WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

The vital function of cyber security in the field of banking industry in India

[1*] Guhan.s, [2*] Falak Fathima,

3rd year BA student, IADC-A, guhananju46@gmail.com
3rd year BA student, IADC-A, falakfathima05@gmail.com

ABSTRACT :

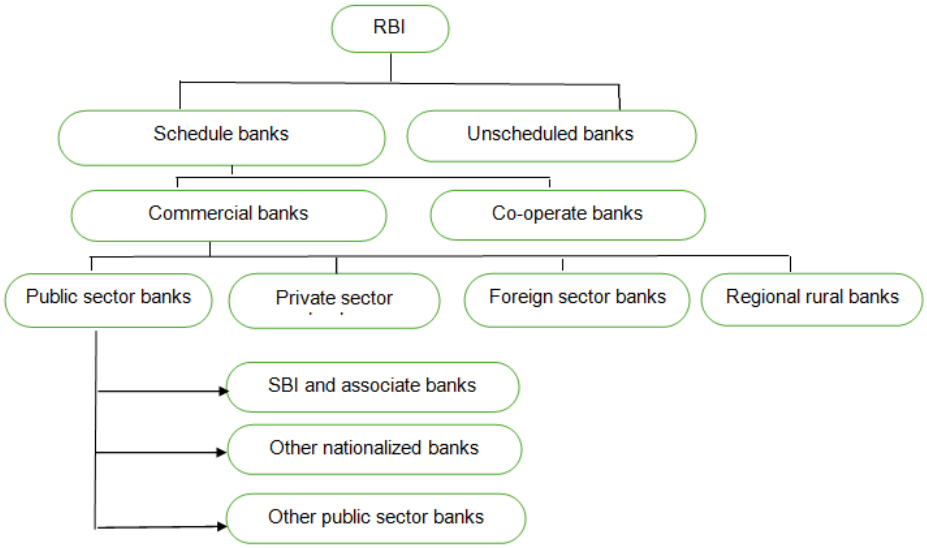
This study aims to understand the importance of cyber security in the banking sector and strategies to prevent cyber threats. The banking industry is at the front of the digital revolution, providing consumers with never-before-seen ease while also turning into a top target for cybercriminals. This paper examines the vital significance of cyber security for the banking sector, especially in India, where financial crime rates have alarmingly increased. Strong cyber security measures are critically needed, as evidenced by the nearly 13 lakh cyberattacks that were reported between January and October 2023 alone. Our study aims to analyze the complex cyber threats that the Indian public faces and clarify the critical role cyber security plays in protecting financial institutions from fraud and maintaining their integrity. We use a defined process to access a wide range of primary materials from reliable sources, such as scholarly publications, peer-reviewed journals, reliable websites, and newspapers. Using a thorough analysis, our goal is to provide a comprehensive overview of the dynamic threat environment, breaking down typical attack routes, pinpointing weak points, and clarifying new developments that influence the cyber security paradigm in the banking industry. Through assessing the advantages and disadvantages of existing approaches, our goal is to offer practical guidance that can guide the creation of stronger defenses against online attacks. In quintessence, this inquiry has not only highlighted the gravity of cyber security challenges confronted by the keeping money segment but also serves as a call to activity for partners to prioritize ventures in cutting-edge advances, vigorous conventions, and comprehensive preparing programs.

Keywords: cybersecurity, Indian banking industry, cyberattacks, and financial frauds.

1. Introduction:

In the modern world, the development of technology in the banking field has made people easily open a bank account which has made their transactions faster we can see there is a shift from cash to cashless payments so when there is innovation there is also a threat in society. The word cybercrime can be split into two words where cyber can be defined as something like the culture of computers, information technology, and AI and crime is a word that is considered offensive. Cybercrimes are committed using computers and other electronic technologies. The goal of the Information technology act 2000 is to ensure privacy , data protection and to pave the way for electronic governance in India. According to the National Cybercrime Reporting Portal (NCRP), nearly 10,319 crores of financial frauds have been reported in the FY 2023 in the same year 2537.35 crore of financial crimes were reported by the Parliamentary Standing Committee of Finance.

