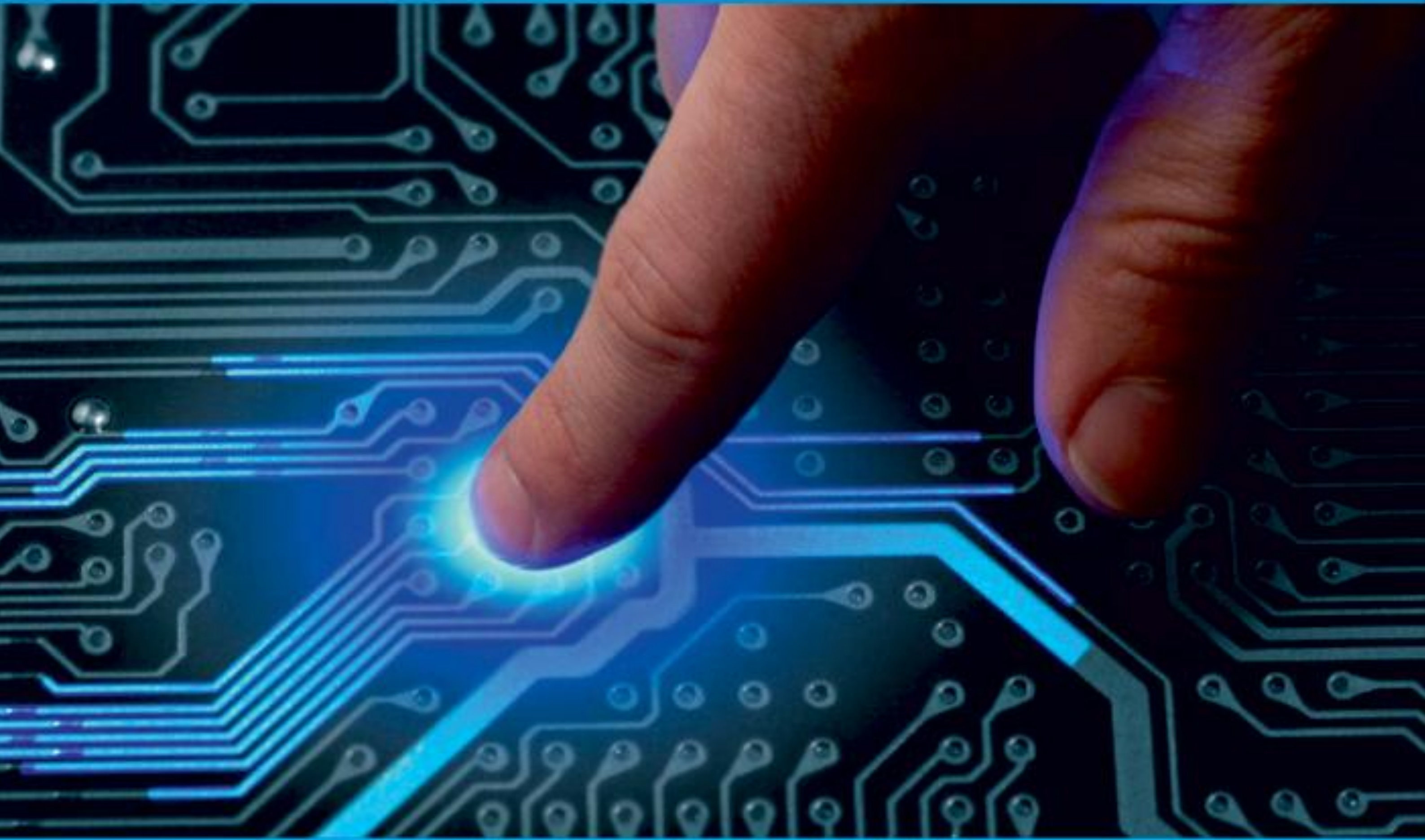
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

A Secure Web Server for E-Banking

Manasi Patil

Department of Computer Engineering JSPM'S Bhivarabai Sawant Institute of Technology and Research, Pune, India

ABSTRACT: The main issue with internet banking is that keeping track of everything is difficult. The system's goal is to keep the information on the web server secure. each and every transaction providing a higher level of anonymity to individual bank customers Traditional systems, unfortunately, do not work. Not enable the storage of a specific client's transaction information on the server to be hidden As a result, there's a risk of being discovered. the person in charge of the system's functioning has been mislead by any bank employee or government authority We shall propose an RC4-based technique for developing a secure web server in this project. The algorithm of an online banking system. In this system, we have a system in place.By establishing a secret key for each client transaction or user in a secure money transaction process. This information is only accessible by a legitimate client or permitted user.

