Digital era of banking with special reference to cyber crime a critical study

Payal malik

Abstract

Customers are now able to access banking services via a variety of digital channels, including mobile devices, personal computers, and automated teller machines (ATMs). This is a direct result of the advent of the digital age. On the other hand, this transition has also resulted in a rise in cybercrime, as hackers and other cybercriminals have begun targeting financial institutions and their clients in order to steal, commit fraud, and engage in other illegal acts. the digital age of banking presents an overview of the digital banking environment, covering the many sorts of digital services supplied by banks and the benefits they bring to clients. a specific reference is made to cybercrime. phishing, spyware, identity theft, and ransomware are just some of the many forms of cybercrime that are rampant in the banking business.

Keywords digital banking, cybercrime, phishing, malware, identity theft, ransomware, cybersecurity

Introduction

The proliferation of digital technology has fundamentally altered the banking sector by providing clients with access to a variety of financial services through digital mediums such as mobile devices, personal computers, and automated teller machines (ATMs). There are a great number of advantages to using digital banking, some of which include greater convenience, expanded access to various financial services, and higher safety precautions. On the other hand, this transition has also led to an increase in cybercrime. Hackers and other cybercriminals are taking advantage of weaknesses in the digital ecosystem in order to steal from banks and their clients, swindle banks, or compromise their assets in some other way. the age of digital banking, with a particular emphasis on online criminal activity. This article examines the many kinds of digital services that banks give to their clients and the advantages that these services provide to those consumers. phishing, spyware, identity theft, and ransomware are just some of the forms of cybercrime that are plaguing the banking sector. the efforts that banks are doing to avoid and minimise the effects of cybercrime, such as investing in systems designed to protect against cyber risks and educating workers on how to recognise and react to cyber threats. the difficulties that banks must overcome in order to combat cybercrime, as well as the need of maintaining vigilance in order to shield client information and financial assets from the hands of hackers.

The frequency and level of complexity of cyberattacks on financial institutions have both grown, which has resulted in large financial losses, harm to reputation, and regulatory fines. Because of this, cybersecurity has evolved into one of the most pressing concerns for financial institutions and government authorities all over the globe. The need of preventing and mitigating the effects of cybercrime has led to a rise in expenditures in technology designed to protect against cyberattacks as well as staff training programmes designed to make people more aware of the dangers posed by the internet. The move towards open banking, which includes the sharing of financial data and services with third-party providers, has resulted in the introduction of new cyber threats and vulnerabilities. In response, regulators are working to develop laws and standards with the goals of promoting the secure exchange of data and minimising the dangers that are connected with open banking. Customers now have better convenience and access to financial services thanks to the advent of the digital age in banking, which has caused a revolution in the financial services business. On the other hand, it has also resulted in a rise in cybercrime, which presents substantial hurdles to banking authorities and financial institutions. It is vital for banks to maintain vigilance, invest in cybersecurity technology, and regularly educate their workers to recognise and react to cyber threats in order to preserve the safety and security of their customers' data as well as their customers' financial assets.

- **Digital Banking Landscape**
- **Types of Cybercrime in Banking**
- **Preventing and Mitigating Cybercrime**
- **Investments in Cybersecurity**
- **Employee Training**
- **Challenges in Fighting Cybercrime**
- **Open Banking Risks and Regulations**

Digital Banking Landscape

The term digital banking landscape refers to the myriad of different digital services and channels that banks make available to their respective consumers. Users will be able to carry out a wide range of banking tasks either online, through mobile devices, or at automated teller machines (ATMs) thanks to these services, which are intended to make banking more convenient and easier to access for customers. Online banking, mobile banking, and digital wallets are all examples of services provided by digital banks. Customers have the ability to

access their bank accounts, check their balances, examine their transaction histories, transfer money, pay bills, and engage in a variety of other banking activities via the website of their financial institution when they use online banking. Mobile banking provides the same services as traditional banking, except they are accessed through an application on a mobile device. Customers are able to use their mobile devices to make payments when they have a digital wallet on their device, such as Apple Pay or Google Pay. Customers have the ability to withdraw cash, deposit checks, or transfer payments at any time, regardless of the bank's operating hours, thanks to the availability of automated teller machines, often known as ATMs. In addition, financial institutions are increasingly turning to chatbots and other applications powered by artificial intelligence in order to offer customer service and automate various banking processes.

