A Study of Cyber Crime on Banking Sector in India

Dr.C.Mallesha[1], M.Govardhan[2]
[1]Assistant.Professor, School of Management, Anurag University.
[2]Student, School of Management, Anurag University.

Abstract- The rise in technology has led to an increase in cybercrime, which is the illicit activities of cybercriminals to steal money and information. The concept of cybercrime, or cybercrime in cyberspace, is not well understood in India. These offenses take place online and on computers. Based on information from several institutions, this study highlights different frauds, including credit card, debit card, and ATM frauds, and focuses on cybercrime in the Indian banking industry. The survey, which spans the years 2016–2017 to 2019–2020, shows a notable rise in bank client transactions as well as cybercrimes.

Keywords: Cybercrime, banking, technology, frauds, cyber security.

INTRODUCTION

The surge in cybercrime in the current digital era is a serious threat to many different industries, the financial sector being especially vulnerable. Cybercriminals use a variety of illicit means to steal financial resources and private information, which is collectively referred to as cybercrime. The tactics and sophistication of these illicit activities are evolving along with technology, putting financial institutions and their clients at ever-greater risk.

India has become a haven for cybercriminals due to the country's quick adoption of digital banking and rising volume of online transactions. Notwithstanding the progress made in technology, a significant portion of the populace is nonetheless ill-informed or uninformed about the risks associated with cybercrime, which leaves them vulnerable to deception. Cybercrimes, such as credit card, debit card, and ATM frauds, have increased in the Indian banking industry. These crimes have not only resulted in large financial losses but have also eroded consumer confidence in the banking system.

The purpose of this study is to present a thorough examination of cybercrime in the Indian banking industry over the course of four years, from 2016–2017 to 2019–2020. The study assesses the impact of cyber fraud on the banking industry and determines the most common forms of cyber fraud by looking at data from different banks. The study also emphasizes the link between the rise in consumer transactions and the increase in cybercrimes, highlighting the pressing need for improved cybersecurity measures and more public awareness to protect India's financial sector.

NEED OF THE STUDY

The banking industry is seeing an increase in cybercrime, which calls for a careful analysis to determine its effects and create efficient defenses. Quantifying this surge and identifying patterns and trends in cyber criminal activities is crucial because of the noticeable increase in cybercrimes targeting financial institutions that has coincided with the spread of digital banking services. These crimes cause banks and their clients to suffer significant financial losses, underscoring the necessity of developing plans to reduce financial risks. Customer confidence in digital banking services is weakened by frequent cyberfraud incidents, so it is critical for banks to comprehend the effect on customer confidence in order to build and preserve trust. In order to safeguard client information and guarantee secure transactions, banks must also adhere to strict regulatory frameworks; this study will identify the areas in which compliance procedures require reinforcement. Cybercriminals' strategies are always changing along with technology, thus it's critical to find weaknesses in the current banking system and create strong cybersecurity measures. Comprehensive public education efforts are necessary because a substantial section of the Indian populace is still ignorant about cyberthreats and effective practices for online security. The study helps banks with strategic planning and investment in cybersecurity technologies and training by offering comprehensive insights into cybercrime trends and their impact. In conclusion, this research is critical to addressing the growing threat of cybercrime in the Indian banking industry. It seeks to give a thorough grasp of the issue, provide light on practical preventative and mitigation measures, and eventually aid in the creation of a more secure banking environment.

OBJECTIVES

1.To study various types of cyber attacks in banking.
2. Impact of cyber attacks on banking sector.
3. To suggest the preventive measures to control the cyber crime.

RESEARCH METHODOLOGY

The information gathered for the project's comparative analysis comes from secondary sources, including several books, websites, journals, and articles.

LIMITATIONS

1. The data acquired from the secondary sources forms the foundation for the study's accuracy.
2. The study only looks at the banking industry.

