WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

E-Banking Log System

Mayur Chaudhari*[1], George Abraham[2], Akansha Sawant[3], Aditi Raut[4]

8th Semester, Department of Computer Engineering St. John College of Engineering,Palghar, Mumbai University of Technology Mumbai, India
Corresponding Author Email :mayur1998c@gmail.com

ABSTRACT

The E-Banking Log System software overcomes the issue that the online banking was facing. It uses geographical location of the user and keeps a track of the transaction activity. An algorithm is created which helps in finding patterns in transaction activities. Algorithm is trained to give a positive and negative response to the patterns generated. It gets a negative response if current transaction activity is different from all the previous transactions. The system blocks the user and informs the bank regarding the transaction made. The user's money in the bank is also kept safe from malicious hackers. Virtual account is created along with the user's account. The virtual account has a default money that the banks fix. When any transaction is made by the user an OTP is generated to the registered mobile number. If the OTP entered is wrong, the money will be deducted from the virtual account keeping user's main balance safe. Then this transaction is reported for further investigation. If the OTP entered is correct then the money is deducted from the main balance. This system contains features like checking for authenticated websites, blocking a particular website and blacklisting unnecessary words. Security risks have constantly increased over a few years or even decades. Preventive measures are not taken to the mark. Banks have been constantly avoiding to stop those risks. This system works on the issues and risks the online banks face and also some remedies to overcome those issues. People do not trust online banks or E-Banks due to the risks. To improve E-banking, preventive measures need to be taken. Security measures need to be focused. This system uses algorithms to secure the transactions and help people feel safe of their money.

Keywords— Bank, Security, OTP, Transaction, Virtual, Privacy

1 .INTRODUCTION

E-Banking is the widely used method in today's world. The security risks that are caused by attacks on the e-Banking systems has also increased. The consequences of attacks can be serious and most of the banks have been avoiding the risks. A confidentiality, integrity, and availability has to be maintained to keep trust of the customer. This paper discusses the security risks of E-Banking systems and the possible ways to prevent such attacks like extracting the data from the customers and from the bank. This paper will focus on the prevention aspects of the attacks by analyzing their effects.For E-Banking to be improved globally, it must be improved in terms of security and privacy.This project refers to important issues regarding how to enhance the online transactions to more secure using SPAM algorithm in the financial sector. The conventional algorithms to offer intensification secure techniques for e- banking transaction with highest performance of SPAM algorithm. This system consists of a Phishing technique, which refers to the act that the attacker allure users to visit a faked Web site by sending them faked e-mails (or instant messages), and cautiously get user's personal information such as his name, password, etc.

LITERATURE REVIEW

Improved E-Banking System with advanced encryption standard and security model [1], refers to the security measures that is needed to be takenfor E-Banking. People and many businesses run online and the transaction is done online. Online banking not only benefits the sellers but also the consumers. But people do not feel safe to have an online transaction or use E-banking. Malicious hackers turn a lot of money into their pocket illegally by breaking the security of E-Banking. To make E-Banking trustworthy people, security needs to be improvised than before.

E-Banking Challenges and Issues [2], refers to the fear that people have in their minds in respect of E-Banking. People often have fear of losing their money due to the news they hear about the online thefts. People have stopped using E-Banking due to this fear. In accordance to this paper, some helpful thoughts are discussed to overcome the issues and the fear of common people. Things like blocking malicious websites, phishing websites can be helpful to overcome security issues.

From this research paper [3], the system can be made powerful by using an algorithm that keeps a log of the location history of transactions and also the transaction activity. By keeping logs of this information, system can detect unusual pattern and can alert the people or the bank thus providing the security.

PROPOSED SYSTEM

This system is designed to provide security in E-Banking by keeping safe the user's money. In this system, the admin can add users exclusively by taking into account the physical information provided to him by the users at the time of registration. After adding a user, an email is sent containing an id and password for logging in the user's portal. The user can then log in using that Id and password. When he logs in, an OTP is sent to the registered number as a two-factor authentication. After entering OTP, he is now able for transactions. User has a main balance as well as a virtual balance. When a user performs a transaction, location is uploaded in the log. And also, an OTP is sent to the registered number. If OTP entered is correct, the transaction is successful and the main balance is deducted accordingly. If the OTP entered is wrong, then the virtual balance is deducted causing no harm to the main balance of the user. Thus, ensuring that the user's money is kept safe. Then this failed transaction is sent for further investigation to the bank or the police. The user can view transaction history in the portal. User can also check for malicious websites and also for phishing websites by just entering the URL's in the search area. These are the additional features provided to the user in this system.

System Architecture

Users can transact from their accounts and also can view balance. The money transfer option is also available for the user where they can transfer their money to any other account. There are a number of users who purchase products online and make payments through online means. There are some E-banking websites that ask the user to provide sensitive data like credit card detailsfor malicious reasons.This type of phishing websiteis intelligent and an effective system using the classification data mining algorithm should be built to prevent them.