The world of digital banking has quickly evolved, which has resulted in a transformation in how clients engage with their banks. These digital services have opened up new doors for banks, allowing them to more effectively communicate with clients and provide services that bring value. However, as a result of this, new cyber risks and vulnerabilities have been created. As a result, it is very necessary for banks to prioritise cybersecurity in order to secure the data and assets of their clients.

Types of Cybercrime in Banking

The illicit use of computer networks, the Internet, or other forms of digital technology is an example of the sort of criminal activity known as cybercrime. It may be as easy as gaining unauthorised access to computer systems or as complicated as launching a sophisticated cyberattack, either of which can result in the loss of data, fraudulent financial activity, or other catastrophic repercussions. Hacking, phishing, identity theft, ransomware assaults, malware distribution, and distributed denial-of-service (DDoS) attacks are only some of the types of criminal actions that fall under the umbrella of cybercrime. Typically, people or groups of persons that have specialised knowledge and abilities in computer technology and are motivated by financial gain, political goals, or personal fulfilment are the ones who carry out these actions. Not only can cybercrime have a big influence on the people who are directly impacted by it, but it may also have a significant impact on companies, governments, and society as a whole. Cybercrime may lead to a variety of negative outcomes, including monetary losses, damage to reputations, loss of intellectual property, and even, in extreme instances, bodily violence. In order to combat cybercrime, governments, law enforcement agencies, and

businesses have implemented a variety of measures, such as stronger encryption and authentication methods, more stringent cybersecurity laws and regulations, and cybersecurity awareness training for both employees and the general public. The battle against cybercrime, on the other hand, will continue to be a difficult one so long as technology continues to advance.

There are several types of cybercrime that are prevalent in the banking industry. These cyber threats can be carried out by individuals, criminal organizations, or state-sponsored actors. Some of the most common types of cybercrime in banking include:

- **Phishing:** This is the act of sending fraudulent emails or messages that appear to be from a legitimate source, with the intention of tricking recipients into providing sensitive information, such as passwords or credit card details.
- **Malware:** Malware is a type of malicious software that can infect a computer or mobile device, allowing attackers to steal data or gain unauthorized access to systems.
- Identity theft: Identity theft involves the use of stolen personal information, such as names, addresses, or social security numbers, to open fraudulent accounts or obtain credit in someone else's name.
- **Ransomware:** Ransomware is a type of malware that encrypts files on a victim's computer, preventing them from accessing their data until a ransom is paid.
- Insider threats: Insider threats refer to attacks carried out by individuals who have authorized access to a bank's systems or data, such as employees or contractors.
- **Distributed Denial of Service (DDoS) attacks:** DDoS attacks involve overwhelming a website or network with traffic, causing it to crash or become inaccessible to legitimate users.
- **Social engineering:** Social engineering involves using deception to manipulate individuals into divulging confidential information or performing actions that are detrimental to the bank or its customers.
- **ATM skimming:** ATM skimming involves the use of a device attached to an ATM to steal customer data, such as credit card numbers and PINs, when they are used to withdraw cash.
- **Credential stuffing:** Credential stuffing involves the use of stolen usernames and passwords to gain unauthorized access to bank accounts or other online services.

- **Advanced persistent threats (APTs):** APTs are sophisticated and long-term cyber attacks that involve a combination of techniques, such as social engineering, malware, and other advanced tactics, to gain access to sensitive data or systems.

These types of cybercrime pose significant risks to banks and their customers, and it is essential for banks to stay vigilant and adapt to emerging threats in the constantly evolving landscape of cybersecurity.

Preventing and Mitigating Cybercrime

Preventing and mitigating cybercrime is critical for banks to protect their customers' data and assets. Banks use a variety of measures to prevent cyber attacks and to respond effectively to any attacks that do occur.

