International Journal of Research Publication and Reviews

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

SAFEGUARDING THE FINANCIAL SECTOR: NAVIGATING CYBER RISKS IN A DIGITAL ERA

AMAN SINGH

Student, LL.M. (Criminal and security laws), Gujarat National Law University Gandhinagar (GJ) Email ID: apal5483@gmail.com

ABSTRACT

The global financial sector faces a complex array of challenges stemming from macroeconomic shifts and technological advancements. With the proliferation of multimedia tools, financial institutions are reevaluating their risk management processes to effectively navigate the evolving landscape. However, the rise of technology, coupled with increased mobile usage, has expanded the reach of financial services to the general public, consequently exposing them to heightened cybercrime risks. Cyberattacks have become increasingly sophisticated, resulting in substantial financial losses for institutions worldwide. Despite efforts to mitigate these risks, the financial industry continues to grapple with substantial monetary losses, prolonged recovery times, and operational disruptions following cyber incidents. Various forms of cyber threats, including hacking, phishing, malware, and online fraud, pose significant challenges to the integrity and security of financial systems. Moreover, cybercrime has become a pervasive issue globally, with substantial increases in reported incidents and arrests in recent years. In response, financial institutions are prioritizing cybersecurity measures to protect both their assets and their customers' sensitive information. Effective strategies include enhancing surveillance, strengthening cybersecurity protocols, and promoting digital literacy among customers. As cyber threats continue to evolve, proactive measures and collaboration between industry stakeholders and law enforcement agencies are essential to safeguarding the integrity of the financial sector and preserving public trust.

INTRODUCTION

The financial sector all over the world is confronting a hard position which is multifaceted due to the international & transnational macro-economic situations. The financial industry is required to assess its existing processes in order to understand & handle its risks efficiently. Multimedia methods have been used for the risk mitigation process. Owing to the rise of Technology, proliferation of mobile operators in daily lives, the finance sector have spread to general public. Yet, this has also raised our chances of being victims of cybercrime. Computer hackers have evolved ultra-fine tactics to not only induce robbery of funds & economics data but also to infiltrate industries & access critical business data which informally damages the financial institutions. Worldwide, USD 114Billion is stolen virtually every year due to cyberattacks, while the expenses foreclosed to counter cyber-attacks is almost double in number i.e. USD 274billion. Banking facilities, on average, require 10 days to completely recoup from a cyber-attack, which increases operational costs. Considering the financial damages incurred by the financial Industry, almost 3.5% damage in capital in contrast to worldwide damage. $ 4 billion is wasted in recuperating from the fraud & USD 3.6 billion is invested to counter such thefts from occurring in future. The estimated duration it takes to solve the fraud in Indian finance industry is considerably greater compared to worldwide scenario i.e. 15 days.

Hacking refers to the act of gaining unauthorised access to a computer system or network with the intention of gaining access to sensitive information. When a customer pays for anything online using a credit card or debit card, fraud occurs when another individual with malicious intent uses the card credentials and password to make unauthorised purchases. With unprotected electronic transactions, hackers can pose as the cardholder and make purchases without their permission. Email fraud occurs when a hacker or malicious organisation sends an email to a bank customer saying something like, "Congratulations, you have won such a huge amount to purchase it, please share your bank details." The recipient of this email then enters his or her credit card number into the vendor's secure website to complete the purchase, giving the hacker access to the victim's account. Customers of financial institutions may be subject to phishing if they get unauthorized communications requesting login credentials such as a username, password, or other personal information.

