$!~v^gdj".

   Enter the OTP Key for data Encryption and Decryption.
   For example "XXXXXX".

   String str1 = Ec{"hello"};
   String str2=Dc{"$!~v^gdj".};
   Output Ec="$!~v^gdj";
   Output Dc="hello";
3. Check that the input data is provided or not.

   Check that he password key is provided or not.

Check that the provided input is valid or not.

4. If Customer call Ec function and provided input for Ec function is invalid then system will get Exception.

   If Customer call Dc function and provided input for Dc function is invalid then system will gives an Exception.

   If user provided all the input correct then system will generate success message else system will generate failure message.

5. Let S is the closed Intrusion Detection system such that
   S = {Message, K | d, A}
   where Message represents the data to be encrypted, K is secret key, A is encrypted Data

   .....
   Let be a rule of K, Message into A such that for given AES; it returns
   . Encrypt (K, Message) |A.
   . Decrypt (K, A) | Message.
   .....
   Encryption / Decryption
   Assuming a 128-bit key, the given key is arranged in the form of a matrix i.e. 4 × 4 bytes. With the input block, the first word from the key fulfils the 1st column of the matrix, and so on.
   Four column words of the key matrix are expanded into a best schedule of 44 words. Each round stage takes four words from the given key schedule.

9. FUTURE SCOPE

1. OTP is the form of security offered. security can further be enhanced with the use of firewalls and antivirus also lot of work is been done on various other authentication and authorization techniques.
2. The security and authentication is obtained by employing morphological attributes like face or finger etc. Further for improving the accuracy and efficiency of the system, biological attributes like heart beat rate, DNA analysis can be used and provide secure authentication to the system.

10. CONCLUSION

- One Time Password using Three Level Security provide tight security for transaction. Password can easily be exploited in general however OTP reduces the chances of misuse of password.

- Hacker can easily hack the OTP from network but using this module the hacker will get OTP in encrypted format which is difficult to decrypt by hacker hence our system increases the security level during transaction.

References

[1] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, 2,Muhammad Khurram Khan " OTP-Based Two-Factor Authentication Using Mobile Phones" 2011 Eighth International Conference on Information Technology: New Generations

[2] Eddy Prasetyo Nugroho, Rizky Rachman Judhie Putra, Iman Muhamad Ramadhan "SMS Authentication Code Generated by Advance Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP)

to Activate New Applicant Account" 2016 2nd International Conference on Science in Information Technology (ICSITech)

[3] Sagar Acharya1, Apoorva Polawar2, P.Y.Pawar3 "Two Factor Authentication Using Smartphone Generated One Time Password" IOSR Journal of Computer Engineering (IOSR-JCE)

[4] W.B.Hsieh, J.S.Leu: "Design of a time and location based one time password authentication scheme", 7th IEEE International Conference,2011.

[5] lloyd alan fletcher and rangachar kasturi, member, ieee "A Robust Algorithm for Text String Separation from Mixed Text/Graphics Images" Ieee Transactions On Pattern Analysis And Machine Intelligence, Vol. Io. No. 6, November 1988

[6]Saqib Hakak, Amirrudin Kamsin, Palaiahnakote Shivakumara, Mohd Yamani Idna Idris, Gulshan Amin Gilkar "A new split based searching for exact pattern matching for natural texts"

[7] G. Krishnamurthy and D. Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box," International Journal of Computer Science and Network Security, vol. 8, no. 9, pp. 388-398, 2008.

[8] E. Sediyono, K. I. Santoso, and Suhartono, "Secure Login by Using Onetime Password Authentication Based on MD5 Hash Encrypted SMS," International Conference on Advances in Computing, Communication and Informatic, pp. 1604-1608, 2013

[9] William Stalling, "Cryptograhpy and Network Security Principles and Practices", 5th ed. New Jersey, United States of America: Pearson Education, 2011.