IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Web Server for Online Banking System

Swapnil Pote
E&TC Engineering Student
Dr. D.Y. Patil Institute of Technology
Pimpri, Pune, India

Aniket Wani
E&TC Engineering Student
Dr. D.Y. Patil Institute of Technology
Pimpri, Pune, India

Vishal Nijwante
E&TC Engineering Student
Dr. D.Y. Patil Institute of Technology
Pimpri, Pune, India

***Abstract*— The main problem in any online banking system is to secure information stored on the web server while simultaneously giving each bank client an added level of privacy during each transaction. Traditional systems, unfortunately, do not allow for the server to hide an individual client's transaction details . As a result, there is a chance of being cheated by any bank employee or the authority who are responsible behind running the system. So we propose a method to design a secure web server for online banking system. In this system, we have introduced a secure money transaction process by introducing a smart key during each transaction made by the client or user. Only the valid client or authorized user can able to access his information. To do so, he must first register with the system by entering some basic personal information. However, it's critical to remember the encryption key, which is used for both encryption and decryption. If a user forgets his or her key, he or she will be unable to complete any transactions.**

Keywords—online banking, web server, smart key, encryption, decryption.

I. INTRODUCTION

Data security is one of the prerequisites of any digital data transaction storage system. Web servers are the place where all the information of a system being stored. To provide secure data we can utilize a lot of processes, for example data encryption in client side or server side [1]. Data encryption is one most familiar sub system for securing digital data. Encryption involves taking a massage as input and producing output with completely different format from input one. To ensure security of data into web server, encryption process is a good choice [2]. The RC4 method is a relatively effective data encryption procedure among several sorts of encryption processes. It is a symmetric method in the sense that it utilises the same key for encryption and decryption [3]. In MySQL server, traditional systems employ less secure and preconfigured AES ENCRYPT () for data encryption and AES DECRYPT () for data decryption [4]. It means that traditional systems (such as online banking systems) will be unable to provide us with the needed capability of accessing encrypted data for a single authorised user. Individual user can't hide or encrypt data because in this system data will be encrypted globally. Using separate key for every individual user's data or information can provide extra degree of security. To ensure the security of data into web server by encryption process, a secure web server using RC4 algorithm has been proposed in this work. Only the valid client or authorized user can able to access his sensitive information privately. Even if any unwanted user enters into the server, he wouldn't be able to recognize any kind of encrypted information. At first individual user or bank client have to registrar himself to the site and while registering he will be provided a registration ID by the system. During registration, he must have to provide his name, national identity number and other relevant personal information .All registration information is maintained in the database after a user successfully registers on the site. By logging into his account, a client can make deposits and withdrawals. A client must enter a smart key during the deposition process. During money withdrawal or balance checking, that client must retype the same secret key. This key will assist him in concealing his balance money from any bank employee.

II HARDWARE AND SOFTWARE REQUIREMENTS

A. Front end Developing Tools

- Hypertext Markup Language (HTML 5)
- Cascading Style sheet (CSS 3)

B. Back end Developing Tools

- Java
- MySQL

C. Apps Tools

- Eclipse
- Apache Tomcat Server

III. APPLICATION IMPLEMENTATION

Online Banking System - offer flexible, client-server technology based on a scalable system. It is centralized, customer centric design to offer a complete set of integral retail banking modules sharing a user-friendly interface. OBS is developed for automate the process of day to day transaction of any bank; it has all the features need to operate the banking procedure. The system can be used to create new customer, modify details, deposit and withdraw the amount from his / her account.

From an end-user perspective, the Online Banking System Project consists of two functional elements:

- Customer transaction module: If you are a user you will be redirected to your Account Home Page.
- Admin transaction module. If you login as an Admin then you will be redirected to the Admin Home Page.
- Staff Module

Customer Transaction Module

An enhanced automized system is developed to maintain customer transaction. Features includes

- Creation of new banking customer
- Customer type – Current Account, Savings Account, Fixed Account
- Customer Creation Form.
- Existing customer details
- Customer Access Form
- Each customer login identified by Access Code and Account No.
- Banking Main menu option like.
- Transaction – Debit, Credit, Transfer
- Customer Detail – Modify Details, Lock Customer.
- Freeze/Unfreeze Account.
- Help – User Manual. • Transaction Summary
- Account Closing.