2. Structure of the banking sector in India



The Reserve Bank of India (RBI) is the topmost authority that regulates all the banks by fixing interest rates and provides guidelines through monetary policy. Under that, there are scheduled banks and unscheduled banks. Under the schedule banks commercial banks of 4 categories are classified through ownership :

- Public sector banks
- Private sector banks
- Foreign sector banks
- Regional sector banks

3. A review of financial fraud

Individuals or groups of people are involved in cyber crimes activities for different motives some are ransomware, DDOS attacks, phishing, insider threats, social engineering, spoofing, targeting big organizations, forgery, etc.

How citizens are affected by e-frauds :

- Online gambling
- Net banking threats
- OTP scams
- ATM crimes

Areas where banking industries witness cyber crimes :

- Automated teller machines (ATM) :
  It is an electronic device that is accessible to all the people who are holding a bank account without any human intervention. It allows consumers to withdraw money anytime. A tiny metal strip is attached to the ATM cards which contains all the confidential information of the user. 2.19 lakhs ATM ' S are existing in India currently.

- Credit cards :
  It is a card issued by financial institutions which allows the cardholder to borrow funds to purchase. The borrowed amount should be repaid deep down by a specified time with an interest rate. They are very adjustable and comfortable for purchasing and borrowing with limits. It is very important to repay the borrowed amount with an interest rate.

- Debit cards :
  These cards are almost used by everyone it is a type of plastic money or plastic cards which will allow the users to do transactions for daily needs. They can be used in ATMs to withdraw money, deposit, check balances, etc. It deducts the amount immediately when the consumer purchases goods and services with a current balance.

- Digital payments :
  When the payments are made through cellular mobiles they are faster and hassle-free for the consumers. UPI unified payment interface improved by National payments cooperation of India which allows cashless transactions. Transactions through smartphones, computers, and other electronic gadgets.

- Electronic fund transfer :
  It is a digital way to transfer money from one bank account to another bank account without cash or paper. Due to their fast transfer of money, many people are adopting digital payments in today's era. They are used for bill payments, salary, and other financial transfers.

How to prevent yourself from financial frauds :

- Educate yourself
- Verify identities
- Use strong password
- Enable two factor authentication (2FA)
- Be caution with emails
- Be aware of phone calls
- Protect your device
- Secure WIFI connection
- Check your bank statement
- Seek legal advice

4. Statement of the problem :

Money is important and plays an important role in society because it gives access to consumers to buy goods and services. All the purchases made by the consumers are tracked by the criminals via cybercrime. Improvement in technology has increased cyber fraud. The use of smartphones and internet accessibility has increased cybercrimes. Therefore the study aims to examine the problems of cybercrimes in the field of banking industries and how cyber security plays a crucial role in avoiding cyber threats.

5. Significant of the study :

The information superhighway (the internet) is an important part of human life in today's world. It also plays a vital role in trade and commerce with a lot of benefits. With the advancement of technologies, there is a rapid increase in electronic frauds also known as cybercrimes has already reached a bad stage. Cybercrime, financial frauds, and threats in the field of the banking sector in India has an immense impact on the society. This paper will be beneficial for policymakers, researchers, consumers, and banks.

6. Objectives :

- To study the cases of financial fraud in the field of commercial banks between 2014 to 2023.
- To analyze the number of amounts involved in the financial threats.
- To find out the amount retrieve by the government of India under cybersecurity.

7. Methodology :

- **Type of study**: quantitative.
- **Area of study**: It covers all the commercial banks of India.
- **Data collection**: Secondary data is used for the study. Secondary data is collected through books, articles, websites, and government records.
- **Periodicity of the study**: This study will include all the financial frauds between 2014 to 2023.