- **Investments in cybersecurity:** Banks invest heavily in cybersecurity technologies and infrastructure, such as firewalls, intrusion detection and prevention systems, and encryption, to protect their systems and customer data.
- **Employee training**: Banks provide regular cybersecurity training to their employees to raise awareness of cyber risks and to teach them how to identify and respond to cyber threats.
- **Multi-factor authentication:** Banks require customers to provide multiple forms of identification, such as passwords, security tokens, or biometrics, to access their accounts, providing an additional layer of security.
- **Incident response planning:** Banks develop detailed incident response plans to identify and respond to cyber attacks promptly, minimizing the impact of any attacks that do occur.
- **Third-party risk management:** Banks assess and manage the risks posed by third-party vendors, such as cloud providers or payment processors, with access to their systems or data.
- **Regular security assessments:** Banks conduct regular security assessments to identify vulnerabilities in their systems and networks, and to implement measures to address any weaknesses.
- **Encryption**: Banks use encryption to secure sensitive data, such as customer information, financial transactions, and communications, to prevent unauthorized access.

- **Access controls**: Banks limit access to sensitive data and systems, implementing strict access controls and requiring authorization for privileged actions, such as system changes or data access.
- **Security audits:** Banks conduct regular security audits to evaluate their cybersecurity posture and identify potential weaknesses or gaps in their security measures.
- **Information sharing:** Banks collaborate with industry peers, government agencies, and other stakeholders to share information on emerging cyber threats and best practices for preventing and mitigating cybercrime.
- **Continuous monitoring**: Banks continuously monitor their systems and networks for suspicious activity, using tools such as intrusion detection systems and security analytics to detect and respond to cyber threats.

By implementing these preventive and mitigating measures, banks can enhance their cybersecurity posture and protect themselves and their customers from cybercrime. It is important for banks to maintain a proactive approach to cybersecurity, continually assessing and improving their security measures to stay ahead of emerging threats.

Investments in Cybersecurity

Investments in cybersecurity are critical for banks to protect their systems and customer data from cyber threats. Banks invest in cybersecurity technologies, infrastructure, and personnel to prevent cyber attacks and respond effectively to any attacks that do occur. Some of the ways banks invest in cybersecurity include:

- **Cybersecurity technologies**: Banks invest in advanced cybersecurity technologies, such as firewalls, intrusion detection and prevention systems, and security information and event management (SIEM) solutions, to protect their systems and data from cyber threats.
- **Security operations centers (SOCs):** Banks establish SOCs, which are dedicated teams responsible for monitoring and responding to cyber threats, to ensure that any incidents are detected and addressed quickly.
- **Third-party security assessments:** Banks conduct security assessments of their third-party vendors, such as cloud providers and payment processors, to ensure that they maintain robust cybersecurity measures.
- **Cybersecurity insurance:** Banks purchase cybersecurity insurance to provide financial protection in the event of a cyber attack.

- **Cybersecurity personnel**: Banks hire cybersecurity professionals with specialized skills and expertise to manage their cybersecurity operations and respond to cyber incidents.

Investments in cybersecurity are critical for banks to protect their customers' data and assets from cybercrime. Banks must continue to prioritize cybersecurity investments to stay ahead of emerging threats and to maintain a robust cybersecurity posture

Employee training

Training for workers is an essential component of making an industry as secure as banking as possible from the threat of cybercrime. When it comes to cybersecurity, a bank's personnel might be a weak link in the chain if they are not effectively prepared to recognise and react to cyber threats. Cyber attacks offer considerable dangers to both banks and the clients they serve. this problem, banks often give their workers with opportunities to improve their cybersecurity skills. The purpose of this training is to increase workers' knowledge of potential cyber hazards and to educate them how to effectively recognise and react to cyber attacks. A range of training approaches, such as general awareness training, role-specific training, incident response training, phishing simulation exercises, and continuing training, are used by financial institutions such as banks. Banks may lower the likelihood of cyber attacks and lessen the effect of any assaults that do occur if they provide regular cybersecurity training to their workers. Employees who have received enough training in cybersecurity are in a better position to recognise and react appropriately to cyber threats. This lowers the probability that an attack will be successful and lessens the severity of any assaults that do take place.

- **Awareness training**: Banks provide general cybersecurity awareness training to all employees, teaching them about common cyber threats, such as phishing and malware, and how to prevent them.
- **Role-specific training:** Banks provide role-specific training to employees who handle sensitive data or have privileged access to systems, teaching them how to identify and respond to specific cyber threats.
- **Incident response training**: Banks provide incident response training to employees, teaching them how to identify and respond to cyber incidents effectively.
- **Phishing simulation:** Banks conduct phishing simulation exercises to test employees' susceptibility to phishing attacks and to provide targeted training to those who need it.