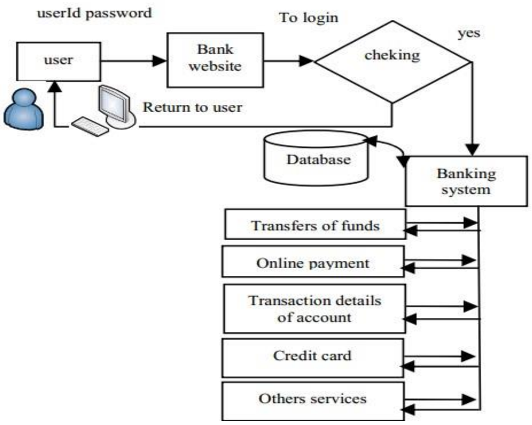
Admin Module

This performs the following functions: Verify created Individual Accounts, Manage existing accounts, View all transactions, Balance enquiry, Delete/close account etc

Staff Module

This performs the following functions:

Can see monthly Salary ,Can see working days details, Get latest notices and messages details.

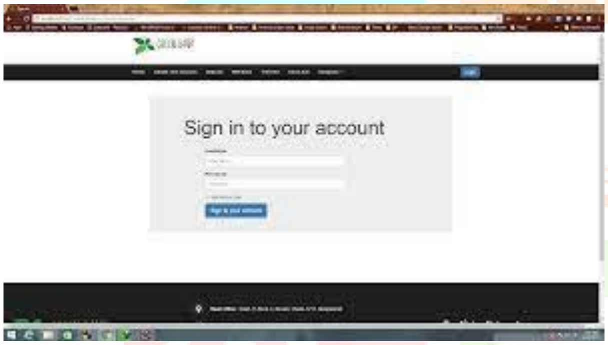


A. Registration Page

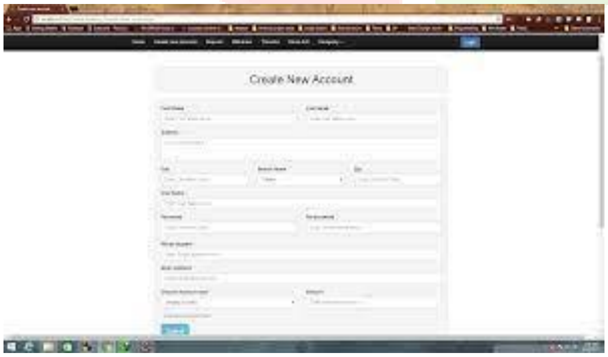
In this system every user must be registered by submitting a registration form. Here a user provides some basic information like Name, Nation Identity Number and Password.After successful registration, this system provides the user a registration number to the user applicant by which he/she can able to log in to the site using this registration number. This number is generated by. It is strongly recommended that user applicant must have to note down this registration number for the future activity.

B. User Profile Form

This page is created for collecting the details information about every user of this site. The administrator stores & analyses this user information.



Sign in to your account



Create New Account

C Transaction Page

This page is main transaction page. Here user can deposit money ,withdraw money ,check balance by clicking the respective button.

a. Withdraw Money Page

Here users can noticed that withdraw balance account has to be less than Deposit Money, withdraw Money, Check balance by the current balance. Also, user must have to insert the same encryption key at the time of deposit money the respective button. User can access this page if & encryption key at the time of deposit money. only if he/she is logged in to the site.

b. Deposit Money Page

By entering a secrete encryption key, user can deposit money to the bank account. This key encrypts the user information into the database.

c. The Check Balance Page

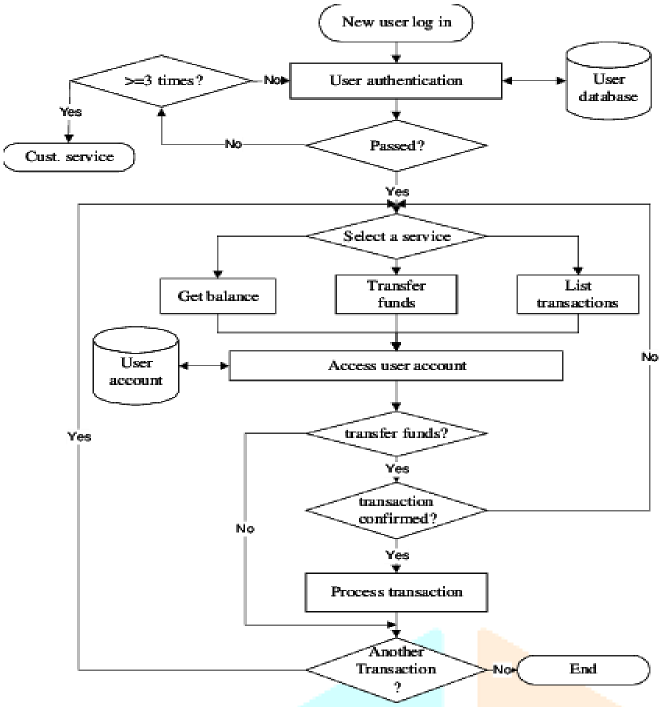
While checking balance in this site user has to insert the same encryption key which is used in previous transactions.