REVIEW OF LITERATURE

1. A thorough summary of cybercrimes in India is given in the technical review by Datta et al. (2020), which also emphasizes the growing sophistication and frequency of these acts. The writers examine several kinds of cybercrimes, their effects on people and institutions, and the difficulties law enforcement has in addressing these problems. The study also examines current legislative frameworks and makes recommendations for strengthening their administration and prevention of cybercrime.
2. An informative analysis of the types and extent of cybercrime on the internet is provided by Deora and Chudasama (2021), who highlight the escalating risks that individuals and companies face. This study looks at several types of cybercrime, how they do it, and how it affects digital security. The writers also cover the topic of precautions and technology's involvement in reducing these online dangers.
3. In their comprehensive assessment of the literature, Mangala and Soni (2023) provide a thorough analysis of the various forms, strategies, and effects of banking fraud. The review emphasizes how fraudulent actions are always changing and how they negatively impact banking institutions' finances and reputation. The writers also go over existing detection and prevention techniques, highlighting the necessity of cutting-edge technical solutions to successfully tackle financial fraud.
4. In his study of Industry 4.0 technology adoption in the Indian banking sector, Gupta (2023) emphasizes the revolutionary potential of digital innovations like blockchain, artificial intelligence, and the Internet of things. This article examines the advantages, difficulties, and present situation of technology integration in banks, focusing on how it affects productivity and client satisfaction. Gupta also delineates pivotal domains for forthcoming investigations to augment and amplify the execution of Industry 4.0 in the banking sector.
5. In their investigation of the fundamental causes of bank frauds in the Indian banking sector, Khan, Ahmad, and Farooque (2023) provide a thorough examination of the various elements that contribute to these crimes, including regulatory loopholes, organizational flaws, and technology vulnerabilities. Their analysis highlights important areas where institutions are more vulnerable to fraud and talks about the complex effects on the financial industry. The authors also suggest ways to improve fraud prevention and detection, with the goal of fortifying Indian banks' general security framework.
6. Sviatun et al. (2021) examine the legal and economic sides of fighting cybercrime, highlighting the crucial interaction between these elements in successfully countering cyberthreats. The economic effects of cybercrime on companies and the overall economy are highlighted in their review, along with the frameworks and legal difficulties associated with prosecuting cybercriminals. To support initiatives against cybercrime, the authors support tighter legal restrictions and increased international collaboration.

Objective: 1 To study various types of cyber-attacks in banking.
1. Attacks by Phishers: Cybercriminals create fraudulent emails, messages, or websites that mimic reputable sources, such banks or other financial institutions, in order to carry out phishing attacks. These fake messages frequently ask for sensitive

information, like credit card numbers, usernames, and passwords, in an urgent manner. Once acquired, this data is utilized to steal money, perpetrate identity theft, or get access to victims' accounts.

2. Virus Attacks: Malware, an acronym for malicious software, encompasses a range of destructive applications, including ransomware, trojans, spyware, and viruses. These applications can be distributed via downloads, compromised websites, or email attachments. Malware can record keystrokes, steal login passwords, encrypt data (ransomware), or grant attackers remote access once it has been put on a user's device or a financial system. This makes it possible for cybercriminals to steal confidential data or demand ransom for the data.

3. Attacks that cause a denial of service (DoS) or distributed denial of service (DDoS): A denial-of-service (DoS) assault occurs when an online bank's services are overloaded with traffic, making them inaccessible to authorized customers. DDoS assaults intensify this by generating bandwidth from several hacked systems, which makes it harder to counteract the attack. These assaults interfere with banking operations, upsetting clients and perhaps resulting in loss of money and harm to one's reputation.

4. Stuffing Credentials: Cybercriminals attempt to get into banking websites by using usernames and passwords that have been stolen or made public from prior data breaches. They take advantage of the widespread practice of reusing passwords by using automated programs to attempt these credentials on several accounts. If they are successful, they can access users' bank accounts without authorization and take money or personal data from there.