A computer virus is a piece of software that, once installed, modifies the behaviour of an executable file. Spyware is the most common vector for stealing banking credentials and using them fraudulently. Watering hole is a form of cyber-attack in which malicious code is inserted into publicly accessible areas of a website that receives limited access. When it comes to online banking, malware-based attacks are among the most dangerous cyber risks. With these types of intrusions, harmful code is purposefully created. Within the next year, phishing will serve as the paradigmatic example of the evolving digital risk that banks and their customers face; this is why it has shot up the priority lists of executives, controllers, and law enforcement agencies. Experts have identified four major categories of risk that financial institutions face. To begin, governments utilise surveillance to either steal or somehow undermine banks' intellectual capital. Second, cyber terrorists often target banks as a symbol of western capitalism to denigrate. Third, so-called "hacktivists" regularly try to breach into banks' IT systems, usually to attract more attention to their cause. Cybercrime was ranked as a top economic crime reported by companies around the world in 2014, including in India. There was a 74.3% increase from 2013 to 2014, with 3,301 people arrested for cybercrime in 2013 and 5,752 arrested in 2014. The highest number of such arrests was reportedly in Uttar Pradesh. Cybercrimes have repercussions in the banking industry as well. Finally, organised crime has mostly shifted from stealing money via traditional bank heists to using more sophisticated methods including online, phone, and card deception, all of which are more difficult to detect. The banking industry supports nation's economy. Everyone responsibly takes steps to safeguard bank accounts and personal information. To protect ourselves, we need to stay vigilant and use strong, one-of-a-kind IDs and passwords whenever we're online. Finally, I would like to stress the importance of staying safe online by only visiting reputable, encrypted.

TYPES OF CYBER CRIME IN BANKING SECTOR

1.HACKING

If you try to hack into a customer's banking site or account, you're committing a felony. Hacking refers to the act of gaining unauthorised access to a computer system or network with the intention of gaining access to sensitive information. Under the revised IT Act of 2000, the term "hacking" is not defined. Nonetheless, a hacker may face legal consequences under Section 43(a) read with Section 66of the Information Technology (Amendment) Act, 2008 and Sections 379and 406 of the Indian Penal Code, 1860. Before the 2008 Amendment Act, Section 66 of the IT Act made it possible to get three years in jail for hacking, or a fine of up to two lakhs rupees. If found guilty of a hacking crime, the offender faces up to three years in prison, a fine of up to five lakhs rupees (or both), or both. The crime of hacking is not only considered cognizable, but also bailable.

2.CREDIT CARD FRAUD

When a customer pays for anything online using a credit card or debit card, fraud occurs when another individual with malicious intent uses the card credentials and password to make unauthorised purchases. With unprotected electronic transactions, hackers can pose as the cardholder and make purchases without their permission.

3.EMAIL FRAUD

These days, the Internet and e-mail are the most common and favoured ways to get in touch with people. Email fraud occurs when a hacker or malicious organisation sends an email to a bank customer saying something like, "Congratulations, you have won such a huge amount to purchase it, please share your bank details." The recipient of this email then enters his or her credit card number into the vendor's secure website to complete the purchase, giving the hacker access to the victim's account.

4.PHISHING

There are a lot of scams online that try to separate people from their money, and phishing is only one of them. Customers of financial institutions may be subject to phishing if they get unauthorized communications requesting login credentials such as a username, password, or other personal information.Customers are tricked into giving their personal information by clicking on links in spam emails purporting to be from legitimate financial institutions. By misusing the information fraudulently obtained from the customer, the fraudster gains access to the client's online financial balance and the funds contained in the bank account. According to a report conducted by F-Secure Corporation, the banking industry in India is a prime target for phishing scams during the first half of 2007.

5.VIRUSES

A computer virus is a piece of software that, once installed, modifies the behaviour of an executable file. In order to spread, it infects executable files like apps and operating systems.If you decide to run the programme, you may be re-infecting your computer. Worms, on the other hand, are self-replicating programmes that don't harm or delete files, but rather make copies of themselves and spread them to other systems.

6.SPYWARE

Spyware is the most common vector for stealing banking credentials and using them fraudulently. Spyware is software that monitors your computer for sensitive data as you use it or while you are connected to the Internet. Pop-up adverts that ask you to download software are a common method of invasion. Standard anti-virus software can identify and eliminate such programmes before they can infect a system by preventing their download and installation.

7.WATERING HOLE

Watering hole is sometimes seen as a subset of phishing scams. Watering hole is a form of cyber-attack in which malicious code is inserted into publicly accessible areas of a website that receives limited access. In a watering hole attack scenario, the victim's information is traced by the attacker after they visit a site injected with malicious code.

