INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Three tier OTP generation and image-based authentication for secure banking application

Renuka Rajendra Mhetre
renukamhetre@gmail.com
JSPM's Jayawantrao Sawant College of Engineering, Pune, Maharashtra

Pranjal Rajendra Hole
holepranjal@gmail.com
JSPM's Jayawantrao Sawant College of Engineering, Pune, Maharashtra

Manali Pravin Gujar
manaligujar1998@gmail.com
JSPM's Jayawantrao Sawant College of Engineering, Pune, Maharashtra

Mayawati Ashok kalewar
maya34kalewar@gmail.com
JSPM's Jayawantrao Sawant College of Engineering, Pune, Maharashtra

ABSTRACT

New method explains a method of how the two-factor authentication implemented using SMS OTP or Email OTP generated by Smartphone One Time Password and image-based authentication to secure user accounts during transactions. As talking about the secured bank login over here so we need to consider and include some factors which can secure the bank account login process. So what is that system is 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 exactly and appropriately System going to do this? In the market we have many security systems for online banking transactions. But many of these systems have lots of limitations which are as follows: Actual password sending to mail: If server send password on mail id and if any person knows your mail credential then he can access your password. So less security is there in the existing system. Permanent storage of passwords in Database: Password comes from server send into the database so if one person knows that password then he can use it for future transactions No usage of Cryptography techniques: IN existing systems there is no use of cryptography. In the market, there are some other security systems for online transactions such as OTP and MOTP, but these systems do not have an enhancement in securities so we are going to enhancement the MOTP security by providing multiple passwords to any transaction. Some of the other technologies available to cater to the same problem.

Keywords— *Encryption, Decryption, OTP, AES, Image-based authentication, Algorithm, Secure, Application, Division*

1. INTRODUCTION

1.1 Two factor authentication using smartphone generated One Time Password

The System involves generation of Secured OTP using Cryptographic algorithm and delivering it to user's mobile in the form of SMS or user can able to create his own OTP using a smartphone and validating the OTP using same Cryptographic algorithm. The proposed system is secured and consists of two parts: (1) The server software (2) The client software: Client application on PC for transaction & android application on a smartphone for creating OTP.

1.2 Providing multi-authentication using multi-biometric cryptosystem for enhancing security

In this system multi biometric features of individuals are used. Multi biometric traits like fingerprint, iris, face, and signature are used. These images are first resized and fused into a single image.

For authentication purposes, elliptic curve cryptography is used. It is a public key cryptography method. One time password is also included for high secured authentication. This one-time password is sent to the user mobile and the user types the password to this system if it is a valid password the user is authenticated. Performance is measured in terms of the false acceptance rate and false rejection rate. Compared to the existing system, the proposed system efficiency and accuracy is increased.

1.3 Purpose

Purpose of our project is to provide an enhancement in banking security for each online banking transactions.

1.4 Project scope

The system is going to provide security for the user password. Each time when user wants to login in the site a new password is generated for him and that password is encrypted and sends to user mail id. User has to decrypt the encrypted password with a private key owned by the user. Decrypted password is sent to user mobile (this is done in application). Now user can log in using his decrypted password.

2. PROBLEM STATEMENT

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

3. FEASIBILITY STUDY

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

3.1 Technical

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

3.2 Financial

The financial investment is feasible for creating this application. For MOTP application development, android plug in can be used in netbean 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.

3.3 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.

3.4 Product Features

- Changing Password Regularly
- Password Encryption using RSA algorithm
- Asymmetric key encryption technique(public key and private key)
- Secure login process(password send to only personal mobile)
- Secure logged out process(used password deactivated)

4. OPERATING ENVIRONMENT

4.1 End user

Web application developed in netbean IDE for doing online transaction

4.2 Server

Minimum Dual-core 2.2 GHz processor, Minimum 4 GB RAM, Windows XP or extended versions of Windows, any web browser, Minimum 160GB HDD, working internet connection with a minimum bandwidth of 1Mbps to cater the user requests quickly.

