International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 10, pp 107-109, October-2022

https://doi.org/10.47001/IRJIET/2022.610017

Preventive Measures to Control Cyber Crime Affecting Banking and Online Transactions

[1]Prof. Sunita Totade, [2]Priya Deshmukh, [3]Sonal Gawai, [4]Snehal Chatur

[1]HOD, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India
[2,3,4]Student, Department of MCA, Vidyabharati Mahavidyalaya, Amravati, India
Authors E-mail: [2]priyajdeshmukh@gmail.com, [3]gawaisonal144@gmail.com, [4]chatursnehal111@gmail.com

***Abstract* - Researcher has given some suggestions for the prevention of cybercrime related to online banking are on the rise. The purpose of this research paper is to control cyber attacks. The misuse of information technology in the cyber space is clutching up which gave birth to cyber crimes at the national and international level. The percentage of risks and the challenges associated with it is increased. Online and mobile banking is never 100 per cent safe. In this paper we focused on how to prevent the cyber crime. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber crime. To tackle the rising bank scams at ATMs, the lender has come up with a set of rules, one of which requires a two-step verification in order to protect debit and credit cardholders of the bank. In the Internet banking site, click the SMS Alerts link in the Requests tab. You are displayed a list of your accounts. Select the account for which you wish to enable SMS alerts and click OK. Select the events for which you wish to receive alerts. When profile password of internet banking is utilized the bank will report the customer via sms, this action control phishing attacks. Use of Strong Encryption and Decryption method, personal firewall, anti-spyware program, effective and updated anti-virus software keep control over cyber crime. DoS (Denial of Service) occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.**

Keywords: Cyber threats, cyber security, OTP, Block chain.

I. INTRODUCTION

i) Aim

In our research paper we are given some ways to overcome cyber crime during online Transactions. Theses ways are two-step or three-step verification during online transaction. OTP Encryption technique, Biometric payment technology. Use of Block chain is a technology so no one can edit the transaction record so it will help to avoid cyber crime.

ii) Objectives

1. Recommendation to Prevent Cyber Crime.
2. Solutions to the threat of cyber security in digital banking.

iii) Application

1. Extracting encrypted text from the Stego-image is Alternative to SMS OTP.
2. Blockchain technology used in Bitcoin crypto currency.

iv) Scope and Advantages

1. The SBI customer, who wishes to draw an amount of more than Rs. 10,000 will have to enter the four digits OTP along with his or her debit card PIN number while making the transaction. This gives an extra layer of security thereby preventing ATM scams. Using same technique, In future we can develop two-step or three-step verification.
2. When profile password of internet banking is utilized the bank will report the customer via sms, if we are not the ultimate user then you should report the bank to block the fraudulent transactions.
3. Use of Biometric payment technology in all the transaction that uses biometric authentication based on physical characteristics to identify the user.
4. Restrictions on transaction to a certain limit.

II.METHODOLOGY

i) Data protected technology adoption

Block chain is a technology that was initially developed for Bitcoin, the crypto currency. Block chain could reduce banks infrastructure costs by US$ 15-20 billion per annum by 2022. Block chain have the potential to transform how the business and the government work in vast variety of contexts.

ii) Cyber Fraud Council in Banks

Whenever a cyber-fraud is committed the victim should report to the Cyber Fraud Council that must be set up by in

ISSN (online): 2581-3048
Volume 6, Issue 10, pp 107-109, October-2022
https://doi.org/10.47001/IRJIET/2022.610017

each and every bank to review, monitor investigate and report about cyber-crime. In case, such Council does not take perform or refuses to perform its duty then a provision to file an FIR must be made. The matter to be brought before such council can be of any value. However, when the value is high then the Council shall act expeditiously. RBI in its 2011 Report stated that when bank frauds are of less than one Crore then it may not be necessary to call for the attention of the Special Committee Board.

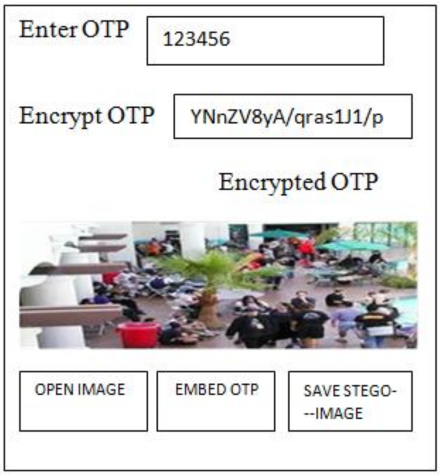
iii) Education to Customer

The customer should be educated and made aware about various bank frauds and measures should be informed to them for safety mechanisms so that they do not fall prey as victims of cyber- crime. If a customer is conscious and report the matter of cyber-crime then in the initial stage also instances of cyber-crimes can be reduced. A customer should be made aware about the Dos and Don'ts' of E-banking. It can be done through publishing it on the bank's website, publishing in the newspaper, through advertisements, by sending SMS alerts, through poster education etc. In case a bank introduce any new policy or there are any changes which are required to be followed by all banks as per RBI then, bank must inform the customer through mails or by informing the customer through telephone. The awareness material should be timely updated keeping in mind the changes in the legislation and guidelines of RBI.