8.MALWARE BASED-ATTACKS

When it comes to online banking, malware-based attacks are among the most dangerous cyber risks. With these types of intrusions, harmful code is purposefully created. The financial industry is increasingly being targeted by malware. Notable examples of banking malware include Carbep, Tinba, Spyeye, Zeus, and KINS.

9.FINANCIAL FRAUD

According to Financial Fraud in UK, a trade group, losses in Britain due to online and telephone managing account extortion increased by 59 percent, to £35.9 million, in the first half of 2018. The article claims that reports of phishing attacks show that this is one of the most rapidly growing types of extortion. As a result, the financial institutions have requested that the telecom companies in the United Kingdom limit the amount of time that customers can remain on the line after a previous caller has ended. There will be a widespread reduction to two seconds as the new standard by next year, when most telecom providers will have implemented the change. In light of this, the banks in the UK have requested that the telecom companies there limit the amount of time a customer can be on hold before giving up and hanging up. Within the next year, phishing will serve as the paradigmatic example of the evolving digital risk that banks and their customers face; this is why it has shot up the priority lists of executives, controllers, and law enforcement agencies.

10.CYBER SECURITY

Experts have identified four major categories of risk that financial institutions face. To begin, governments utilise surveillance to either steal or somehow undermine banks' intellectual capital. Second, cyber terrorists often target banks as a symbol of western capitalism to denigrate. Third, so-called "hacktivists" regularly try to breach into banks' IT systems, usually to attract more attention to their cause. Finally, organised crime has mostly shifted from stealing money via traditional bank heists to using more sophisticated methods including online, phone, and card deception, all of which are more difficult to detect.

THE EFFECT OF CYBER CRIME IN CURRENT WORLD

FINANCIAL LOSS

Network intrusion detection (N.I.D.) approaches identified spoofing behaviour affecting a service's privacy, accessibility, & authenticity. A technique for categorising distributed denial of service (DDoS) & detecting this together was invented by Fraudster. In this, it was presented a Cloud layer-based DDoS attacks detection method to identify malicious activity in the Network infrastructure. The given resolution utilises grouping as well as a time complexity technique & is done on the OMNeT++ emulator.

Internet baiting is a serious cyber threat, which tends to depend arduously on massive messages, fraud I.D., & the distribution of hazardous links. The objective is that cybercriminals leverage social media to make malicious activity, market associate websites & disseminate virus. Data - sets are a vital feature of cybersecurity research, emphasised by these works. Analysed several cyber - attacks datasets in detail. The truth motivated the analysis that with the expansion of the internet & inventive technology, the method of cyberattacks is also evolving. Thus, to counter this assault, one must first notice them; cybersecurity datasets dissemination and evolution are crucial.

INDIA'S SITUATION

According to both private & public banks, the amount of damage caused by cyberattacks, which includes scams involving ATM/Debit Card, Credit Card, & Online Banking. If a customer reports an unpermitted online payment to the bank within 3 working days of receiving details about the money transfer from the bank, the consumer will have no liability & the bank will credit the sum of the transaction to the customer's account. This policy applies to financial crime involving cards & internet banking.

Furthermore, if the customer notifies the unlawful online payment within 4 to 7 working days, their greatest penalty will be between Rs. 5000 & Rs. 25,000; if they notify it after 7 days, their penalty would be based on the Board's policy.

Banks have the duty to monitor scams on a yearly basis & present a letter to the chairman of the board or local advisory board with information, which may include, among other things, the amount recovered. In order to monitor and follow up on cases of fraud involving sums of Rs 1 crore and above, banks are also required to establish a Special Committee of the Board. This committee will, among other things, keep an eye on the progress of the CBI/Police investigation and the retrieval place in such fraud accounts.

Loss of Production or Production Cost due to Cyber Attacks

A cybercrime is nothing less than a terrible nightmare that keeps a business up at night because it frequently affects them and several times they are unable to even trace its origin. Oftentimes after an attempt, the organisation is unable to view their site or must halt all activity during this period to avoid more harms, therefore it may only take a click or an email to cause them significant harm. In addition, following the attacks, they must disinfect their complete network in order to make it secure once more, & during this time, in addition to potential reputational & goodwill damages, they suffer significant financial losses.