5. Skimming ATMs: In order to obtain the information contained on a credit or debit card's magnetic stripe, skimming devices are covertly put on ATMs. In addition, the user's PIN may be recorded via fictitious keypads or hidden cameras. Criminals can use this information to make fake cards and take money out of the victim's account. These gadgets can result in large financial losses and are frequently hard to find.

6. Insider Dangers: Employees or contractors that abuse their permitted access to a bank's systems and data are considered insider threats. Insiders may steal confidential data, embezzle money, or aid outside attackers due to motivations such as financial gain, grievances, or coercion. Because these dangers come from within the company, they are very difficult to identify and neutralize.

7. Injection of SQL: By injecting malicious SQL queries into input fields, SQL injection attacks take advantage of weaknesses in a bank's web applications. By manipulating the underlying database, these queries give attackers the ability to retrieve, change, or remove sensitive data. A successful SQL injection could result in serious data breaches that expose client information and jeopardize the reliability of the bank's systems.

8. Social Engineering: Social engineering attacks use psychological manipulation to fool people into sharing private information or taking activities that put their security at risk. Pretexting, or fabricating a situation, baiting, or presenting an alluring offer, and phishing are examples of tactics. Social engineering is a useful tool used by cybercriminals to obtain sensitive information or systems because it takes advantage of human psychology.

9. One-Day Workarounds: Zero-day exploits profit from flaws in software or systems that have not yet been discovered. These vulnerabilities give attackers a window of opportunity because developers haven't yet patched or identified them. Because zero-day attacks go around current security measures, they can be very harmful because they let hackers steal data, compromise banking systems, or interfere with operations until the vulnerability is fixed.

The Reasons Behind Bank Cybercrime

1. Revenue: The majority of cybercriminals attack banks primarily for financial gain. Due to their huge volume of financial transactions and substantial cash holdings, banks are attractive targets for theft, embezzlement, and fraud.

2. Theft of Data: Millions of clients' sensitive financial and personal data is stored by banks. On the criminal market, this information is worth a lot and can be sold to perpetrators of identity theft, credit card fraud, and other crimes.

3. Weaknesses in Technology: Rapid technological development may expose financial systems to problems. Cybercriminals can obtain illegal access by taking advantage of outdated software, unpatched systems, and inadequate security configurations.

4. Inadequate Safety Protocols: Certain banks might have antiquated or inadequate cyber security protocols. Banks may become targets of cyber-attacks

if they don't have strong firewalls, encryption, intrusion detection systems, and frequent security audits.

5. Insider Threats and Human Error: Workers may purposefully or unintentionally jeopardize security. Cybercriminals can gain access through human error, such as falling for phishing scams or improperly configuring systems. There are also serious dangers from insider threats, which occur when staff members utilize their access for nefarious ends.

6. Digitalization is Growing: The shift to digital financial services has made it easier for cybercriminals to launch attacks. ATMs, smartphone banking apps, and online banking are all possible entry sites for cyberattacks.

7. Advanced Nature of Cyber-attacks: Cybercriminals are always coming up with new and advanced ways to get into banking systems. Complex approaches are used by state-sponsored attacks, advanced persistent threats (APTs), and zero-day exploits to avoid detection and compromise security

Objective 2:

	2016-2017		*2017-2018*		*2018-2019*		2019-2020	
STATE NAME	No. of frauds	Amt. involved	No. of frauds	Amt. involved	No. of Frauds	Amt. involved	No. of frauds	Amt. involved
Andaman & Nicobar islands					10	0.12	20	0.09
Andhra Pradesh	31	0.64	72	0.27	181	0.36	465	1.85
Assam	3	0.11	218	2.03	87	0.85	423	2.58
Bihar	4	0.07	50	0.24	151	0.61	260	1.02
Chandigarh	7	0.19	90	0.27	111	0.37	146	66.67
Chhattisgarh	1	0.01	46	0.22	106	0.41	164	0.57
Dadra & Nagar Haveli			10	0.01	16	0.02	21	0.03
Daman & Diu							20	0.04
Goa			18	0.08	114	0.57	176	0.44
Gujarat	16	0.53	563	9.41	1135	2.23	1788	4.79
Haryana	238	8.28	8444	24.05	8983	21.20	5083	17.52
Himachal Pradesh	1	0.02	26	0.16	47	0.17	125	0.58
Jammu & Kashmir	1	0.09	53	0.38	27	0.07	71	0.20
Jharkhand	9	0.12	40	0.15	109	0.61	155	0.53
Karnataka	221	9.16	1573	10.59	1886	5.17	2845	17.57
Kerala	9	0.46	120	0.64	212	1.46	745	3.75
Madhya Pradesh	4	0.10	104	0.83	212	0.62	515	1.72
Maharashtra	379	12.10	15629	43.44	21673	42.35	21897	44.99
Manipur			1	0.00	8	0.07	5	0.02
Meghalaya			8	0.03	12	0.05	20	0.13
Mizoram					5	0.01	8	0.06
Nagaland			9	0.04	3	0.02	9	0.07
New Delhi	156	3.44	1697	13.37	4191	15.76	5499	15.37
Odisha	1	0.06	51	0.35	115	0.53	456	2.55
Overseas	7	0.22	27	0.16	27	0.29	12	0.09
Pound cherry	2	0.05	9	0.04	6	0.05	12	0.05
Punjab	3	0.27	214	0.99	288	0.92	501	2.14
Rajasthan	10	0.16	132	1.18	374	1.47	755	9.17
Sikkim			2	0.01	4	0.00	15	0.06
Tamil Nadu	208	4.39	3855	50.36	5497	24.06	5258	17.03
Telangana			586	4.30	974	2.61	1284	2.75
Tripura			6	0.04	9	0.03	25	0.10
Uttar Pradesh	37	1.04	763	3.16	5109	7.80	2130	10.57
Uttarakhand			119	0.57	128	0.53	141	0.44
Uttaranchal	5	0.13						
West Bengal	19	0.67	245	1.50	493	17.99	951	2.86
GRAND TOTAL	1372	42.29	34791	168.99	52304	149.42	52006	228.44

The above table indicates that state scams in India are rising.2019-2020 (52006) is close to 2018-2019 52304 but higher than 2017-2018 34791. Cyber crime frauds are threatening India's financial system. Each year, debit card, credit card, ATM, and online banking fraud instances rise. The difference in fraud instances between 2018-2019 and 2019-2020 is 100, but the sum is 79.02 cores. Indian banking transactions are rising, as is fraud. For banking fraud control, RBI provides fraud awareness.