- **Ongoing training:** Banks provide ongoing cybersecurity training to employees, keeping them up to date with the latest cyber threats and mitigation techniques.

Challenges in Fighting Cybercrime

Due to the continuously shifting nature of the threat environment and the increasingly sophisticated nature of cyberattacks, combating cybercrime in the banking sector is a difficult and complicated undertaking. For banks to be successful in their fight against cybercrime, they will need to surmount a number of obstacles. Cost is one of the most major problems, since it may be costly to invest in cybersecurity technology and infrastructure, especially for smaller banks. This is one of the most critical challenges. In addition, the costs associated with reacting to cyber disasters, such as legal bills and harm to a company's brand, may be very high. The complexity of cyber security is still another obstacle, since it calls for the application of specific knowledge and abilities in order to be managed properly. Particularly difficult for smaller banks that have less resources to devote to research and development is maintaining a state of awareness about newly emerging dangers and new technological developments. In addition to external threats, insider threats, risks posed by third parties, regulatory issues, and cultural hurdles are key obstacles that banks must overcome in their fight against cybercrime. These difficulties call for a strategy that combines many strategies, including investments in cybersecurity technology and staff, the development of efficient rules and processes, and the promotion of a culture that emphasises knowledge of and responsibility for cybersecurity issues. The banking sector has tremendous obstacles when attempting to combat cybercrime, but with the appropriate policies and investments, financial institutions can continue to safeguard the data and assets of their clients from the effects of cyberattacks.

- **Cost**: Investing in cybersecurity technologies and infrastructure can be expensive, especially for smaller banks. Additionally, the cost of responding to cyber incidents can be significant, including legal fees, customer notification costs, and reputational damage.
- **Complexity**: Cybersecurity is a complex and constantly evolving field, requiring specialized skills and expertise to manage effectively. Keeping up with emerging threats and new technologies can be a daunting task, especially for smaller banks with limited resources.
- **Insider threats**: Insider threats, such as employees or contractors with authorized access to systems or data, can be challenging to detect and prevent.

- **Third-party risks**: Banks rely on third-party vendors for a variety of services, including cloud providers and payment processors, and these vendors can introduce additional cyber risks.
- **Compliance**: Banks must comply with a range of cybersecurity regulations and guidelines, which can be complex and time-consuming to implement and maintain.
- **Cultural barriers:** Some employees may view cybersecurity as an obstacle to productivity, rather than a necessary aspect of their job. This can lead to resistance to implementing cybersecurity measures and a lack of buy-in from employees

Open Banking Risks and Regulations

Open banking is a system that allows third-party financial service providers to access customer financial data, with the aim of increasing competition and innovation in the banking industry. While open banking offers many benefits, it also introduces new risks that must be addressed.

Some of the risks associated with open banking include:

- **Data privacy and security risks:** Open banking requires the sharing of sensitive customer data with third-party service providers, increasing the risk of data breaches and cyber attacks.
- **Fraud risks**: Open banking increases the risk of fraud, as third-party providers may not have the same level of security measures in place as banks.
- **Reputation risks:** Banks that participate in open banking risk damaging their reputation if a third-party provider experiences a security breach or engages in fraudulent activity.
- **Regulatory risks:** Open banking is subject to a range of regulations and guidelines, and banks must ensure that they comply with these regulations to avoid penalties and reputational damage.

in order to mitigate these risks, authorities have enacted a variety of laws and standards, some examples of which are the Payment Services Directive 2 (PSD2) in Europe and the Open Banking Standard in the UK. In order to comply with these rules, financial institutions must employ stringent client authentication procedures, data security safeguards, and secure data-sharing protocols. Additionally, banks are required to undertake due diligence on third-party service providers, checking to see whether or not these companies uphold the same level of

safety standards as the bank itself. In addition, financial institutions have to put in place mechanisms for the identification and prevention of fraud, such as the monitoring of transactions and the discovery of anomalies. Even while open banking introduces new dangers, financial institutions have the ability to reduce these dangers by strengthening their security protocols and adhering to all applicable rules and laws. By acting in this manner, banks will be able to take part in the open banking system while still shielding the data and assets of their clients from potential cyberattacks.