4.3 Design and Implementation Constraints

Our web application is developed in JSP using netbeans 7.4 IDE. Our application will have the following modules

- Registration Module
- Encryption and Decryption Module
- Mail Module
- Mobile Module
- Login and Transactions Module

5. SYSTEM FEATURES

Functional Requirements should include

- Descriptions of data to be entered into the system. The input to be entered includes user credentials.
- Descriptions of work-flows performed by the system

5.1 End user

Customer will enter his credentials for online transactions.

5.2 TPA

TPA will receive public key sent by the server and then that key gets converted into a private key and send it to the user mobile.

5.3 ImageBased Authentication

Username and password are the most commonly used mechanism for authentication because of simplicity and convenience. However it suffers from few drawbacks like the selection of weak passwords by the users, users disclosing their passwords etc. This weakens the security posture of the organizations. Hence we propose a new image based authentication system. Research suggests that the use of images may be more effective in terms of security and ease of use for some application. This is because we, humans are good at recognizing images than remembering password. In this project, we describe a new image based authentication system which can be used independently or along with the current character based authentication system to improve security and usability. We implemented the said system along with current authentication system (username and password).

We carried out the user survey. Around seventy users including students and faculty tested the system and gave their feedback. After analysis, one of the key outcomes is that 97% were able to register with the system and 94% we able to successfully authenticate with the system.

In this project, we have added one more security level for login. When customer registration happens, customer can select his/her images for verification during the login process.

When Customer does login after entering account number and password then it moves to the image verification page where some images will be displayed including one image of that customer. When a customer selects his own image then the only login will be success otherwise login will fail and it will redirect to login page again.

For this process, we created one page where customer can select some selective images for the further login process. We are storing that images into a folder in the application only and that image names into the database. During the login process, we are fetching some images from different users including login user also. If login user properly selects his image then the only login will be a success, otherwise, login will fail.

5.4 Mobile Module

This module is used to receiving a decrypted key which comes from TPA.

- External Interface Requirements
- User Interfaces
- Customer

JSP pages will be required for the following functionalities:

- Sign up or log in
- Deposit Transaction
- Pay Online

6. SYSTEM DESIGN

The system design is shown in the figure 1 below.

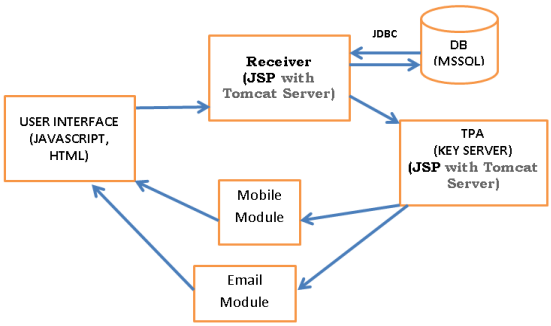

Fig. 1: Block diagram of system

6.1 Mobile Device

A device used by the end user to see the decrypted key. This mobile device supports Android OS or Windows OS.

6.2 I/O management

Input data will be customer's credentials, the output of server will be the public key which will be input for TPA, the output of TPA will be the private key which will decrypt and receives to the mobile as the output of TPA.

6.3 Network

The goal is to make browsing the Web application from any machine is more reliable and easily accessible. Standards improve the interoperability, usability, and accessibility of web applications.

6.4 TPA

Use of TPA is very important to convert the public key into the private key. TPA provides RSA algorithm to decrypt key sent by sever.

6.5 Database

The Oracle database is an entity that contains detailed information of all the users, clients and bank server stored in the form of tables. Normalization of database helps in removing redundancies and various anomalies.

6.6 Website

Website is just a medium of interaction for the bank customers and the bank server. A website that is accessible to the server and the customers will be built using JSP.

7. ALGORITHM

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on the public and private key system. The public key is made available to everyone. With this key, a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.

7.1 RSA Algorithm

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers greater than 10154. We then generate the encryption key e which must be co-prime to the number $m = '(n) = (p ¡ 1)(q ¡ 1)$. We then create the decryption key d such that $de\ modem = 1$. We now have both the public and private keys.