The classification algorithm and techniques used to extract the accessible data sets criteria to classify their content. The phishing websites can be detected by specific aspects like URL.

Ifany user makes online transactions through thisE-Banking website the system will use a data mining algorithm to detect phishing websites. This application can be used by many enterprises, web marketing payment sitsin order to make the whole transaction process secure. The data mining algorithm used in this system provides better performance as compared to another traditional classification algorithm. With the help of this system, the user can purchase products online without any hesitation. The architecture of the proposed system in given in fig 1.

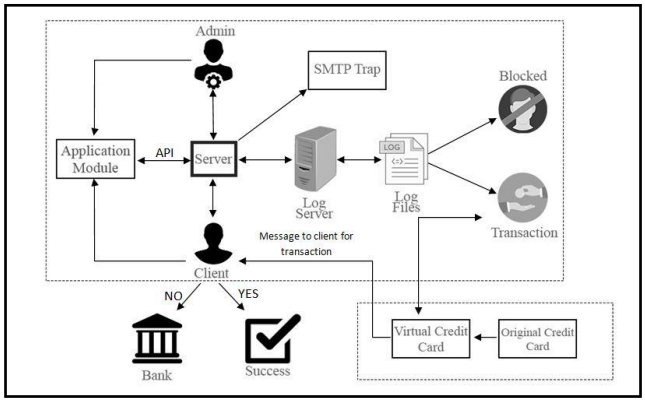

Fig 1: System Architecture

RESULTS AND IMPLEMENTATION

Login Page

The above snapshot shown in fig 2 is the first step of interaction. The admin uses admin login page to go into admin's portal.

Fig 2: Login Page

Viewing Users' Information

The admin in his portal can perform various actions as shown in fig 3. One of such actions is viewing the existing users in E-banking System. Admin can view the entire history of the user.

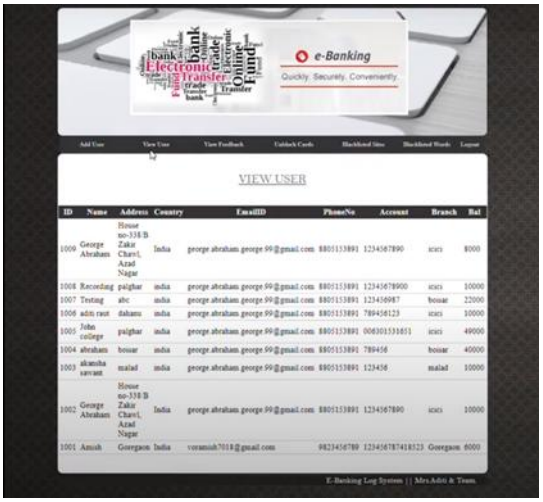

Fig 3: Viewing Users' Information

Adding user Data

User details are added by the admin as shown in the Fig-4. The details are entered manually. Card details are also recorded in the database as shown in Fig-5.

Fig 4: Adding User's Data

Fig 5: Adding User's Card Data

Gmail Verification

When a user is added, the user is assigned with an Id and a password to login into customer's portal as shown in fig 6. The credentials are E-mailed to the user to his registered email Id. This ensures security for the user portal.

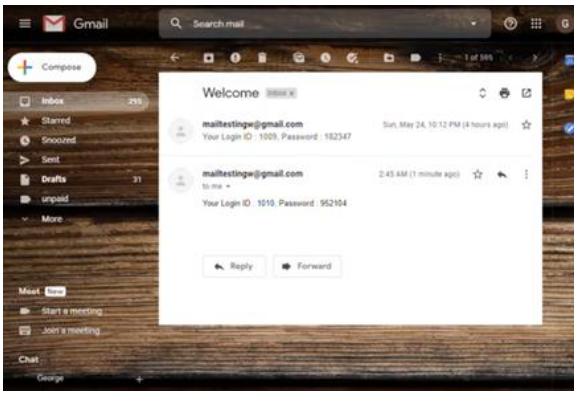

Fig 6: Gmail Verification

Customer Login and OTP

When the user enters his credentials that he received through email, he also receives an OTP to his registered phone number for authentication purpose as shown in Fig-7& 8. After successfully entering OTP, he is then transferred to the next page.