Review of literature

Chen and Wen (2017) studied "a survey of banking customers in Taiwan to assess their perceptions of cybercrime and their attitudes towards online banking" discovered that this, along with consumers' perceptions of their own security and trust, was the most critical factor in determining whether or not they would use online banking services.

Kamal and Al-Harbi (2018) studied "a study on the impact of cybercrime on the reputation and brand equity of banks in india" According to the findings of the study, incidents of cybercrime can have a significant detrimental effect on the reputation and brand equity of financial institutions. However, preventative measures such as efficient crisis management and communication strategies can help mitigate the risks associated with these occurrences.

Kumar and Jain (2019) studied "a study on the role of social media in cybercrime targeting the banking industry" found that criminals are increasingly using social media platforms to carry out phishing attacks and other types of cybercrime, and that banks need to be vigilant and proactive in monitoring and responding to these threats. [Cyber] criminals are increasingly using social media platforms to carry out phishing attacks and other types of cybercrime.

Alruban et al. (2021) studied "a study on the effectiveness of cyber risk management practices in the banking industry in India" discovered that although many financial institutions are adopting best practises for cyber risk management, such as building security frameworks and performing frequent risk assessments, but that there is still space for improvement in areas such as staff training and incident response plans.

(Day 2002) studied "Impact of Cyber Crimes on Technology Enabled Banking Services" The Indian banking business relies heavily on information technology, both for the processing of transactions and for the implementation of a wide range of additional internal systems and operations. The banks' approach to reporting transactions and the manner in which interbank

transactions and clearing are conducted have both changed dramatically over the years, and banks now have access to a wide range of technological platforms on which to carry out their day-to-day operations. Technology in banking and finance is shown in the meteoric rise of online transactions enabled by services such as the National Electronic Fund Transfer (NEFT), the Real-time Gross Settlement Systems (RTGS), the Electronic Clearing Service (ECS), and mobile transactions. As the use of computers and the internet has spread rapidly, a new category of international crime has emerged: cybercrime. According to William Duer's research, 40% of cyberattacks target retail banks. The financial services industry has its own unique set of problems. Financial institutions are actively pursuing the decentralisation of their services by means of digitalization. Criminals and hackers often attack banks and other financial organisations. All industries have been hit by Ransomware attacks recently, and each one has been viewed as if it were a major assault on the whole economy. The effects of cybercrime on the financial industry and strategies for preventing such attacks in the future are the primary topics of this article.

(Dutt and Chaudhary 2013) studied "CYBERCRIME: THE TRANSITION OF CRIME IN THE INFORMATION ERA" Companies, colleges, and other institutions have reason to be concerned about the rise in sophistication and frequency of computer crime, often known as Cybercrime. The world's governments, police forces, and intelligence agencies have begun to respond. Because it has its roots in actual urbanisation, police-based enforcement does not and cannot use digital technology to protect its citizens from criminals. Information necessary to run our enterprises, government, national defence, and other essential services is provided in this article. As the incidence and severity of cybercrime continues to rise, we must reconsider how we apply existing criminal laws. How the current, reactive paradigm of cybercrime, cybercrime kinds, cybercrime modes, and security measures, including blockages, fail to successfully combat cybercrime. It demonstrates the urgent need to reevaluate current methods of combating this emerging kind of cybercrime in the IT sector. While it's hard to completely eliminate cybercrime, raising awareness among the general public may help cut down on it significantly. We propose an incentive-based system of administrative control and criminal punishments to reduce cybercrime effectively.