8. Review of literature

"Cybercrime in the Banking Sector "by Rao (2019) is an investigation that examines previous studies on how technology developments have affected the Indian banking industry and how cybercrimes have increased in tandem. Experts investigate how technological advancements like RTGS, ECS, NEFT, and mobile transactions have changed banking operations, increasing their efficiency but also increasing their susceptibility to cyberattacks. They can talk about how cybercrimes that target banks and other financial organizations have evolved, emphasizing how sophisticated these attacks have become. Researchers would also look at the motivations behind cybercrime, which are frequently based on monetary gain. The book would also go over the difficulties that cybercrimes present as well as the necessity of strong security measures to reduce the hazards that they bring. Given the circumstances, the evaluation would shed light on the technological elements of banking cybercrimes and make recommendations for improving security protocols to successfully counter these dangers. (Harshitha rao,2019)

A study by Jana, Khedkar, and C.E Khedkar "Importance of cyber security in banking "investigates the growth in online banking has resulted from the growing use of the internet, raising the possibility of cyberattacks. The primary reason for this is that as more transactions move online, banks are more susceptible to security breaches. For banks, cybersecurity is essential for a few reasons, including preserving their brand, reducing the time and costs associated with resolving security breaches, and protecting the enormous amounts of sensitive consumer information they store. Banks use a variety of tools, such as firewalls, antivirus software, and multi-factor authentication, to combat these threats. For further security, biometrics like fingerprint scanning are also utilized. Protecting against online crime also requires frequent security audits and educating consumers about cyber threats. Given the circumstances; banks must continue to implement strong cybersecurity measures in today's age. (Jamkhedkar and C.E Khedar , 2017)

"An Overview of Cyber security in the Digital Banking Sector "by Sekhar and Kumar provides an overview of how Online technology has become essential in several industries in the twenty-first century, including banking. Because they are so convenient, digital banking services like Phone Pay, Google Pay, and NEFT have become increasingly popular. Cybercrime in the banking industry has been on the rise, though, despite the growing popularity of Internet banking. Reports suggest that debit card, ATM, and online banking fraud account for around half of all cybercrimes. When it comes to cyberattacks, the banking industry is more vulnerable than other sectors. Investigating strategies to improve cybersecurity secure against these threats is critical to meet this dilemma. (Shekar and Kumar, 2023)

A study "Evaluation of Cyber security threats in the Banking system" by Stanikzai and Shah scrutinizes that the financial sector, including banks, insurance companies, and real estate corporations, is comparable to the engine that powers money management for individuals and enterprises. Unfortunately, fraudsters who aim to benefit from vulnerabilities frequently target these institutions. Banks are easy targets for these kinds of attacks

because they are stores of wealth and provide opportunities for theft, fraud, and extortion. Furthermore, national governments assist some hackers, giving these cyber threats additional political and ideological components. Approximately 1.2 billion adults globally hold bank accounts as of 2011, underscoring the wide range of targets. The purpose of this study is to evaluate how well-suited the present cybersecurity defences are to thwart financial crimes and protect commercial activities. It looks at previous research to find effective tactics and suggest improvements to strengthen security procedures. (Stanikzai and Shah scrutinizes, 2021)

