BLOCKCHAIN: A PANACEA FOR CYBER-CRIME IN BANKING

U. Padmavathi[1], U. Sakthivelu[2] and K. Lakshmi Narayanan[3]

[1]Assistant Professor, Department of AI & DS, School of Computers, Madanapalle Institute of Technology & Science, Andhra Pradesh

[2,3]Research Scholar, Department of Computer Science & Engineering, SRM Institute of Technology and Science, Kattankulathur, Chennai

ABSTRACT

The term cybercrime is defined as an illegal activity in which the cybercriminals make use of computer and internet as a medium to invade into the financial account of users without their authorization with a motive to harm them. Cybercrime could otherwise be called as computer-oriented crime, since it involves computer and network to carry out the criminal activity. This growing threat mainly targets the banking sector in which the accounts of users stand as the prey for these attackers. This paper first gives an overview of cybercrime and then envisions the various statistical reports on cybercriminal activity. It also elaborates the various ways by which the cybercriminal activity is carried out in banking sector. Finally the paper concludes that Blockchain could be a panacea for all the problems caused by the cybercriminals in banking sector.

Keywords: *cybercrime, banking, cybercriminals, smishing, vishing, blockchain*

INTRODUCTION

In the recent years, the rapid digitalization and proliferation of mobile data paves way for cybercrime all over the world. The term cybercrime is defined as "offence that are committed against individual or group of individuals with a motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss to the victim directly or indirectly, using modern telecommunication networks such as internet and mobile phone" [1].

With the help of computer and internet, the cybercriminals are able to carry out this cybercrime activity in almost every field. The main target of cybercrime is finance. Other targets include e-mail fraud, identity theft, ransomware attacks, viruses, credit card fraud, and internet fraud and so on [2]. Cybercriminal must possess a little technical skill or he might be an expertise to carry out the cybercriminal activity. Usually, this kind of activities is carried out from countries with weak or nonexistent cybercrime laws.

In India, Banks are the critical players in contributing to the economic development of the country. Banks are called the backbone of Indian economy. In the recent past, banking frauds have evolved ranging from

technology frauds to hi profile loan frauds. At present, India stands in the third position in terms of cybercrime activities. Generally, cybercrimes are classified as cyber-deceptions, cyber-pornography, cyber-violence, and cyber-trespass. Banking frauds belong to cyber-deception [3]. In banking sector, cybercrime could either take place in a direct manner or in an indirect manner. The following table 1 shows the various direct and indirect methods used by the hackers to carry out the cyber crime in banking sector.

Table 1: Types of Cyber Crime in Banking

Cybercrime in banking	**Direct**	Credit card fraud Debit card fraud Money mule Internet & banking fraud Smishing Vishing
	Indirect	Phishing Pharming Hacking Viruses Spam Malware Simswap Trojan

Although several methods exist to carry out the cyber crime in banking, this paper focuses on smishing, vishing, phishing, money mule, Trojan and SimSwap which are the popular methods to perform cyber crime in banking sector.

Methods to Carry Out Cyber Crime in Banking Sector

Smishing

Smishing or SMS phishing is a type of security attack carried out using mobile phone text message [4]. In this social engineering attack, the recipients are deceived to download a trojan horse virus or other malware into their phone or they are made to call back on a fraudulent number or visit fraudulent websites. This attack is carried out in order to steal data about the user including his personal information, financial information, credentials such as username and password. The motive of this attack is money laundering. In this attack, the attackers send a message containing a malicious link to the victim's mobile number. When the victim opens the message and clicks the malicious link, he will be re-directed to a phishing website

page, where all the information including the user name and password about the victim is obtained.

Vishing

Vishing also known as voice phishing is a type of cybercrime in which the attackers makes use of automated voice recordings to steal personal information like customer user name, password for net banking, credit card information such as ATM Pin number, OTP, CVV, card expiry date etc., In this attack, an automated voice call is made to the victim stating that his account has been compromised [5]. It then asks the victim to make a call to specified toll-free number where the user's personal information such as his bank details are harvested.

