IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, June 2024

Guarding Against Cyber Threats: Managing Risks in the Digital Age

Anish Shrimali
Chief Manager, Union Learning Academy- Digital Transformation,
Union Bank of India, Mumbai, India

Abstract: *The digitalization wave has transformed the world, bringing numerous benefits to individuals and businesses. Communication has become more efficient, transactions are easier, and access to information is faster. This transformation is particularly evident in the banking sector, where the adoption of online platforms and mobile applications has revolutionized traditional banking methods. However, the increasing reliance on digital technologies has also brought about significant cyber security risks. The study focuses on the rapid growth of digital transactions in India, the types of cyber threats, the impact on financial institutions and customers, prevalent cyber frauds, and comprehensive measures to enhance cyber security. This paper delves into the cyber security threats faced by the banking sector, their impacts, and strategies to mitigate these risks.*

Keywords: Cyber Security, Digital Banking, Cyber Threats, Mitigation Strategies, Digital Transactions

I. INTRODUCTION

The digitalization of the banking sector has led to increased efficiency and accessibility of banking services. However, this transformation has also heightened the vulnerability of financial institutions to cyber-attacks. This paper investigates the cyber security challenges faced by the banking industry, particularly in the context of the significant growth in digital transactions in India. The study aims to provide insights into various cyber threats, their impacts, and effective mitigation strategies.

1.1 Growth of Digital Payments in India

The Indian banking sector has witnessed a substantial increase in digital transactions. From FY 2021-22 to FY 2023-24, the number of transactions rose from approx.7200 crore in FY 2021-22 toapprox. 16400 crore by March 2024. UPI transactions alone registered 45 billion in FY 2021-22, with a total transaction value of 1.39 lakh billion in FY 2022-23.

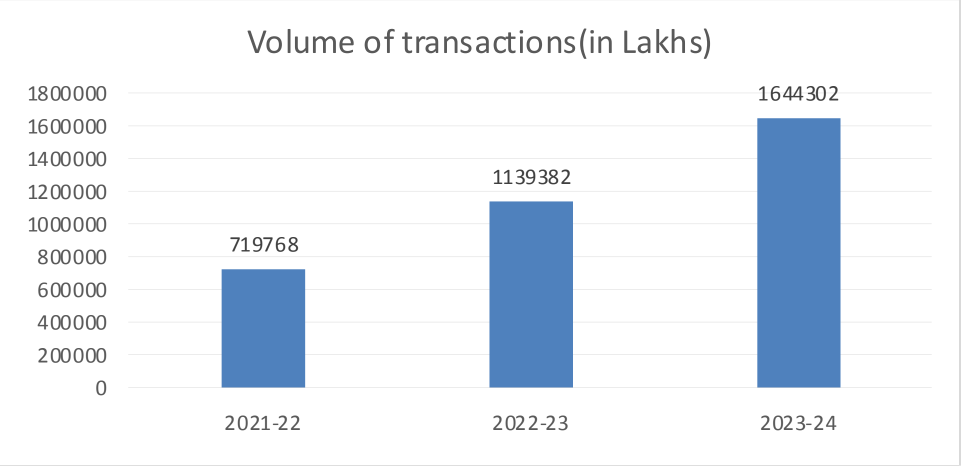

Fig 1 Growth of Digital Payments (Source: RBI Annual Report 2023-24)

DOI: 10.48175/568

1.2 Impact of Digital transformation on Banking

The transition to digital platforms has made banking services more accessible but has also expanded the attack surface for cyber criminals. The rapid adoption of digital technologies, accelerated by the COVID-19 pandemic, has increased the banking sector's exposure to cyber threats.

1.2.1 Factors Contributing to Cyber Security Risks

Cyber security risks refer to the potential of unauthorized access, theft, damage, or destruction of digital data, systems, and networks. These risks can come from a variety of sources, including hackers, cyber criminals, insiders, and even state-sponsored actors. With more and more sensitive information being stored and transmitted online, cyber security has become a critical concern for businesses, governments, and individuals.