I. INTRODUCTION

Data security must be a prerequisite in any digital data transaction storage system. Web servers store all of a system's data. in the interest of To protect data, for example, a variety of strategies might be used. Data encryption on the client or server side. The most well-known data security subsystem is encryption. a computer's stored information Encryption is performed using a massage as an input. and generating output in a different format than that which was used to input Encrypting data on the web server is an excellent technique to keep it safe. There are many different kinds. The RC4 algorithm is a popular encryption technique. Data encryption works well. It has a symmetrical layout.

Individual users will not be able to hide or encrypt data because the system will encrypt data worldwide. Using a different key for each user's data or information might add an extra layer of security. This study proposes a secure web server that uses the RC4 algorithm to assure the security of data entering the web server through encryption. Only the genuine client or authorized user has private access to his sensitive data. Even if an un-authorized person gains access to the server, he will be unable to decrypt any encrypted data.

Traditional systems (for example, online banking systems) are unable to provide us with the required capability of allowing a single authorized user to access encrypted data. Individual users are unable to conceal or delete their data. Because data will be encrypted in this system, encrypt data. Using a unique key for each user's information or information might add an extra layer of protection. To Encryption is used to protect the security of data entering the web server. Using the RC4 algorithm, a safe web server has been created. this work's proposal Only the legitimate client or authorized user has access to this information. The user will be able to access his personal information in a secure manner. Even if an unauthorized person gains access to the server, would be unable to decrypt any encrypted data information. Individual users or bank clients must first register on the site, and the system will supply them with a registration ID during the process. He must complete the registration process. must supply his full name, national identification number, and other personal information that is appropriate When a user clicks on a link After a user successfully registers on the site, all registration data is saved. is going to be saved in the database A customer can make a deposit or withdraw money. By logging into his account, he may withdraw money. Throughout the A client must input a secrete key during the deposition procedure. That During the money transaction, the customer must retype the same secret key. Checking your balance or withdrawing money. This key will assist you in concealing your identity. Even from any bank employee, he might get his balance money.

II. OBJECTIVE

- A secure web server for online banking that uses the RC4 algorithm;
- A secure money transaction mechanism that uses a secret key.
- Only the legitimate client or authorized user has access to his data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005315 |

III. SYSTEM ARCHITECTURE

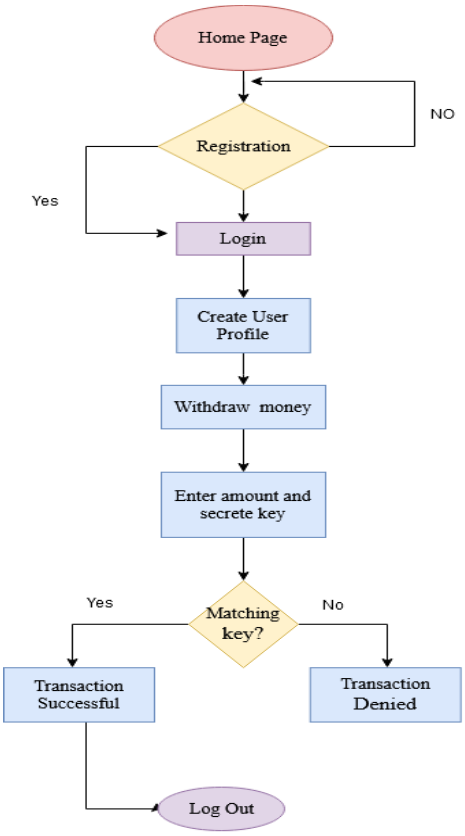


Fig 1. Flow Diagram

Proposed work:

A. Registration Page: Every user in this system must first register by filling out a registration form. A user enters basic information such as his or her name, national identity number, and password. After successful registration, the system issues the user with a registration number, which he or she may use to log in to the site. The php predefined function "math random" generates this number. It is strongly advised that the user application write down this registration number for future reference. After completing the registration process, you will be sent to the log in page. The account is secured by the user password and the unique registration ID.

B. User Registration Database Table: Once a user has successfully registered on this site, all registration data is saved in the database. For this site, we'll establish a database called "assessment." The Evaluation data base has multiple tables for recording user input from various fields. The "Login" table stores information about user registration. First name, last name, NID, username, password, date, regId, and submission are the eight fields in this table. The user registration identity number is stored in the "regId" field. Each user's registration identifying number is a one-of-a-kind piece of information. By authenticating this registration ID, we were able to join all tables belonging to the database "evaluation."