Phishing

Phishing is a type of fraudulent attempt carried out by email spoofing or instant messaging. It aims to gain personal information of users such as customer ID, credit card number, debit card number, CVV, card expiry date, Net banking user name and password. It sometimes target online auction sites, e-commerce sites or other online payment sites. This type of criminal activity is carried out by sending phishing email to the victim, asking him to follow a link to a phishing website that looks like a legitimate site. In this email, the victim is asked to update his bank account details such as username and password. When the user clicks the link and updates his account details, the phishing website captures all the details about the victim and sends these details to the third-party website. In this attack, the fraudsters who created the phishing website act as bakers and ask the user to update all his banking information [6]. After getting the necessary information from the victim, the attackers start transferring all the funds from the victims account to their accounts without the knowledge of the victims. Phishing can be spear phishing, whaling or clone phishing type.

Money Mule

It is a type of cybercrime in which the victims are duped by fraudsters for the purpose of laundering illegal money through victim's bank accounts. Money mule is otherwise called as smurfer in which a person transfers illegally acquired money through courier service or through other user's accounts. Money mules are recruited and they are paid for the services they provide and sometimes money mules do not know that they are indulged in transferring illegally obtained money through various bank accounts [7]. Money mules are usually recruited online and they are employed to transfer money, which they do unwittingly or unknowingly thinking that they are employed legitimately. The money is transferred from the mule's account to the scam operator, typically in another country. When this kind of activity is reported to the police, then the smurfer becomes the target of police investigations, due to their involvement in transferring money.

Trojan

It is a harmful software code that appears to be a legitimate code when downloaded and installed into the computer will start to steal personal information from the computer or will delete files on the computer. Trojan codes are designed to steal sensitive information of the victim including login credentials, Account number, financial information and credit card information .

There are different types of Trojan. Each Trojan attacks using different methods. In recent years, banking Trojans are on the rise. Banking Trojans are special kind of malicious software programs, when installed on the victim machine; these Trojans inject botnet, steal credentials and money from the victim account using various techniques [8]. Banking Trojans are pervasive and they try to make more money for the attackers by stealing sensitive credentials from various users' accounts. A recent report by checkpoint stated that banking Trojans have been on the rise by a massive 50%. The following table 2 shows some of the notable banking Trojans.

Table 2: Types of banking trojan

S.No	Banking Trojan
1	Zeus
2	Gozi
3	GozNym
4	Caberp
5	SpyEye
6	Shylock
7	Citadel
8	Tinba
9	Vawtrak
10	Emotet

Sim Swap

It is a type of cybercrime in banking sector in which the fraudsters are able to get a new SIM card issued against the user's registered mobile number [9]. They get this SIM card from the Mobile Service Provider by some means. Using this new SIM card, the attacker is able to get the One Time Password (OTP) and other alerts that are sent to the user mobile for verification purposes at the time of making financial transactions through the bank account. After getting access to the OTP and other information, the hacker is able to move funds from the victims account to his own account.

 ISSN-2581-8953

Recent Reports on Cybercrime

1. Group-1B expert evaluations states that almost 99% of all cybercrimes in the world now involve money theft.
2. In 2013-2014, the number of cyber frauds reported by Reserve Bank of India (RBI) is around 9500.
3. In 2014-2015, RBI stated that the number of cyber frauds in the banking sector is 13,083.
4. The number of cyber frauds in the fiscal year 2015-2016 is 16,468 as per the report of RBI.
5. In the fiscal year 2016-2017, according to the RBI report the number of cyber crime in the banking sector is 28,823.
6. The number of cyber frauds reported by RBI in the year 2017-2018 is 37,743.
7. In 2018-2019 fiscal years, around 50,000 cyber frauds in the country's Scheduled Commercial Banks (SCB) were discovered by RBI.
8. RBI stated that the losses incurred due to the banking fraud in the fiscal year 2018-2019 are Rs. 67,432.26 Crores. More than 4269 frauds occurred due to insiders in the banks.
9. RBI reported that in the financial year 2019 – 2020, about 84,000 bank fraud cases causing a loss of 1,85, 772.42 crores.
10. The fiscal year 2020-2021 saw a slight decrease in the number of fraud cases reaching about 83,585 causing a loss of 1.38 lakh crores. This was due to the pandemic situation prevailed throughout the world.
11. According to an RBI report, the financial year 2021-2022 saw about 91,000 bank fraud cases causing a loss of 60,414 crores. The following Fig. 1 shows the growth of cyber frauds in the banking sector from the financial year 2013 to 2019.