Some of the main factors contributing to cyber security threat or risks are:

Rapid adoption of digital technologies: The COVID-19 pandemic has significantly accelerated the adoption of digital technologies. Businesses and individuals have increasingly relied on digital solutions to maintain operations and stay connected. This shift has led to a surge in the use of online platforms for communication, e-commerce, and remote work. However, this increased reliance on digital technologies has expanded the number of potential targets for cyber criminals. Businesses storing sensitive information, such as financial data, customer details, and intellectual property, face heightened risks of cyber attacks. Likewise, individuals using online banking, social media, and e-commerce platforms are more susceptible to identity theft, phishing attacks, and other forms of cybercrime.

Complexity of modern digital systems. As technology has advanced, digital systems have become more complex and interconnected. This makes it harder to identify and address vulnerabilities in the system, and makes it easier for cyber criminals to exploit these vulnerabilities.

Use of emerging technologies: The increasing use of cloud computing, mobile devices, and the Internet of Things (IoT) has created new opportunities for cyber-attacks. For example, the proliferation of IoT devices such as smart home appliances and wearable technology has created new targets for cyber criminals to exploit.

Shortage of skilled cyber security professionals: The shortage of skilled cyber security professionals is another factor contributing to the increase in cyber security risks. As the demand for cyber security experts has grown, there has been a shortage of qualified professionals to fill these roles. This has led to a situation where many businesses and organizations are not able to adequately protect themselves from cyber threats.

II. METHODOLOGY

The research methodology involves a comprehensive review of existing literature, including reports from the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), Indian Computer Emergency Response Team (CERT-In), and various cyber security firms. The study also analyses recent cybercrime statistics and trends, focusing on their impact on the banking sector.

III. LITERATURE REVIEW

Digital transactions in India have seen exponential growth, with digital payment transactions increasing from 2071 crore in FY 2017-18 to 12009 crore by March 2023. However, this growth has been accompanied by a rise in cyber incidents. In 2022 alone, India witnessed 13.91 lakh cyber security incidents. Various reports highlight that a significant portion of frauds in the banking sector are cyber-related, with insider threats, phishing attacks, and advanced persistent threats (APTs) being particularly prevalent.

According to recent reports, India encountered approximately 13.91 lakh cyber security incidents in 2022, as highlighted by CERT-In, the national agency coordinating cyber incident response activities. Deloitte India's Banking survey for 2022 indicated that around 40% of fraud cases in India were linked to digital and cyber-related issues. In 2023, India saw a notable 15% weekly rise in cyber-attack incidents per organization, positioning it as the second most targeted nation in the Asia Pacific region after Taiwan, according to Check Point, a leading cyber security firm. Globally, organizations faced an average of 1,158 weekly cyber attacks, marking a slight increase from the previous year. In the APAC region, India's surge in attacks ranked second with a 15% increase, following Korea's 21% rise. The

education and research sector observed a decrease in attacks by 12%, while the retail and wholesale sectors experienced a 22% uptick. The healthcare sector's 3% rise in attacks is of particular concern due to the critical nature of its services.
The RBI's report :Trend and Progress of Banking in India 2022-23" highlights a significant increase in banking sector frauds, with 14,483 cases reported in the first half of the financial year 2023-24, involving Rs 2,642 crore. Despite the rise in incidents, the amount involved represents a decrease of 14.9% compared to the previous year. Emphasizing the imperative to safeguard banking and payment systems from cyber threats, the report underscores the risks posed by frauds, which encompass reputational, operational, and business risks for banks. It calls for enhanced technological defenses and robust risk management practices to mitigate vulnerabilities. Additionally, the report notes the growing adoption of AI among Scheduled Commercial Banks in India for fraud detection, data analytics, and customer service enhancements, highlighting AI's transformative potential across financial services, from algorithmic trading to risk management and customer experience improvements.
The RBI's annual report 2023-24 highlights a significant 46.7% decline in the total value of financial frauds reported during the fiscal year 2023-24 compared to the previous year. According to the report, private-sector banks reported the highest number of fraud cases, while public-sector banks reported the highest value of frauds. Digital payments, including card and internet transactions, constituted the majority of fraud cases in terms of number, whereas frauds in loan portfolios accounted for the highest value. The report also notes that the amount involved in past financial year frauds constituted a significant portion of the total reported in 2022-23. Looking ahead to 2024-25, the RBI outlines its priorities focusing on regulation, supervision, and enhancing financial stability. Initiatives include bolstering cyber incident response capabilities among Scheduled Commercial Banks (SCBs) through a new cyber range and leveraging AI and machine learning for fraud prevention.