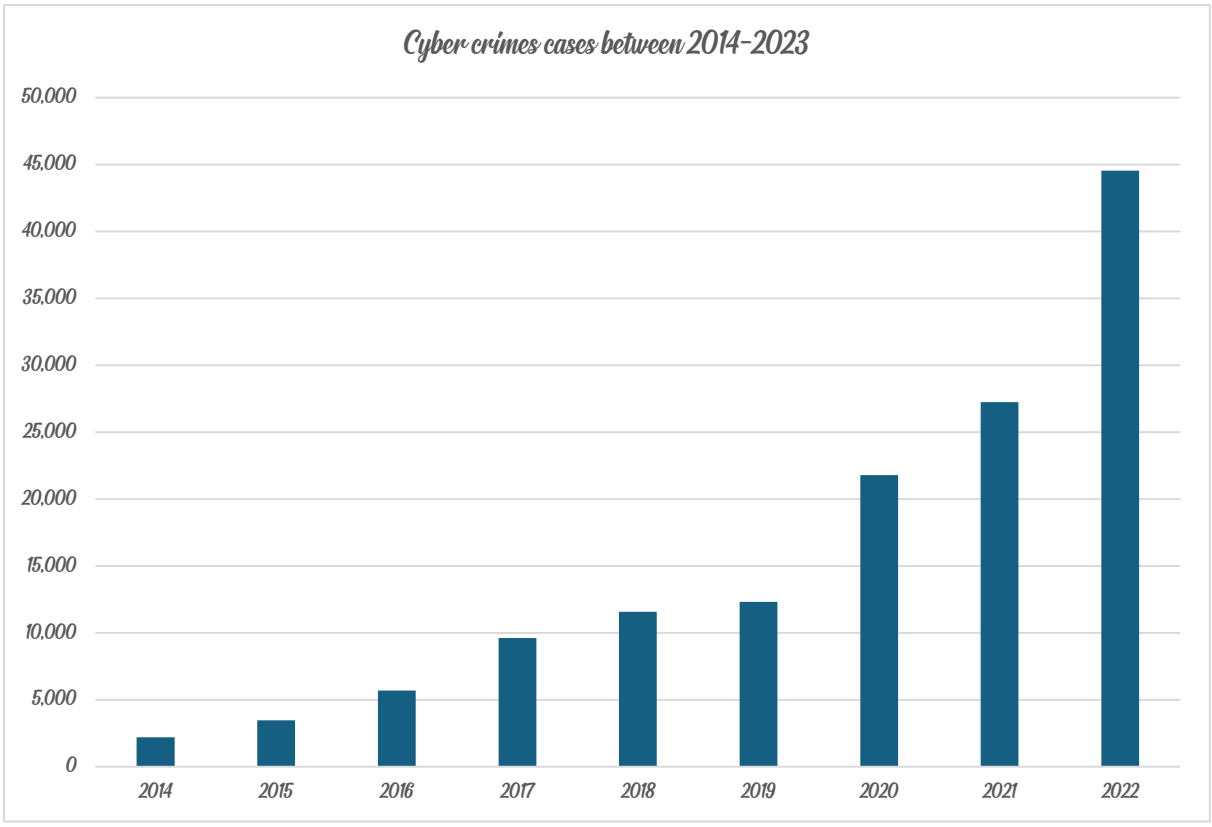
A Research by Mohammed (2015) "Cybersecurity compliance in the financial sector "examines that it is a difficult burden for legislators and regulators to manage cybersecurity in the diversified financial industry, which ranges from small local banks to large multinational enterprises. This study explores the federal and state legislation and rules about cybersecurity in the US banking industry. It compares the effects of various rules on financial institutions and breaks down compliance and regulatory issues. It examines the effects of the Dodd-Frank, Sarbanes-Oxley, and Gramm-Leach-Bliley Acts on cybersecurity procedures for both big and small organizations. It also draws attention to the increasing complexity that international companies operating in different nations with varying degrees of cybersecurity sophistication face. Through an analysis of the benefits and drawbacks of stricter compliance standards, the study clarifies how cybersecurity management is changing within the banking industry.
(Deepak Mohammed, 2015)

The paper cyber crimes in India with reference to banking sector in India by Dr. Prateeksha and Richika projects the importance of cyber security in the field of banking sector of India. It covers how financial frauds are done and how many cases have been recorded with the amount of money retrieved by the schedule commercial banks of India. The objective of this paper is to find out the total number of financial frauds and the retrieved amount by the schedule banks. It also contains statistics analysis like bar chart in conclusion they stated that increase in technology there is also increase in cybercrimes. (Dr. Prateeksha and Richika, 2023)

9. Data analysis and interpretations

Table 01: Number of financial crimes between 2014-2023

YEAR	CASES REPORTED
2014	2,213
2015	3,477
2016	5,693
2017	9,622
2018	11,592
2019	12,317
2020	21,796
2021	27,248
2022	44,546
2023	50,035