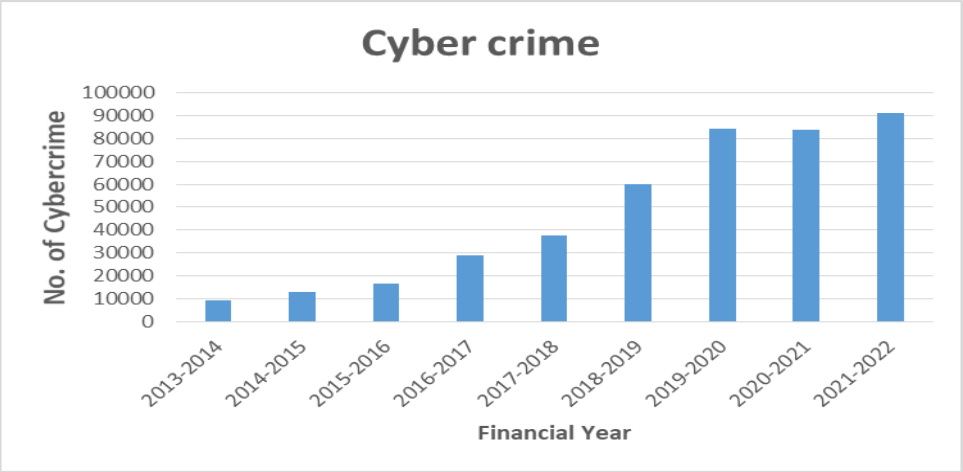

Fig 1. Increase in Cyber crime in banking sector [10-13]

Blockchain: the Panacea?

The term Blockchain refers to a decentralized, distributed ledger technology in which the data are stored as records in an immutable and efficient manner. Blockchain could simply be defined as the "chain of blocks" linked to each other. Each block is linked to the previous block using the cryptographic hash value and each block contains block header and block body. The block header contains the information about the block such as the version, timestamp, difficulty, nonce, merkle root and the previous hash value [14]. The block body contains a number of transactions. The figure below shows the structure of blockchain. Fig. 2 shows the structure of Blockchain.