IV. RESULTS AND DISCUSSION

4.1 Key cyber security risks and threats

In the age of digitalization, financial and banking institutions face several critical cyber security risks and threats:

- Ransomware Attacks: Traditional ransomware attacks involved encrypting data and demanding a ransom for decryption. The new trend of double extortion is even more threatening, as attackers now also threaten to expose sensitive information publicly if the ransom is not paid promptly.
- Malware and Phishing Attacks: Malware and phishing attacks are among the most common cyber security threats in the banking sector. Malware refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks. Phishing attacks are fraudulent attempts to obtain sensitive information, such as usernames, passwords, and credit card details, by posing as a trustworthy entity through email or other electronic communication.
- Insider Threats: Insider threats pose significant risks for the banking sector. These threats can originate from current or former employees, contractors, or others with privileged access to sensitive information. Insider threats can range from unintentional errors to deliberate theft or sabotage.
- Social Engineering AttacksSocial engineering attacks exploit human psychology to manipulate individuals into divulging sensitive information or performing actions that compromise security. These attacks can take various forms, including phishing, pretexting, baiting, and QR-phishing (quishing).
- Distributed Denial of Service (DDoS) Attacks: DDoS attacks involve overwhelming a network or server with traffic to disrupt or disable it. These attacks can cause significant downtime and financial losses for banks and other financial institutions.
- Advanced Persistent Threats (APTs): APTs are sophisticated, targeted cyber-attacks designed to gain access to sensitive information and remain undetected for extended periods. These attacks are difficult to detect and require specialized expertise to combat.
- Third-Party Risks: Many banks and financial institutions depend on third-party vendors for services such as cloud computing, data storage, and payment processing. However, these third-party vendors can introduce new risks and vulnerabilities into the bank's systems and networks.

DOI: 10.48175/568

4.2 Key Insights on Cybercrime in India: 2023 (Report from Indian Cyber Coordination Centre (I4C), 2023)

- Cybercrime Rate: India experienced 129 reported cybercrimes per lakh population in 2023, with Delhi leading at a rate of 755, followed by Chandigarh (432), Haryana (381), and Telangana (261).
- Fraud Composition: Local-origin cybercrimes were primarily constituted by customer care, refund-based, and KYC expiry frauds (35%), sextortion (24%), online booking frauds (22%), AePS frauds, and biometric cloning (11%), with Android malware contributing 8%.
- Financial Impact: Online frauds resulted in a staggering loss of Rs. 10,319 crore between April 2021 and December 31, 2023. However, timely intervention through the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) and the '1930' financial cyber fraud helpline saved Rs 1,127 crore, accounting for 9-10% of the total defrauded money.
- Victim Support: The CFCFRMS and '1930' helpline have assisted 4.3 lakh victims to date. Efforts are underway to address delays in restoring defrauded money through the formulation of standard operating procedures.
- Reporting Mechanisms: The Indian Cyber Coordination Centre (I4C) facilitates citizen reporting via the National Cybercrime Reporting Portal (NCRP), which has received over 31 lakh complaints. Approximately 5,000 complaints are registered daily, with 40-50% involving actors from outside the country, particularly China, Cambodia, and Myanmar.
- Trend Analysis: Complaints on the NCRP increased by 61% to 15.6 lakh in 2023 from 9.66 lakh in 2022, although the rise was lower compared to the 113.7% increase between 2021 and 2022.
- Fraud Categories: Internationally originated frauds were dominated by investment and task-based scams (38%), illegal loan apps (23%), gaming frauds and crypto scams (21%), ransomware attacks (7%) and other scams (11%).