C. User Login Database Table: When a user successfully logs in to this site, all of their login information is saved in the "evaluation" database. The "User" database stores information on user logins. RegId (registration number), User, Password, and Date are the four fields in this table.

D. User Profile Form: The User Profile Form was intended to collect detailed information about each site user. This user data is saved and analyzed by the administrator. All profile information will be kept in the "ATM" database, and user profile information will be recorded in the "Pdetails" table, if a user successfully submits the user profile form to this site. This database can only be accessed by administrators, and this information may be erased from the database using the admin panel.

i.] Transaction Page: The transaction page is the most important page. By pressing the appropriate button, consumers may deposit money, withdraw money, and check their balance. If and only if the user is logged in to the site, he or she will be able to view this page.
ii.] Deposit Money Page: The user can deposit money into their bank account by inputting a secret encryption key. This key is used to encrypt user data before it is stored in the database.
iii.] Withdraw Money Page: This is the page where you may withdraw money. It's worth noting that the account's withdraw balance must be smaller than the current amount. In addition, while depositing money, the user must utilize the same encryption key.

IV. MATHEMATICAL MODEL FOR PROPOSED

WORK MODEL MATHEMATICAL

Let S stand for the entire system.
S stands for I, P, and O.
I-input
P-procedure
o-output
I-input
Textual Data = I
Where Data refers to a textual data of tweets.
P = I,
Using I, P
The system executes operations and calculates the forecast.
1. Encryption
2. Decryption

V. ALGORITHM

Rivest Cipher (RC4):

Rivest Cipher 4, often known as RC4, is a stream cypher and key algorithm with variable-length keys. This method encrypts each byte separately (or larger units at a time). Without knowing the input key, a key input is a pseudo random bit generator that creates an 8-bit stream that is unexpected.

The output of the enervator is known as key-stream, and it is merged with the plain text stream cypher one byte at a time using the X-OR operation. The RC4 encryption technique's key stream is completely independent of the plaintext used. In an 8 * 8 S-Box (S0 S255), each entry is a permutation of the integers 0 to 255, with the permutation being a function of the variable length key. Two counters are used in this approach. In an 8 * 8 S-Box (S0 S255), each entry is a permutation of the integers 0 to 255, with the permutation being a function of the variable length key. The approach employs two counters, I and j, which are both set to zero.

The method uses a configurable length key ranging from 1 to 256 bytes to create a 256-byte state table. After that, the state table is utilized to generate pseudo random bytes and a pseudo-random stream, which is then XORed with the plaintext to generate the cypher text. At least once, each state table element is swapped.

.

VI. CONCLUSIONS

The most important component of a website is the web server. Any unauthorized access to the server renders all of the server's data available to the public. We used a novel method in this research. Some sensitive information will be hidden via an encryption procedure. By storing it on the server, you've added an extra layer of protection. Regardless of the system, the client ID (bank) has been encrypted here. An online banking system's account number and user name. The RC4 technique is used to achieve this. No one will be barred from taking part. By figuring out the encryption key, they'd be able to decipher the data. You will never be permitted to remain in the system. The administrator has access to this data. There will be no one who is barred from taking part. By determining the encryption key, they would be able to decipher the data. The administrator has access to this information. However, I am unable to remove any user's general information. Any user's transaction data is accessible.

VII. RESULT

In this paper, we present a way for designing a safe web server for online banking systems utilizing the RC4 algorithm. We've implemented a safe money transaction method in this system by inserting a secrete key into each transaction conducted by the client or user. Only the legitimate client or authorized user has access to his data. 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.

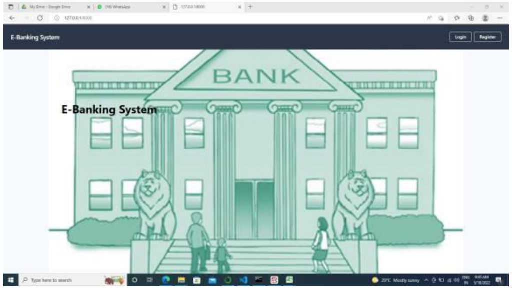
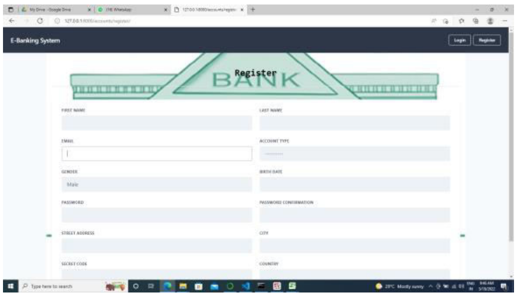