Effects of Cyber-attacks on the Financial Industry

1. Losses in Money: Cyberattacks frequently cause banks to suffer large financial losses. These losses may be from outright financial theft, expenses for containing the assault, court costs, regulatory fines, and payments to impacted clients.
2. Damage to Reputation: A bank's reputation can be seriously harmed by cyberattacks. Client loyalty and business suffer as a result of customers losing faith in the organization's capacity to protect their funds and personal data. Potential clients may potentially be turned off by unfavorable press.
3. Disturbances in Operation: Banking operations may be hampered by cyberattacks, particularly those involving ransomware or DDoS attacks. These interruptions may result in lost business continuity, inconvenience to clients, and transaction halts as well as restricted access to online services and daily banking operations.
4. Regulatory Sanctions: Strict regulatory standards for cybersecurity and data protection apply to banks. Successful cyber attacks have the potential to reveal violations of these rules, which might lead to significant fines and legal action from the regulatory authorities.
5. Higher Security Expenses: Following a cyberattack, banks frequently have to make significant investments to strengthen their cybersecurity infrastructure. This entails carrying out extensive security assessments, introducing new security measures, updating systems, and giving employees more training.
6. Inaccuracies in Data: Cyberattacks have the potential to expose private client data, including as transaction history, account information, and personal information. Customers may suffer greatly as a result of identity theft, financial fraud, and other negative behaviors brought on by data breaches.
7. Repercussions Legally: Customers and business partners who lose money as a result of a cyberattack may take banks to court. Suits can lead to high settlements and legal costs, which exacerbate financial losses.
8. Attrition of Customers: Customer attrition may arise from a loss of confidence and trust. Customers who are impacted can decide to transfer their accounts to other banks that they believe have stronger security protocols, which would cause the bank to lose market share.
9. Effect on Equity Prices: Following a cyberattack, stock values of publicly traded banks may drop. The market value of the bank may drop if investors lose faith in the safety and future performance of the institution.
10. Theft of Intellectual Property: Intellectual property and private information can be stolen as a result of cyberattacks. Trade secrets, business plans, and exclusive technology are a few examples of this, as they can be used by rivals or sold illegally.
11. Customer Service Disruption: Customers may become frustrated and dissatisfied if online and mobile banking services are unavailable due to attacks like denial-of-service (DDoS). Extended disruptions in service may prompt clients to look for more dependable banking options.
12. Failures in Compliance and Audits: A cyberattack that is successful enough can reveal gaps in a bank's audit and compliance procedures. This may result in stricter audit requirements and heightened regulatory scrutiny, taking time and resources away from other company operations.
13. Psychological Effects on Staff Members: Bank workers may experience stress as a result of cyberattacks, which might lower morale and reduce output. Managing the aftermath of an incident and putting new security measures in place can come with a lot of strain.
14. Reduction of Advantage in Competition: A bank may lose its competitive edge if their strategic plans or confidential business information is compromised. Rivals may use this knowledge to enhance their own business practices or increase market share.

In conclusion, there are many different ways that cyberattacks harm the banking industry, including operational effectiveness, consumer trust, financial stability, and regulatory compliance. To tackle these effects, a thorough approach to cybersecurity is needed, one that incorporates strong preventive measures, efficient incident response plans, and ongoing security practice improvement.

Objective 3: Preventive Measures to Reduce Cybercrime in the Banking Industry

1. Install Robust Authentication Systems: Apply multi-factor authentication (MFA) to bolster security even more. By requiring users to supply two or more authentication criteria, this lowers the possibility of unwanted access.
2. Continuous Vulnerability Assessments and Security Audits: To find and address any possible vulnerabilities in the financial system, conduct frequent security audits and vulnerability assessments. This proactive strategy aids in reducing the possibility of cyberattacks.
3. Programs for Employee Awareness and Training: Provide regular cybersecurity training to staff members, including topics such as spotting phishing scams, protecting sensitive data, and reacting to possible dangers. Programs that raise awareness can dramatically lower human error.
4. Sophisticated Encryption Methods: Use robust encryption for both in-transit and at-rest data. Data encrypted is guaranteed to remain unreadable and safe even in the event of interception or unauthorized access.
5. Strong Intrusion Detection Systems (IDS) and Firewalls: To monitor and manage incoming and outgoing network traffic, implement sophisticated firewalls and intrusion detection systems. Potential cyberattacks can be stopped by these systems' ability to recognize and stop suspicious activity.
6. Continuous Software Upgrades and Patch Administration: Update all software with the most recent security patches, including operating systems and apps. Frequent updates aid in addressing security holes that cybercriminals could potentially exploit.
7. System and network configuration that is secure: Verify that every network and system is set up securely. Disable unused services and ports, impose strict password requirements, and put security standards and guidelines into practice.
8. Reaction Plan for Incidents: Create an incident response plan and update it frequently. Procedures for identifying, addressing, and recovering from cyberattacks should be included of this plan. Damage can be reduced and regular activities can be promptly resumed with a well-prepared reaction.
9. Applying Sophisticated Anti-Malware Products: Install cutting-edge anti-malware programs with real-time threat detection and neutralization capabilities. Update these solutions frequently to defend against the most recent malware iterations.
10. Solutions for Data Loss Prevention (DLP): Use DLP solutions to keep an eye on, identify, and stop illegal access to and transfers of private information. DLP assists in preventing the theft or leakage of private information.
11. Network Segmentation: Divide networks into segments to stop cyberattacks from spreading. The network can be made more difficult for attackers to traverse laterally and access important systems by breaking it up into smaller, more isolated portions.
12. Control of Third-Party Risk: Assess and keep an eye on the security procedures used by outside suppliers and service providers. Make sure they follow the same security guidelines and put in place safeguards to lessen the hazards brought on by unauthorized access.
13. Continuous Plans for Backup and Recovery: Make regular backups of your vital systems and data. To ensure that data can be promptly restored in the case of an attack, make sure backup and recovery methods are routinely verified.
14. Application of Behavior Analytics: Utilize behavioral analytics to keep an eye on user activity and spot any unusualities that might point to possible security risks. Algorithms that use machine learning can recognize questionable activity and send out alerts.
15. Consumer Security Awareness: Inform clients on cybersecurity best practices and hazards. Give them pointers on how to spot phishing scams, make secure passwords, and protect their online banking.
16. Regulatory Standard Compliance: Assure adherence to pertinent legal frameworks and standards, including GDPR, PCI DSS, and regional cybersecurity laws. A high degree of security is maintained and legal ramifications are avoided with the aid of compliance.
17. Staying Aware and Gathering Threat Intelligence: Keep an eye out for indications of cyber dangers by continuously monitoring systems, and use threat intelligence to stay up to date on new risks. An early detection and prevention of cyberattacks can be