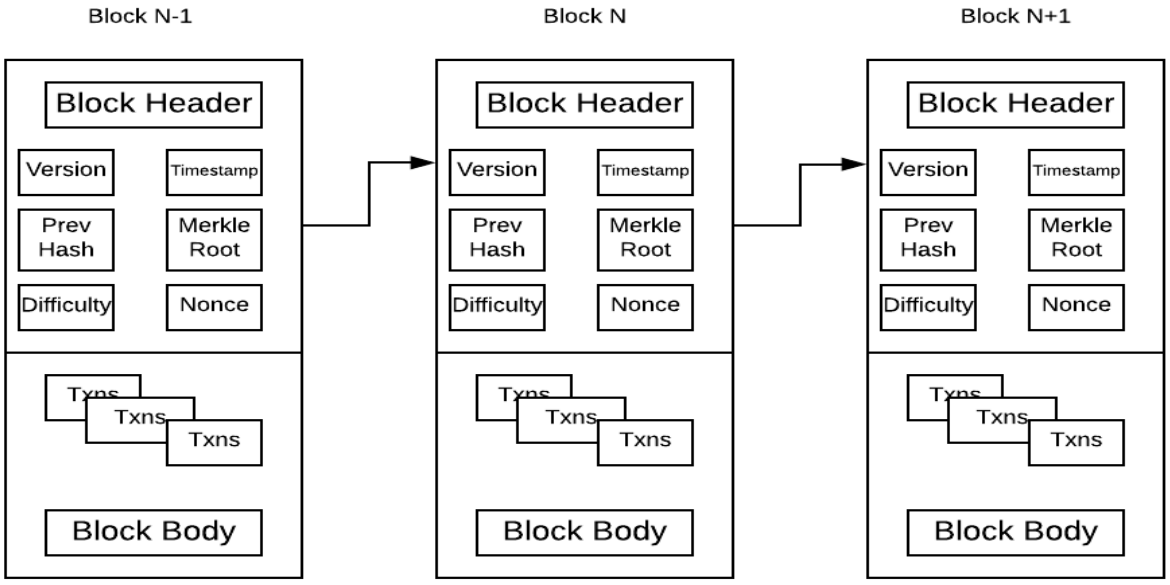

Fig 2. Structure of Blockchain

Blockchain technology is born with the concept of Bitcoin, the digital cryptocurrencies introduced by Satoshi Nakamoto in the year 2009 [15]. Initially, this technology finds its growth in the financial sector. Later, it invades into other application areas such as healthcare, education, governance, manufacturing, insurance and so on.

Some of the highlighting features of blockchain are

1. Immutability
2. Security
3. Confidentiality
4. Integrity
5. Privacy
6. Efficiency

Blockchain has the capability to store data in a tamper-proof manner. That is, the data stored in the blockchain cannot be altered or deleted. The data can only be appended to the blockchain. There are three types of blockchain [16]:

1. Public blockchain – anyone can be the member and anyone can view the transactions.
2. Private blockchain – only a particular organization have control over the blockchain.
3. Consortium blockchain – this type of blockchain is developed for applications where more than one organisation needs to get involved.

Consortium blockchain can be helpful to solve the issues associated with the banking sector. Once the banks start using blockchain for storing their data, no hacker would be able to change or alter the data as well as the user credentials when stored using this blockchain technology could never become prey for the fraudsters.

CONCLUSION

Banking sector, the real backbone of Indian economy suffers from cyber crime. According to the RBI report, every year the number of cyber crimes is found to be increasing and the action taken against these cyber crimes is not found to be fruitful. It is found that, Blockchain a tamper-proof ledger technology could be a panacea for all the problems faced by banking sector. Various researches done on blockchain technology prove that it is immutable and has the capability to stand against various types of attacks. Thus, it is concluded that Consortium blockchain could be the correct solution for the banking sector to fight against cybercriminal activity.

REFERENCES

1. https://www.bbau.ac.in/dept/Law/TM/1.pdf
2. https://www.techtarget.com/searchsecurity/definition/cybercrime
3. https://www.clearias.com/cybercrime/
4. https://www.trendmicro.com/en_us/what-is/phishing/smishing.html#:~:text=Smishing%20is%20a%20form%20of,attack%20the%20name%20%E2%80%9CSMiShing.%E2%80%9D
5. https://terranovasecurity.com/what-is-vishing/
6. https://www.imperva.com/learn/application-security/phishing-attack-scam/
7. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules
8. https://heimdalsecurity.com/blog/banking-malware-trojans/

9. https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html
10. https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/
11. https://economictimes.indiatimes.com/industry/banking/finance/banking/about-84545-bank-fraud-cases-reported-during-2019-2020-says-rbi-in-reply-to-rti/articleshow/77200022.cms
12. https://www.business-standard.com/article/finance/frauds-reported-at-banks-financial-institutions-decreased-in-2020-21-rbi-121052700748_1.html
13. https://www.indiatoday.in/business/story/229-banking-frauds-day-2020-21-recovery-rate-rbi-rti-reply-1888096-2021-12-15
14. https://www.ibm.com/in-en/topics/what-is-blockchain
15. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.”
16. https://www.oracle.com/middleeast/blockchain/what-is-blockchain/