D. Admin Panel

Only the Admin of this site can access this admin panel page. This page contains highlighted info about every registered user. Admin can check or delete any user by clicking the profile option of that particular user.

IV. ENCRYPTION PROCESS

We have encrypted the client's registration ID & the user name and keep them into database table named Passbook. We have collected these two information (plain text) from the login database table using MySQL query.. We get the encryption key from the transaction query form. This key works as both encryption & decryption key. This key never saved or stored anywhere in this entire system .As we have both plain text & key text, we can apply the RC4 algorithm. Here variable $id & $person respectively contains the encrypted version of user registration ID & user



1.Create New Account: A customer who having the account in the world can create a virtual account through this module. This module receives the customer profile details and the bank account details with the proof of the ownership of the bank account.

2. Login: Virtual account holders can login in to the system using this module. Thus this is the secured login page for the customers in the website.

3.View balances: Firstly login your account with your account number and password. Then checking your balance doesn't require much work. You simply select Account balances and take a look at your balance and past transactions. If you have more than one account, you can also do transfers between accounts.

4. Bank Accounts: A customer may have more than one bank account in various banks, in this case, the customer prompted to decide which bank account should reflect in the account debit or amount credit. For these operations customers can add their owned bank accounts here and it will be approved by the administrations of the system.

5.Fund Transfer: This is the module to make fund transfer to the virtual bank account holders or the usual bank account holders from the customer's specified bank account.

6Beneficiary: Beneficiary is a person who receives money. Here the customer can add the beneficiaries to make fund transfer in the future.

7Transactions: This module displays the transactions made by the customer in the particular date with the transaction details.

8Administrative Control: This module contains the administrative functions such as view all virtual account, transactions, approve bank accounts, approve virtual accounts etc.

V. CONCLUSION

A web server is the most important component of a website. Any unauthorised attack on the server will make all of the information on the server public. We have built an encryption procedure in this work that will hide some of the sensitive data saved on the server, offering additional protection to any system. Here we have encrypted the client ID (bank A/C no) & client user name of an online banking system with. No unauthorized person would be able to know the encryption key & this key will never be stored anywhere in the system. Admin can check or delete any user's general information but still can't access any user's transaction information. It's very difficult to recover the user password. However, if the user can provide certain legitimate information, such as the last date of money transection, transection details (i.e., the purpose of money transection), and the user account number, the bank authority will renew the account with a new password based on the user's preferences.

REFERENCES

[1] Orvila Sarker, Mehedi Hasan, N.M.Istaiak Chowdhury, "A secure web server for E Banking",21st International Conference of Computer and Information Technology (ICCIT)(December 23,2018)

[2] Alexey V. Bataev, "Innovation Forms of Finnancial Institution Management :Cloud Automated Banking System "IEEE (2018)

[3] Chunsheng Song, Ruiping Huo , Shuiqing Wang, "Transformer Equipment Temperature monitoring based on the Network Framework of Django", University of Wollongon IEEE(2019)

[4] Jin Hyeong Jeon, Ki Hyung Kim, Jai Hoon Kim , "Block Chain based data Security Enhanced IoT Server Platform ", ICOIN , IEEE(2018)

[5] Kiyoshi Kanazawa, Kazumasa Takami , "Standby P2P Network to Substitute for Client-Server Network in Event of Interruption of Communication with the Server", Proceedings of TENCON 2018 IEEE Region 10 Conference (October 2018)

[6] Zhang L , Fan J , Zhou Y, "The Security Analysis of MYSQL's Encryption Functin ",IEEE Conference on on Computer Science and Mechanical Automation (2015)

[7] Yoso Adi Setyoko, Maman Abdurohman ,"SMS Banking Encryption Scheme", IEEE international Conference on Communication , Network and Satellite (2017)