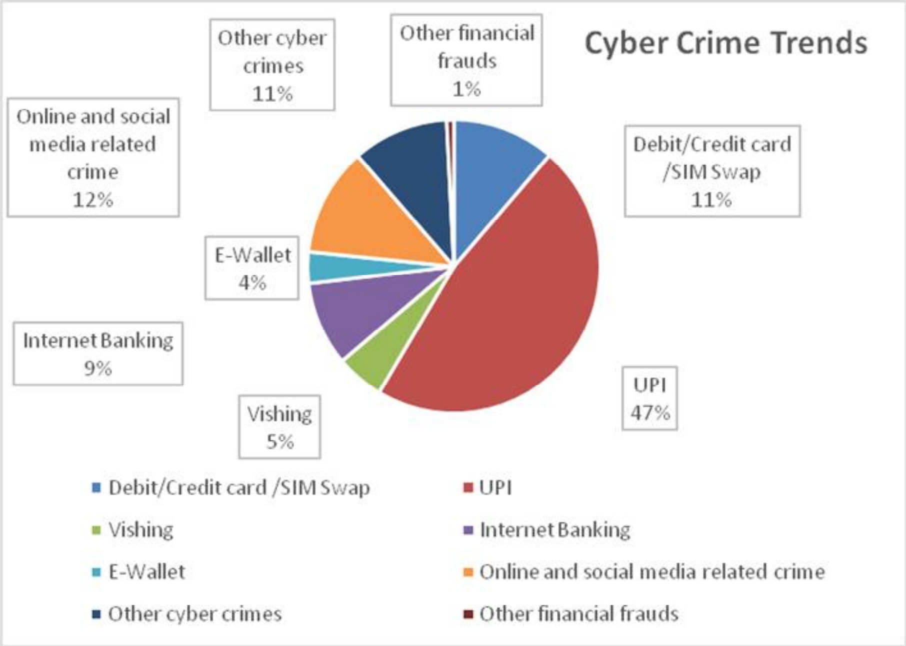

Fig 2. Cyber Crime trends (Break-up of online financial frauds between Jan 2020 and Jul 2023, Source: Future Crime Research Foundation))

4.2.1 Key Insights on Cybercrime in India: 2023 (Report from Indian Cyber Coordination Centre (I4C), Jan-Apr 2024)

- Between January and April 2024, Indian citizens reported losses exceeding Rs 1,750 crore due to cybercrime.

- Over 740,000 complaints were lodged on the National Cybercrime Reporting Portal during this period.
- The Indian Cyber Crime Coordination Centre (I4C) noted a 113.7% surge in daily cybercrime complaints in May 2024 compared to 2021-2023.
- Financial online fraud constituted 85% of these complaints.
- Reported cases to I4C escalated from 26,049 in 2019 to 740,957 in the first four months of 2024.
- Fraud types included online investment schemes, gaming app scams, algorithm manipulations, illegal lending apps, sextortion, and OTP frauds.
- Trading scams alone resulted in Rs 1,420 crore losses across 20,043 cases in early 2024.
- The I4C collaborates with regulatory bodies like RBI and fintech firms to curb misuse of mule accounts and telecom infrastructure.
- Efforts continue to disrupt cybercrime operations involving Skype, Google, Meta advertisements, SMS headers, SIM cards, and bank accounts.