(Neeta 2019) studied "Cyber Crimes In Banking Sector" E-banking, sometimes known as online banking, is the practise of conducting financial transactions through the Internet. In the past, customers had to wait in a lengthy line only to withdraw their money or do other menial banking tasks. The distance between the bank and the consumer has shrunk because to the

advent of 24-hour banking services provided by ATMs (Automated Teller Machines), online banking, transfer through NEFT and RTGS, etc. The scope of e-banking extends beyond the provision of financial services through IT infrastructure. With the proliferation of smartphones in the current age, e-banking has expanded to include mobile banking. E-banking services were first introduced because liberalisation, privatisation, and globalisation made it such that banks needed them. The purpose of this article is to introduce the reader to the notion of electronic banking and the benefits it offers in India. The author will also give data showing the meteoric rise in popularity of online banking in India. The study will also focus on the Reserve Bank of India and its efforts to improve online banking in India. With the use of data on cybercrime recorded over the previous several years, will next go into the downsides of e-banking by outlining numerous cyber-crimes connected to banking, with a particular emphasis on the Information Technology Act, 2000. The author will conclude by emphasising the importance of the Cyber Appellate Authority in the fight against cyber-crime in the financial industry. The bank's and the customer's respective responsibilities in this regard will be explained. At last, the author will advise on the precautions both the consumer and the bank should take while conducting business online.

(KALPANA 2020) studied “CYBER CRIME: A GROWING THREAT TO INDIAN E-BANKING SECTOR” Exchange of data and word-of-mouth Technology is now fundamental to how we function. Broadband internet and smartphones have made it possible for almost everyone to get online, creating a global network of what amounts to millions of people. As our reliance on the internet grows, so do the risks of becoming a victim of cybercrime. Even a little lapse in digital hygiene might leave us vulnerable to fraud and financial loss. Therefore, we must be watchful and cautious whenever we use any kind of digital connection to the outside world, whether for monetary transactions, social networking, playing games, looking for items online, etc. This article gives readers an overview of cybercrime in the E-banking industry and some basic advice for avoiding becoming a victim.

(Gaokar and Tundejwala 2021) studied “Cyber Crime in Online Banking” Security is of paramount importance in today's highly digitalized environment. Most of our errands, including shopping, office work, e-banking, other transactions, etc., may be accomplished with the aid of the internet. With mobile banking, everyone can make transactions and purchase online, but most people are unaware of the risks involved in doing so. Hackers and cybercriminals take advantage of this lack of awareness in cyber security. By 2020, instant payments and other electronic payments had captured 15.6% and 22.9% of India's transaction

volume share, respectively; -based payments nevertheless accounted for a sizeable 61.4%. The proportion of all transactions conducted electronically is projected to rise to 51.9% by 2024 and to 71.7% by 2025. India is a growing nation that is making strides in the realm of information technology. During this time, it will become more difficult to safeguard any information or financial transactions conducted online. Although online banking saves time and is more convenient, it is not secure and cannot be trusted completely. And the rate of growth of cybercrime is astonishing. The key topics covered in this research include banking frauds in India, e-banking problems, online transactions, and the experiences of cybercrime victims. Cybersecurity and methods for preventing most forms of online banking fraud are also discussed.

(Sravika 2022) studied "A Study on Cyber Security Issue Affecting Banking And Online Transactions" Internet banking, sometimes known as online banking, has been one of the most game-changing innovations of the twenty-first century. Because of his social nature, it is crucial for man to be able to share and learn from the experiences of others. With the development of e-banking technology, completing a transaction takes no more than a few mouse clicks. With the advent of online and mobile banking, managing one's finances is now a breeze. There has been a rise in cybercrime on a global scale due to people abusing their access to computers online. There is a greater potential for harm and more difficult obstacles to overcome. But there is no such thing as completely secure mobile or internet banking. This study aims to provide an overview of cyber assaults. In this article, we explored the latest hacking methods and how they relate to online banking fraud. This research relied only on already published literature. This study's results highlight the increasing prevalence of both online banking-related criminality and the use of information technology in India. Young adults between the ages of 18 and 30 (especially young men) perpetrate the vast majority of cybercrimes. Our judicial system needs better tools to combat and prevent cybercrime. In conclusion, the study's authors provide some recommendations for the secure and preventative usage of electronic banking.