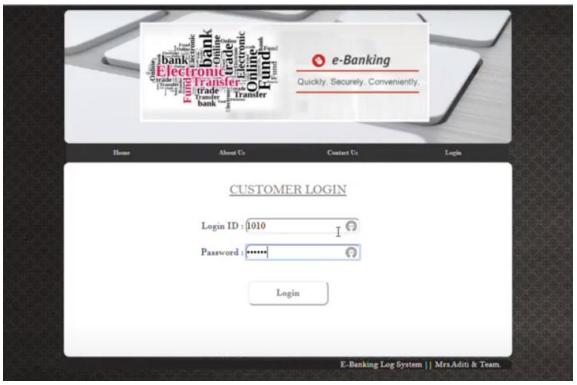

Fig 7: Customer Login

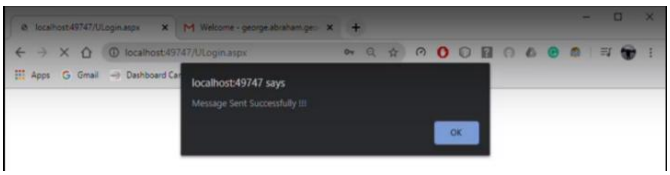

Fig 8: Message Sent Successfully

Virtual money Concept

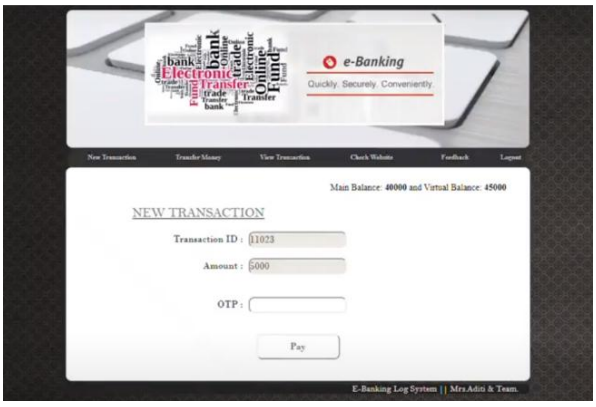

Fig 9: Virtual Bank

As from the above Fig-9, the virtual balance is deducted and no harm is done to the main balance. The OTP is required for transaction to complete. If the OTP entered is correct, the main balance will be deducted and the virtual balance will be restored back to normal again as shown in Fig-10 and Fig-11.

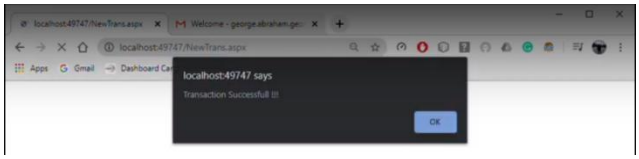

Fig 10: Transaction Successful

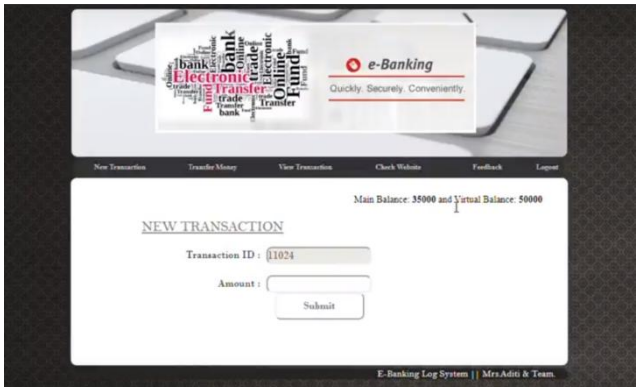

Fig 11: Virtual Balance Restored

Viewing transaction

The user can view the transaction history to keep a track of his activity or any suspicious activity as shown in fig 12.

Fig 12: Virtual Balance Restored

CONCLUSION

E-Banking threats has become a serious problem in this modern world. In this pandemic attack of Corona, people need to use E-Banking for daily essentials. But people fear of the online thefts and fear of losing money in this financial crisis. It is necessary to remove the fear by providing proper measure against thefts. E-Banking Log System is the perfect system that people need. It not only helps people to transfer money with ease but also fearlessly. Although there may be some drawbacks which can be improved in the future by introducing new techniques which are more securethen traditional once.

REFERENCES

[1]. M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, EUROCRYPT, Springer, 1995.
[2]. Ben-Aroya "Differential Cryptanalysis of Lucifer", CRYPTO, Journal of Cryptology, Springer, 1996.
[3]. D. Wagner, “The Boomerang Attack, Fast Software Encryption”,Fast Software Encryption, Springer, 1999.

[4] P. C. Van Oorschot, Mohammad Mannan, "Security and Usability: The Gap in Real-World Online Banking", 2007.
[5]Sang-Gon Lee, Sang-Il Cho, Hyo-Taek Lim, , "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October, 2009.
[6] Jean-Daniel, "Smart Cards and Digital Identitification", Telektronikk. 2007.
[7] Ashok Bahadur Singh,"Mobile banking based money order for India Post:", International conference on emerging economies-Prospects and challenges (2012)
[8]Yoon,Jeong, B. K., "An Empirical Investigation on Consumer Acceptance of Mobile Banking Services and Technology", Business and Management Research, (2013)
[9] Ravinder Kumar Sehgal,] Rajpreet Kaur Jassal1" Study of Online Banking Security Mechanism in India , IOSR journal of computer engineering,(2014).