8. THE ENCRYPTION AND DECRYPTION PROCESS

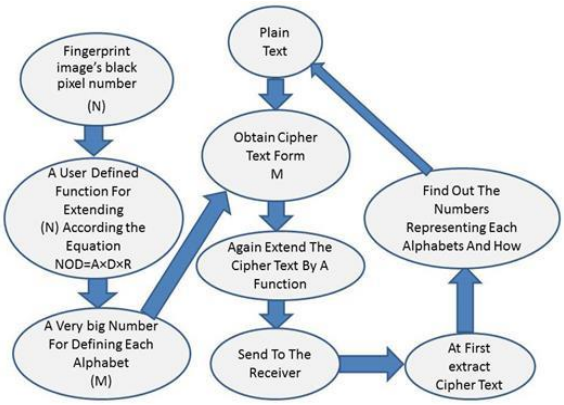

Fig. 2: Block diagram of the encryption and decryption process

8.1 Encryption

We let $y = E(x)$ be the encryption function where x is an integer and y is the encrypted form of x

$$y = xe\ mod\ n$$

8.2 Decryption

We let $X = D(y)$ be the decryption function where y is an encrypted integer and X is the decrypted form of y

$$X = yd\ mod\ n$$

8.3 Mathematics of the RSA Algorithm

Given: n = pq where p and q are distinct primes.

$$gcd(e;\ '(n)) = 1$$

$$de = 1\ mod\ '(n)$$

When

$$y = xe\ mod\ n \text{ and } X = yd\ mod\ n$$

Where

$$x < minfp;\ qg$$

Prove that:

$$X = x\ mod\ n\ 8\ x < n$$

Proof:

$$X = xde\ mod\ n$$

$$de = 1\ mod\ '(n)$$

$$'(n) = (p ¡ 1)(q ¡ 1) \text{ if p and q are distinct primes}$$

$$de = 1 + k(p ¡ 1)(q ¡ 1)$$

9. SCREENSHOTS

9.1 Login page

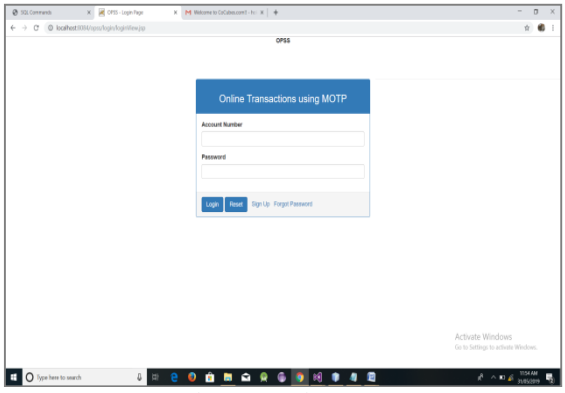

Fig. 3: Login page

9.2 Sign up page

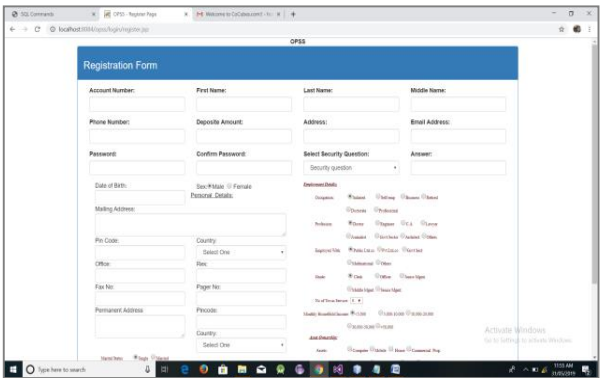

Fig. 4: Sign up page

9.3 Login validation

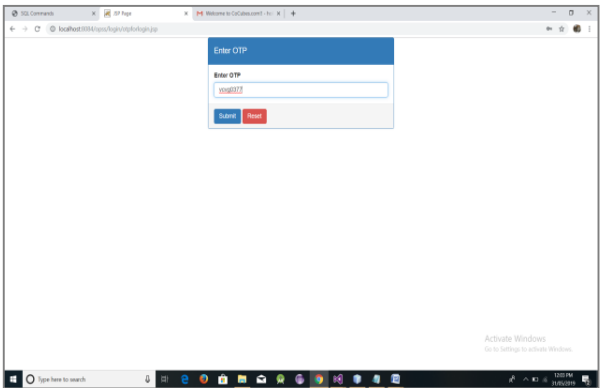

Fig. 5: Login validation

9.4 Image selection

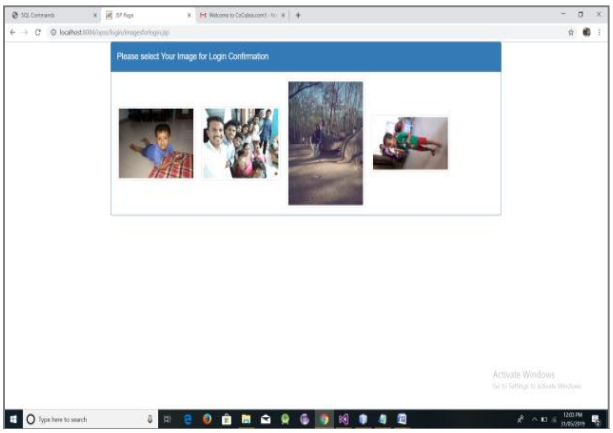

Fig. 6: Image selection

9.5 Login failed if incorrect image selection

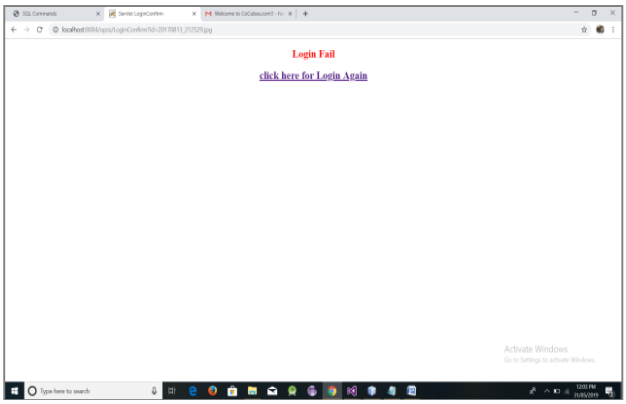

Fig. 7: Login failed if incorrect image selection

9.6 Main page

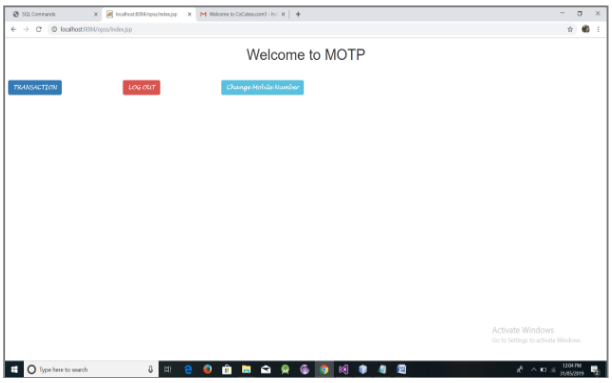

Fig. 8: Main page

9.7 Change mobile number

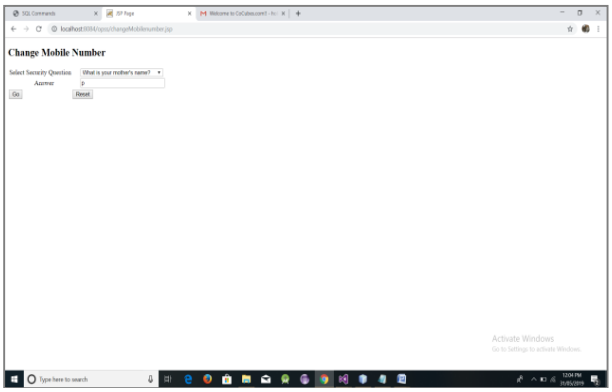

Fig. 9: Change of Mobile Number

9.8 Transaction portal

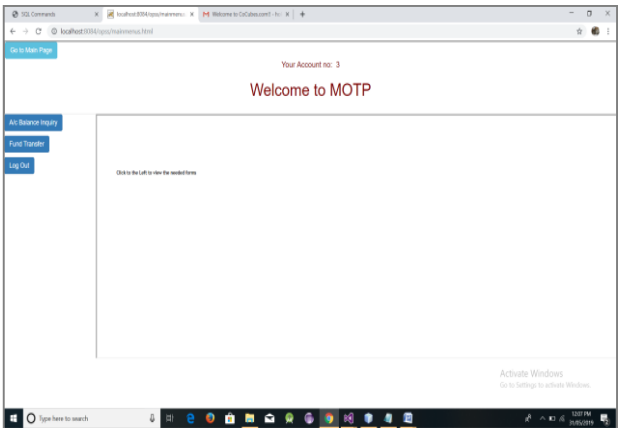

Fig. 10: Transaction portal

9.9 Balance enquiry

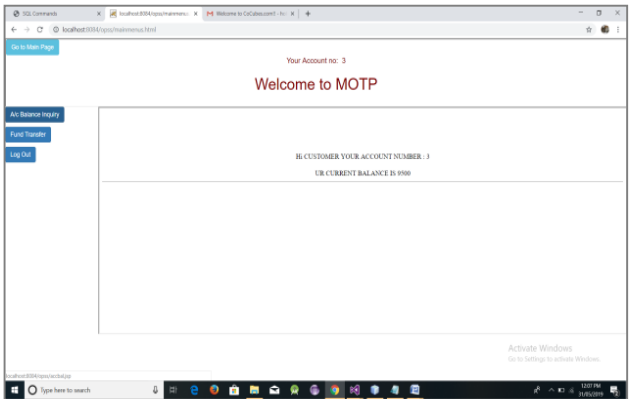

Fig. 11: Balance enquiry

9.10 Fund transfer

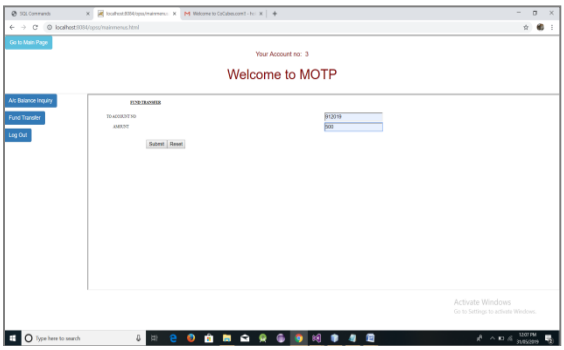

Fig. 12: Fund transfer

9.11 OTP authentication