conclusion

Customers now have access to user-friendly and time-saving methods of managing their financial affairs as a direct result of the digital transformation that has taken place in the banking business. On the other hand, this progress in technology has also resulted in a surge in cybercrime, as criminals online continue to take advantage of loopholes in financial systems in order to engage in unlawful operations. Because it may result in monetary losses, theft of data,

and other catastrophic repercussions, cybercrime in the banking industry constitutes a substantial danger to people, organisations, and society as a whole. Financial institutions have introduced a variety of security measures, such as two-factor authentication, encryption, and fraud monitoring systems, in order to address the increasing threat posed by cybercrime. The battle against cybercrime is a never-ending struggle, despite the fact that these preventative measures have shown to be successful in preventing cybercrime to some level. In order to stay up with the ever-evolving dangers posed by cyberspace, ongoing innovation and adaptability are required. To safeguard the safety and security of the digital banking ecosystem, it is also necessary for financial institutions, governments, and law enforcement agencies to work together. The transition from analogue to digital banking has been accompanied by a proliferation of advantages, but it has also given rise to a new set of difficulties in the shape of cybercrime. It is very necessary for us to maintain vigilance in the protection of our sensitive information and to keep knowledgeable on the most recent cybersecurity dangers and best practises as we continue to depend more and more on digital technology in our day-to-day lives.

References

- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.007
- Smith, J. A., & Moorthy, K. S. (2017). Cybersecurity and financial institutions: A practical guide to implementing robust cybersecurity policies and procedures. John Wiley & Sons.
- Verma, R., Sinha, R. K., & Kaur, R. (2020). Cybercrime and cybersecurity in the banking sector: A review of literature. Journal of Money Laundering Control, 23(1), 44-62. https://doi.org/10.1108/JMLC-07-2019-0068
- World Economic Forum. (2019). Cybercrime prevention principles for banks. https://www.weforum.org/whitepapers/cybercrime-prevention-principles-for-banks
- Yoo, C. Y., & Lee, H. (2020). How do cybersecurity investments affect bank performance? Journal of Business Research, 107, 230-240. https://doi.org/10.1016/j.jbusres.2019.10.040
- Chen, D., Sharma, S. K., Zhang, J., & Kumar, V. (2019). Blockchain and cybersecurity: A survey. International Journal of Information Management, 46, 216-229. https://doi.org/10.1016/j.ijinfomgt.2018.10.011

- International Monetary Fund. (2018). Fintech and financial services: Initial considerations. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/09/28/Fintech-and-Financial-Services-Initial-Considerations-46233
- Jones, S. (2020). The impact of COVID-19 on cybersecurity: A review. Journal of Cybersecurity, 6(1), taaa032. https://doi.org/10.1093/cybsec/taaa032
- Kaspersky. (2021). Financial threat landscape 2020. https://securelist.com/financial-threat-landscape-2020/99992/
- World Bank Group. (2021). Cybersecurity diagnostic for the financial sector. https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-diagnostic-for-the-financial-sector
- European Central Bank. (2021). Cyber resilience: Oversight expectations for financial market infrastructures. https://www.ecb.europa.eu/paym/pdf/cyber_resilience_oversight_expectations_for_financial_market_infrastructures_202101.en.pdf
- Gartner. (2021). Top 10 security projects for 2021. https://www.gartner.com/smarterwithgartner/top-10-security-projects-for-2021/
- McAfee. (2020). Economic impact of cybercrime – No slowing down. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/economic-impact-cybercrime-no-slowing/
- National Institute of Standards and Technology. (2020). Cybersecurity framework. https://www.nist.gov/cyberframework
- Ponemon Institute. (2021). The cost of cybercrime study. https://www.ibm.com/security/digital-assets/cost-of-cybercrime-study/
- Day, Terry. 2002. Management Today. *Fire Engineers Journal* 62(227):44–45. doi: 10.4324/9781003166740-1.
- Dutt, Shailza, and Asha Chaudhary. 2013. Cybercrime: The Transition of Crime in the Information Era. *International Journal of Advanced Research in IT and Engineering* 2(6):27–37.
- Gaokar, Vihang Dilip, and Karan Harish Tundejwala. 2021. Cyber Crime in Online Banking. *International Journal of Advanced Research in Science, Communication and Technology* 7(1):377–79. doi: 10.48175/ijarsct-1659.
- KALPANA, : Mrs. S. 2020. Cyber Crime – a Growing Threat to Financial Institutions. 7(12):964–69.

- Neeta, Ms. 2019. Cyber Crimes In Banking Sector. (25):25–31.
- Sravika, M. 2022. A Study on Cyber Security Issue Affecting Banking And Online Transactions. 8(8):58–63.