iv) System for Safeguarding OTP

By sending OTP to the intended user through email will protect it from criminals who try to gain the same by attacking SMS through all possible ways. The user will be provided with an application as shown in Figure which helps in extracting encrypted text from the Stego-image. After getting the text, an OTP retrieval application has to be used by the user to decrypt the OTP. The key for decrypting OTP is ATM pin along with last four digits of user's Credit/Debit card number and his Date of Birth in DDMMYYYY format which all is available with every user. Also this number is unique for each user. The application will help in retrieving One Time Password within seconds of time. The reason for this is that, the banking system will be producing one time password using time synchronization mechanism because of which every OTP.

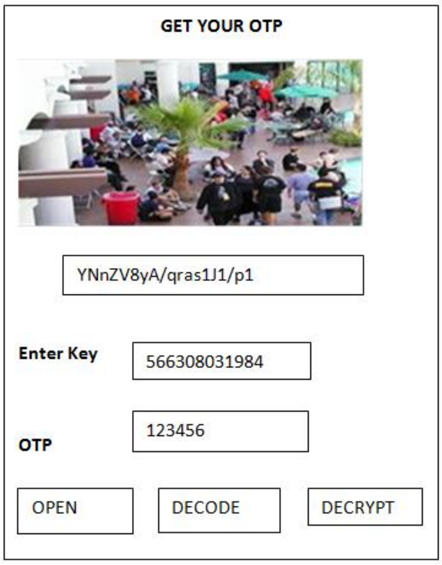
The OTP needs to be generated using time synchronized mechanism. This ensures that the generated OTP is unique and valid for a very short period of time. The generated OTP is then encrypted using AES encryption algorithm [1]. AES, a cryptographic algorithm is normally used to protect electronic data. AES which is the successor to the older Data Encryption Standard (DES) has become the standard for encrypting all private and electronic data. Also the time required to crack 128-bit AES key using brute force attack is approximately 1 billion years.



Enter OTP 123456

Encrypt OTP YNnZV8yA/qras1J1/p

Encrypted OTP



GET YOUR OTP

YNnZV8yA/qras1J1/p1

Enter Key 566308031984

OTP 123456

Stego image is the output of embedding process

v) Use a personal firewall

It is a minor program that assistances to protect your workstation and its contents from unknowns on the internet. When mounted and properly and configured, it stops unauthorized traffic to and from your workstation. There are many effective plans to choose from. Common viable examples include Check Point Zone Alarm (free) and Windows Firewall, Norton Personal Firewall and McAfee Personal Firewall.

vi) Always log off

Always remember to log off from banking site and close your browser after completion of your online banking. This will remove all traces of your stopover from the workstation's memory.

vii) Keep your passwords secure

Keep your password to yourself only, Make them hard to guess, differ them: Try to use unlike passwords for different services, Change your passwords frequently and never write them down.

viii) Beware of fake calls

Don’t leak your banking credentials.

III. CONCLUSION

Information Technology has become the backbone of the banking system.. The growth in cyber-crime and complexity of its investigation procedure requires appropriate measures to be adopted. According to National Crime Records Bureau it was found that there has been a huge increase in the number of cyber-crimes in India in past three years. Indian banking sector has carried out all their banking activities through electronic medium as the study suggest that there has been an increase in the number of payments in online banking. However, the change in the banking industry must be such which suits the Indian market. The only propitious step is ‘to create awareness among people about their rights and duties and to further making the implementation of the laws more firm and stringent to check crime’. In our study we have found that different technologies have played an important role to control the risk factors through Authentication system.

REFERENCES

[1] Cyber security attacks in banking sector: Emerging security challenges and threats. Available on at http://www.iasir.net

[2] A Study on Cyber Security Issue Affecting Banking and Online Transactions.

[3] https://www.ijert.org/research/sms-based-one-time-password-vulnerabilities-and-safeguarding-otp-over-network-IJERTV3IS051538

[4] https://www.hsbc.com/internet-banking/types-of-online-attack

[5] http://en.wikipedia.org/wiki/Internet_safety

[6] “Online Banking Quick Reference User Guide” Community Banks of Colorado, N.A. Rev. 05/12.

[7] “One-Time Password Service Using Mobile Phone Applied to Personal Internet Banking for the First Time in Japan” NTT data corporation, June 18, 2007.

Citation of this Article:

Prof. Sunita Totade, Priya Deshmukh, Sonal Gawai, Snehal Chatur, “Preventive Measures to Control Cyber Crime Affecting Banking and Online Transactions” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 10, pp 107-109, October 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.610017

****