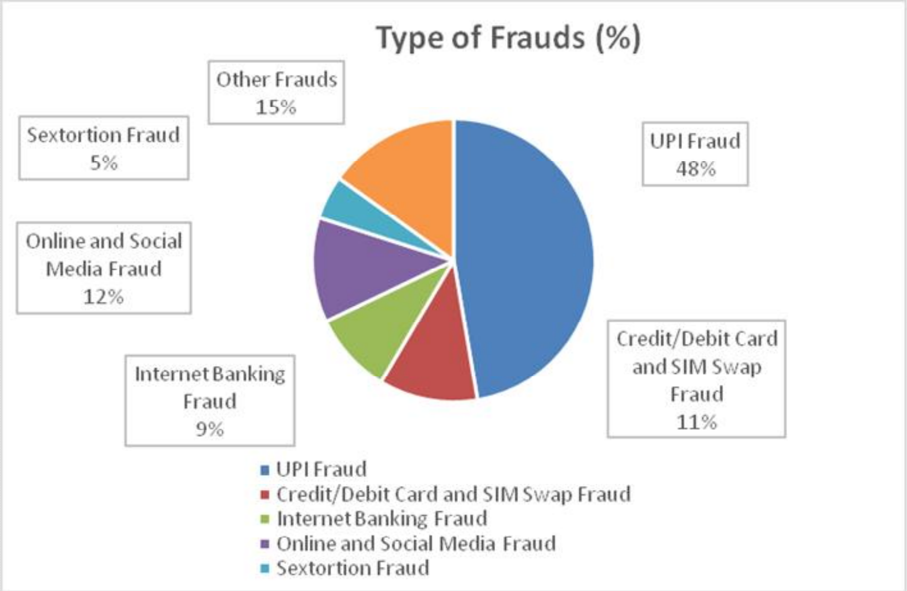

Fig 3 Cyber Crime trends (Break-up of online financial frauds between Jan 20204 and Apr 2024, Source: Indian Cyber Crime Coordination Centre (I4C)

4.3 Impacts on Banking Systems and Customers

Cyber-crimes have profound and far-reaching consequences for banking systems and their customers:

4.3.1 Impacts on Banking Systems

- Financial Losses and Operational Disruptions: Cyber attacks result in significant financial losses and disrupt banking operations, leading to downtime and compromised services.
- Regulatory Penalties and Reputational Damage: Banks face heavy fines and penalties for failing to protect customer data. Data breaches and service interruptions erode customer trust, affecting customer retention and acquisition.
- Increased Operational Costs: Following a cyber incident, banks must invest in cyber security measures, recovery efforts, and regulatory compliance. These increased operational costs can impact profitability and may be passed on to customers.
- Broader Economic Implications: Large-scale cyber attacks on banking systems can destabilize financial markets, undermine investor confidence, and threaten overall economic stability.

- Regulatory Scrutiny and Legal Consequences: Banks face heightened regulatory scrutiny and potential legal consequences for non-compliance with cyber security regulations. This can affect their overall regulatory standing and operational viability.

4.3.2 Impacts on Customers

- Financial Loss and Identity Theft: Customers can suffer direct financial losses and identity theft, leading to compromised personal information.
- Distress and Inconvenience: The aftermath of cyber incidents often involves prolonged processes to recover stolen funds or restore credit ratings, causing significant distress and inconvenience to affected individuals.

Overall, the impacts of cybercrimes on banking systems and customers are extensive, necessitating robust cyber security measures and proactive risk management strategies.

4.4 Prevalent Cyber Frauds Targeting Customers

- Electricity Bill Payment Scam: Fraudsters send text messages demanding immediate payment to avoid power disconnection. Customers should verify any payment requests and sender information before proceeding with transactions. Use only official websites and apps from legitimate electricity providers for online payments. Check website URLs for security indicators like "https://" and a padlock symbol. Communicate through secure channels for payment-related inquiries. Download UPI apps exclusively from official app stores and verified sources.
- KYC fraud: It is becoming increasingly common, mainly targeting retired officials. Theyreceived a call from someone claiming to be from their bank, requesting KYC details. Trusting the caller, they followed instructions, only to find their savings depleted. Banks never request financial transactions over calls. To update KYC, customers should use secure online banking portals or visit the bank directly.
- SIM-Swap Fraud: SIM swap fraud, also known as SIM hijacking or SIM splitting, involves fraudsters deceiving a mobile carrier into transferring the victim's phone number to a new SIM card under their control. With access to the victim's phone number, they can intercept calls, text messages, and authentication codes, enabling them to bypass security measures like two-factor authentication (2FA). This allows unauthorized access to accounts, including bank and social media accounts, often resulting in financial loss and identity theft.
- OTP Fraud: OTP fraud involves scammers tricking individuals into providing one-time passwords (OTPs) sent via SMS, email, or authenticator apps. These OTPs are used as an additional security layer for verifying transactions, logging into accounts, or completing sensitive actions online. Fraudsters use various tactics to obtain OTPs, such as phishing emails or messages, fake websites, or social engineering techniques. Once they have the OTP, they can conduct unauthorized transactions or gain access to accounts, leading to financial loss or identity theft. Individuals must be cautious and never share OTPs with anyone, especially if they were not expecting a verification request.
- Aadhaar-enabled Payment System (AePS) Fraud: Scammers exploit vulnerabilities in the Aadhaar-enabled Payment System (AePS) to drain bank accounts without SMS or OTP authentication. Reports show a rise in Aadhaar card-related scams in India, where scammers use leaked biometric details to bypass OTPs and steal money from bank accounts. They even use silicone thumbs to manipulate biometric devices and ATMs for unauthorized withdrawals.
- QR Code Scam (Quishing): Quishing involves fraudsters creating QR codes that appear genuine but redirect victims to fake websites controlled by attackers. Victims are tricked into divulging sensitive information like login credentials or credit card details, which are then exploited by the attacker. These QR codes often promise cashbacks, discounts, or special offers to lure unsuspecting individuals.
- Stock trading scam: Fraudsters lure victims through social media platforms with promises of high returns. Using fake profiles, apps, and WhatsApp groups, they build trust with potential victims before blocking withdrawals.