Hackers occasionally employ technologies that allow them to attack multiple businesses simultaneously, which results in a significant loss of output. For instance, the Wanna Cry assault from 2016 was able to simultaneously access numerous computers and networks. Many hospitals and crucial computers were infected, rendering them ineffective and having an impact on the global health care system. The same way, hackers can access account information and simultaneously target numerous corporate accounts.

LEGAL REMEDIES AVAILABLE TO NETIZENS IN INDIA

As long as the severe Indian Penal Code regulations and the Information Technology Act, 2000 provisions are simultaneously enforced, the risk posed by viruses for cyber-attacks can be effectively controlled. In order to try & do the whole justice, judges may combine the rules of different statutes in their discretion. The laws may apply concurrently. In order to regulate cyber-attacks, the Indian Penal Code and the laws of the IT Act are added on. According to claims, the following are covered by the IT Act:

PRIVACY VIOLATION

As stated in Article 21 of the Indian Constitution, the right to life & to private liberty may include the right to privacy. The many clauses of the IT Act 2000 effectively defend netizens' rights to their online privacy. The legal action that can be taken against the malware-using offender. The rules established by the Act may be applied extraterritorially according to Section 1(2) of the IT Act 2000 read with Section 75.

So, under the rules of the IT Act 2000, anyone (including a foreign national) who violates the privacy of an individual using a computer, system, or network that is based in India is accountable. A person's right to privacy is wholly violated when someone's private property is hacked or when someone's creative content is stolen. Although the "right to privacy" is safeguarded by the IPC, the Indian Constitution does not clearly list it as one of the essential rights granted to Indian citizens.

The term "cyber space" refers to an artificial environment made by computers. Citizens, commonly referred to as "netizens," have been progressively using the internet to isolate themselves from their social media network in recent years. Most people have the impression that these folks value their privacy and seek to protect it. In fact, it appears that there is a significant risk of a person's privacy being violated through the internet.

PREVENTION OF DATA AND DATA THEFT:

Provisions of IT Act 2000 handling the information theft under section 43, section 65, Section 66, Section 70 and Section72 may be successfully invoked. Likewise Provisions of ITA Act 2008 under section 43A and section 72A jointly supplemented with section 22 of I.P.C., 1860 & 378 of Indian Penal Code,1860 will be came into effect.

THE CORE OF THIS ACT IS FOUND IN SECTION 43

To interpret this clause in light of numerous cybercrimes, one must be flexible. The first & most important problem brought up by the 2008 amendment has to do with the application of Section 43 of the IT Act of 2000.

Kewal Seth v. Canara Bank

Complainant had account with OP Bank since 2005. OP provided facility of internet banking and provided him internet ID and password for online transactions and he utilized this facility lastly on 7.11.2009. On 21.6.2010, he received call from Manager of OP. Then he went to OP bank and was intimated that someone has internet transactions from his account and has withdrawn Rs. 37,500/- on 17.6.2010 between 12.20 to 01.30 p.m. Manager further informed him that money was transferred firstly in Kamal Verma's Account in OP's Branch at Gurgaon, then transferred to the Account of Zia Mohd. Nazir and Rizwan Pawar in OP's Mira Road Branch and amount was withdrawn through ATM at Vashi.

It was further submitted that Manager assured him that money will be received back, but later on, refused to credit money in his account. It was further submitted that internet banking system used by OP is not full proof, so, money was withdrawn from his account. Alleging deficiency on the part of OP, complainant filed complaint before District forum. OP resisted complaint and submitted that OP offered service of net-banking to complainant after providing internet ID and password. Services provided by OP are certified Very Sign confirming and OP has secured internet banking as per international standards. It was further submitted that complainant was explained precautions to be taken in internet banking. Complainant was responsible for keeping ID and password secretly. Transactions could have been done either by the complainant himself or by the person to whom he provided password, etc. Denying any deficiency on their part, prayed for dismissal of complaint. Learned District forum after hearing both the parties allowed complaint and directed OP to pay Rs. 37,500/- along with cost of Rs. 5,000/-. Appeal filed by OP was dismissed by learned State Commission with cost of Rs. 10,000/- vide impugned order against which, this revision petition has been filed.