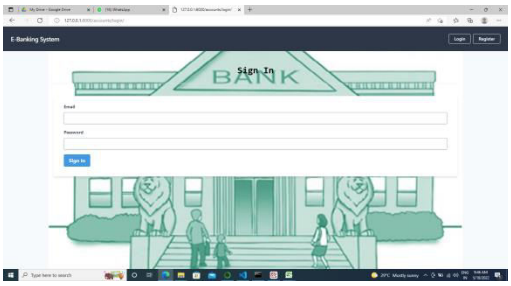
Fig 2 Main Page



Register

FIRST NAME
LAST NAME
EMAIL
ACCOUNT TYPE
GENDER: Male
BIRTH DATE
PASSWORD
PASSWORD CONFIRMATION
STREET ADDRESS
CITY
SECRET CODE
COUNTRY

Fig 3 Registration

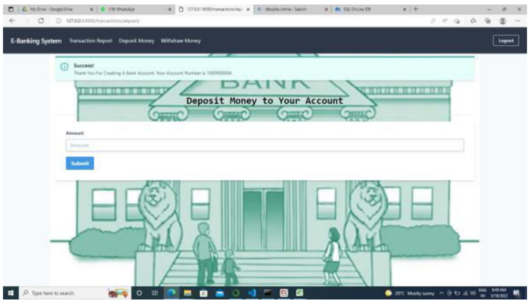


Sign In

Email

Password

Fig 4 Sign in

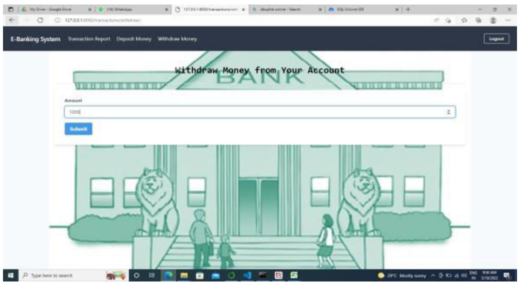


Success!
Thank You For Creating A Bank Account. Your Account Number is 1000000004.

Deposit Money to Your Account

Amount: Amount

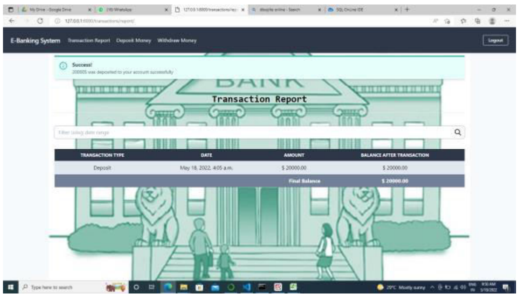
Fig 5 Deposit Money



Withdraw Money from Your Account

Amount: 1000

Fig 7 Withdrawn Money



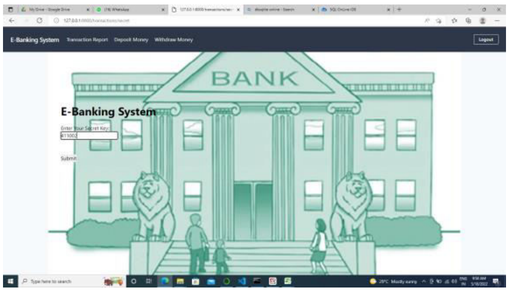
Success!
20000$ was deposited to your account successfully

Transaction Report

Filter using date range

TRANSACTION TYPE	DATE	AMOUNT	BALANCE AFTER TRANSACTION
Deposit	May 18, 2022, 4:05 a.m.	$ 20000.00	$ 20000.00
		Final Balance	$ 20000.00

Fig 8 Transaction Report



E-Banking System

Enter Your Secret Key: 811002

Fig 9 Secrete Key

REFERENCES

1.]Orvila Sarker ,Mehedi Hasan, N. M. Istiak Chowdhury.A Secure Web Server
for E-Banking 2018 21st International Conference of Computer and Informa_x0002_tion Technology (ICCIT), 21-23 December, 2018

2.] Hao Wenning Zhang Hongjun He Dengchao Chen Gang Zhao Shuining
Design and Implementation of Database Encrypting Middleware 2012 Inter_x0002_national Conference on Computer Science and Service System

3.]Jayakrishnan Ashok, K. N. Dheeraj, Chaitanya Subhedar, Rajeev Tiwari Homomorphic Encryption over Databases International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8, June 2019

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details