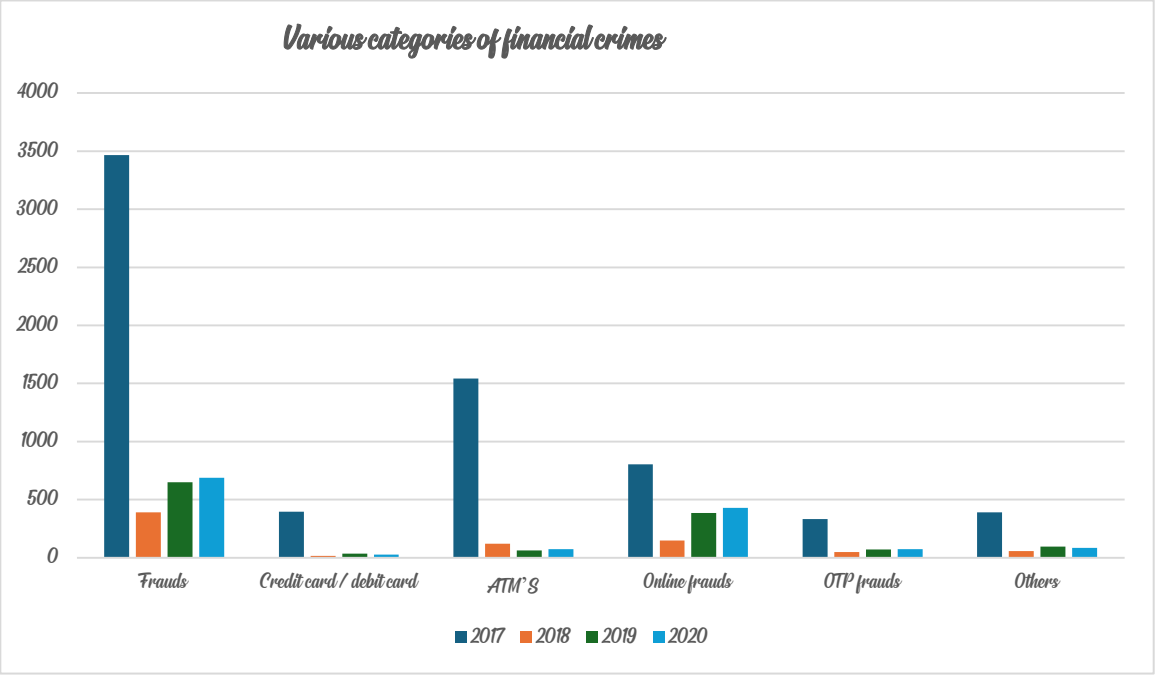


Interpretation

Therefore the above table and bar chart shows that the cases of cyber crimes are increasing over the years so this phase should be considered as an important threat to society. The year 2023 has the maximum number of cases.

Table 02 : Various categories of financial frauds between 2017 – 2020

Types of financial frauds	2017	2018	2019	2020
Frauds	3466	392	651	688
Credit card / debit card	395	16	34	28
ATM'S	1543	120	64	73
Online frauds	804	148	384	430
OTP frauds	334	50	72	73
Others	390	58	97	84
Total	6932	784	1302	1376



Interpretation

In the year 2017 there were many financial cases observed which covers frauds, ATM'S, credit and debit cards, OTP scams, and other types of threats. The number of cases has been withheld between 2017-2020.

Conclusion

This research paper has covered all the number of general cyber crimes in Banking sector. The study provides an overall view of what is cyber crime , how are they done , total number of cases , measure to prevent cyber crime and the total amount retrieved by the schedule commercial banks of India. Banking industries and IT are the crucial for the Indian Finance system. Still IT also has negative effect on the society which includes phishing , hacking , forgery , theft etc. Government of Indian should take a step to prevent these cyber crimes with appropriate measures. So this paper portraits both good and bad side of use of technology if it's used for improvement of the economy with proper measures and when we use technology to threaten or steal something from someone for their benefits using gadgets it's a threat to our society.

REFERENCE :

1. Reserve bank of India , Act 1934.
2. Indian penal code , 1860.
3. Information technology , Act 2000.
4. Kedia, R., & Barman, P. (2023). Cybercrime in India with reference to banking sector. Rabindra Bharati Journal of Philosophy, XXV(4), 17.
5. Kumar, M. (2023). An overview of cyber security in digital banking Sector. *East Asian Journal of Multidisciplinary Research*, *2*(1), 43-52
6. Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce*, *20*(1), 1-11.

7. Rao, H. S. (2019). Cybercrime in banking sector. *International Journal of Research-Granthaalayah*, *7*(1), 148-161.
8. Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-4). IEEE.
9. Jana, D. S., Khedkar, A. E., & Khedkar, C. E. Importance of cyber security in banking. Vidyabharati International Interdisciplinary Research Journal, 13(1), 203-206.