DOI: 10.48175/568

- UPI-related Scams:A May 2023 report from Business Standard reveals that UPI-related scams dominate digital payment frauds in India, making up 55% of reported cases. In comparison, card-related scams account for 18%, internet banking for 12%, and phishing calls for 9%. Despite the high frequency of UPI frauds, most involve small amounts, with 50% having an average transaction size below ₹10,000.The report highlights the increasing popularity of UPI, which accounted for 57% of non-cash retail transactions in FY22, and is projected to contribute to a 74% growth in digital payments by 2027. This surge in digitization creates new opportunities for fraudsters, particularly in identity-related scams.
- Voice-Cloning and Deepfake Scams Using AI: A McAfee report reveals that 83% of Indians have lost money to AI voice scams, with 48% losing over ₹50,000. Scammers use AI technology to mimic the voices of family members in distress, leading to an alarming number of victims. The survey, titled "The Artificial Imposter," indicates that 69% of Indians struggle to distinguish between AI-generated and real voices, contributing to the rise of these scams. Cybercriminals can clone voices with just three seconds of audio, fuelling the proliferation of online voice scams. This technology poses significant dangers as voices are as unique as biometric fingerprints. With 86% of Indian adults sharing voice data online weekly, this vulnerability is heavily exploited by fraudsters.

The report also reveals that 66% of Indian respondents would respond to voice messages purportedly from loved ones in need, demonstrating the effectiveness of these scams. Additionally, concerns over deepfakes and disinformation have heightened distrust in social media platforms, with 27% of Indian adults becoming less trusting and 43% expressing concerns about misinformation.

This alarming trend underscores the need for increased awareness and caution when dealing with voice messages and online communications.

4.5 The key findings from the secondary data collected:

- Cyber Threat Landscape: The banking sector faces a multitude of cyber threats, including ransomware, malware, phishing, insider threats, and social engineering attacks.
- Impact on Financial Institutions: Cybercrimes lead to financial losses, operational disruptions, and reputational damage for banks. Regulatory penalties and increased operational costs are also significant concerns.
- Impact on Customers: Customers suffer from financial loss, identity theft, and the inconvenience of recovering stolen funds or restoring credit ratings.
- Cybercrime Trends: Recent trends indicate an increase in sophisticated cyber-attacks such as SIM-swap fraud, OTP fraud, stock trading scam and AI-driven scams like voice-cloning.

Recommendations for mitigating risks(Mitigation Strategies)

To effectively mitigate cyber security risks, financial institutions can implement the following measures:

Implement Strong Access Controls and Authentication Mechanisms:

- Utilize multi-factor authentication to verify user identities and restrict access to sensitive information.
- Restrict access to sensitive information to authorized personnel only.
- Regularly review and update access controls to ensure their effectiveness.

Conduct Regular Risk Assessments:

- Perform ongoing risk assessments to identify vulnerabilities within systems and networks.
- Use the results to prioritize cyber security efforts and allocate resources efficiently.