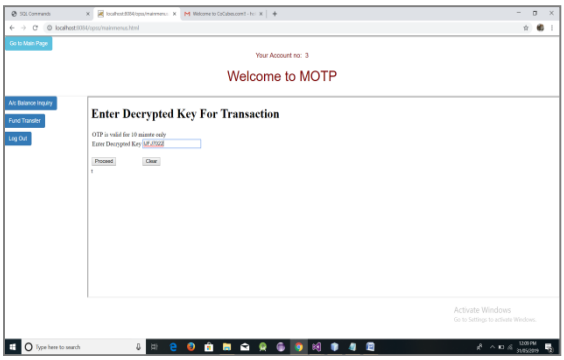

Fig. 13: OTP authentication

9.11 Successful transaction

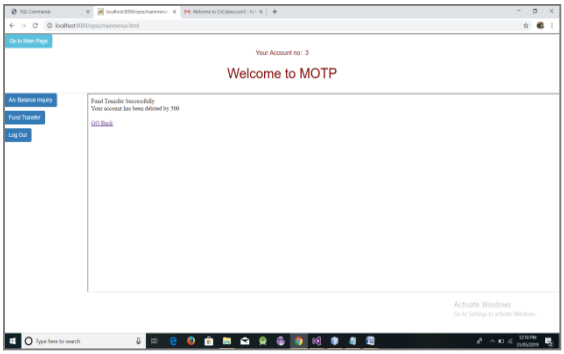

Fig. 14: Successful transaction

10. FUTURE SCOPE

- OTP is the form of security offered. Security can further be enhanced with the use of firewalls and antivirus also a lot of work is been done on various other authentication and authorization techniques.
- The security and authentication are 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.

11. CONCLUSION

One Time Password using Three Level Security provide tight security for the transaction. Provided password can easily be exploited in general however with the use of OTP user can make sure that the password will not be misuse 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 using image-based authentication, encryption and decryption.

12. 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 Advanced 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 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 Informatics, pp. 1604-1608, 2013

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