facilitated by proactive monitoring and intelligence exchange.

CONCLUSION

The banking sector is facing an escalating and substantial risk from cyber crime, which is fueled by the advancing expertise of cyber thieves and the swift transition to digital financial services. These attacks can have a severe impact, resulting in significant financial losses, harm to reputation, disruptions to operations, and loss of client trust. In order to counteract these dangers, financial institutions must implement a comprehensive strategy for safeguarding against cyber attacks. This strategy should include the implementation of robust authentication systems, conducting frequent security audits, providing thorough employee training, utilizing advanced encryption techniques, and establishing effective incident response strategies. Banks may strengthen their security position, safeguard sensitive data, and maintain the trust and confidence of their clients by implementing thorough preventive measures and remaining alert to new threats. Consistently enhancing cybersecurity policies and adopting a proactive approach to risk management are crucial for protecting the financial ecosystem from the constantly changing realm of cyber crime.

REFERENCE

[1] Tanwar, S., Datta, P., Panda, S. N., and Kaushal, R. K. (March 2020). a report about cybercrimes in India that is technical in nature. "Emerging Smart Computing and Informatics: 2020 International Conference" (pp. 269-275). IEEE.

[2] Chudasama, D., and Deora, R. S. (2021). a succinct overview of online fraud.11(1), 1-6, Journal of Communication Engineering & Systems.

[3] Soni, L., and Mangala, D. (2023). a thorough analysis of the literature on banking sector frauds.30(1), 285–301, Journal of Financial Crime.

[4] Gupta, Richard. (2023). A evaluation and research strategy for the Indian banking sector's adoption of Industry 4.0.27(1) Vision, 24-32.

[5] Ahmad, S. A., Khan, A. H. J., and Farooque, A. (2023). Journal of Research Administration, 5(2), 4709-4721. A STUDY TO INVESTIGATE THE REASONS FOR BANK FRAUDS IN THE INDIAN BANKING INDUSTRY.

[6] Goncharuk, O. V., Kuzmenko, O., Roman, C., Sviatun, O. V., & Kozych, I. V. (2021). Legal and financial issues of fighting cybercrime.Journal of Business and Economics at WSEAS, 18, 751–762.