Educate employeeson cyber security best practices:

- Provide comprehensive training on identifying and avoiding phishing attacks.
- Teach employees how to create strong passwords and recognize suspicious activities.
- Conduct regular training sessions and awareness programs to keep cyber security practices top of mind.

Use Encryption and Data Protection: Implement robust encryption protocols and secure data storage.

- Apply encryption protocols for sensitive data both in transit and at rest.
- Ensure all data is stored securely to prevent unauthorized access.

DOI: 10.48175/568

Monitor Systems Continuously: Establish systems to detect and respond to suspicious activities in real-time.

- Set up monitoring systems to detect unauthorized access attempts, malware infections, and unusual traffic patterns.
- Early detection of threats can help prevent data breaches and cyber-attacks.

Develop Incident Response Plans:

- Prepare and regularly update response plans to minimize the impact of cyber security incidents.
- Include procedures for identifying the cause, containing the damage, and notifying customers and stakeholders.
- Collaborate with Industry Partners: Work with other financial institutions and regulatory bodies to share information and develop best practices for mitigating cyber security risks across the financial sector.

Leverage Automation and Machine Learning:

- Use automation and machine learning to quickly and accurately identify and respond to threats.
- Employ machine learning to detect patterns and anomalies indicating potential threats.
- Automate the patching of vulnerabilities to enhance security posture.

Implementing these strategies will help financial institutions strengthen their cyber security defenses and protect against evolving threats.

4.7 Indian Government's Cybercrime Combat Efforts: Key Highlights

The Government of India has implemented numerous initiatives to combat cybercrime effectively. Here are some key measures and their impacts:

National Cyber Crime Portal and Helpline:

- The National Cyber Crime Portal (cybercrime.gov.in) was launched to report cyber threats and attacks.
- A dedicated helpline number, 1930, was introduced to address the rising instances of cyber financial frauds.

Strategies and Actions: Various strategies have been put in place, including blocking IMEI numbers and websites associated with cybercrime activities.

Impact of the National Cybercrime Reporting Portal: Since its inception in August 2019, the portal has received over 3.26 million complaints, leading to the filing of 66,000 FIRs.

Financial Recovery and Coordination:

- Between 2021 and 2023, over ₹1,127 crore belonging to 430,000 victims was recovered.
- More than 263 banks and e-commerce companies have been integrated with the 1930 helpline to enhance coordination. This integration enables real-time actions such as restricting fraudulent funds and marking lien-money.

Technological Integration:

- The National Cybercrime Reporting Portal is integrated with the Crime and Criminal Tracking Network and Systems (CCTNS) to streamline FIR filing and avoid duplication.
- The National Automated Fingerprint Identification System (NAFIS) supports interstate identification of cybercriminals.

Telecom Regulation: The Department of Telecommunications (DoT) has initiated measures like blocking IMEI numbers and implementing stricter Know Your Customer (KYC) norms for SIM card sales to curb cybercrime activities

These initiatives highlight the Indian government's proactive approach to combating cybercrime and protecting citizens from digital threats.

DOI: 10.48175/568

V. CONCLUSION

The digitalization of the banking sector has brought significant benefits but also increased cyber security risks. Financial institutions must adopt a proactive approach to cyber security, implementing robust security measures, educating employees, and collaborating with industry partners to effectively mitigate these risks. By doing so, banks can protect their operations, maintain customer trust, and ensure the stability of the financial system. This report provides a detailed analysis of cyber security threats in the banking sector and offers actionable recommendations to enhance security and resilience against cyber-attacks.

REFERENCES

[1]. RBI Annual Report 2023-2024

[2]. https://www.npci.org.in/

[3]. https://www.cert-in.org.in/

[4]. Report from Indian Cyber Coordination Centre (I4C), 2023

[5]. https://www.cybercrime.gov.in/

[6] Indian Cyber Crime Coordination Centre, I4C, Report 2023-2024

[7] Article "Here is how much Indians lost to cyber frauds between Jan and Apr of 2024", Business Standard, 27.05.2024

[8] Article "Online fraud: A raging menace," India Today, 30.10.2023

DOI: 10.48175/568