PREVENTION OF DISTRIBUTED DENIAL OF SERVICES ATTACK

A virus programme may employ the distributed denial of service (DDOS) tactic to overwhelm users' electronic infrastructure. Hence, the clauses of sections 43, 65, and 66 of the IT Act 2000 will be used jointly to address distributed denial of service attacks that involve virus.

IMPACT OF CYBER CRIME IN BANKING SECTOR

Cases of cybercrime have increased dramatically as the number of mobile devices capable of accessing the internet has risen. Criminals are always on the lookout for new ways to gain access to personal information because smartphones are used for so many different online activities now, including online banking, online shopping, and the payment of utility bills. The most common reason given for perpetrating a cybercrime is financial gain, which has been the case for a long time despite competition from other reasons, such as political purposes, extortion, and the desire for revenge. Despite broad information about how to avoid falling victim to cybercriminals, even the simplest phishing attempts have a startling success rate of 45 percent.

There is no definition of crime or cybercrime in the IPC or the Information Technology Act, 2000; instead, these laws just outline penalties for specific violations. The word "cyber" can mean anything related to computers, computer networks, or computer systems. All forms of criminal activities that include the use of a computer, computer resource, or computer network can be categorised as cybercrime. Douglas and Loader's definition of cybercrime describes any activity facilitated by a computer and carried out across worldwide electronic networks that is viewed as illegal by some.

In order to better understand cybercrime, Wall has broken it down into four distinct types. Internet crimes include phishing, stalking, extortion, and pornographic intrusions. Among the types of fraud that fall under the umbrella of "cyber-deception" are those perpetrated against online banks. Theft, credit card fraud, and IP infringement are all examples of cyber-deception, which is described as an immoral behaviour. Most fraud is conducted for two reasons: (1) to steal the victim's money or personal information, and (2) to move money from one account to another. The second is to damage the bank's reputation by disrupting its server and preventing the customer from accessing his or her account.

India is among the top five countries in terms of the total amount of ransom ware, identity theft, and phishing attacks. Cybercrime was ranked as a top economic crime reported by companies around the world in 2014, including in India. There was a 74.3% increase from 2013 to 2014, with 3,301 people arrested for cybercrime in 2013 and 5,752 arrested in 2014. The highest number of such arrests was reportedly in Uttar Pradesh. Cybercrimes have repercussions in the banking industry as well. The Reserve Bank of India defines fraud as "any intentional act of omission or commission by any individual during the execution of a banking transaction or in the books of accounts kept manually or under computer system in banks, actually results into wrongful gain to any individual for a limited period of time with or without monetary loss to the bank".

The geopolitical and global macroeconomic situations have created a challenging and thought provoking environment for the banking industry worldwide. When it comes to analysing and managing its risks, the banking sector must evaluate its current methods. Modern methods of risk management are heavily reliant on technological innovations. The expansion of financial services to the public is attributable to the development of information technology and the widespread adoption of mobile networks in everyday life. Banking services have been made affordable and easily available by technological advancements, allowing them to benefit a wide audience.

On the other hand, it has increased the possibility that we will become the targets of cyberattacks. Cybercriminals have developed sophisticated methods to spy businesses and access crucial corporate information, all of which has a knock-on effect on the bank's bottom line. The annual loss from cybercrime is estimated at USD 114 billion, with the expense of fighting it reaching USD 232 billion. A cyber-attack can delay a bank's operations for up to ten days, increasing the already high costs of running the business. If we look at the losses sustained by the Indian banking sector in contrast to the worldwide loss, we see that it amounts to almost 3.5% of the monetary loss. The cost of the crime and its aftermath is estimated at $4 billion, while efforts to prevent future attacks cost an additional $3.6 billion.

Similarly, the Indian banking system takes longer than the global average of 15 days to resolve a crime. The financial sector must work with international regulators and watchdog groups to combat cybercrime, with the goal of creating a model that can be used to better manage and deal with cyber threats. The lack of a reliable compilation service in the financial industry that can spot emerging cybercrime patterns and build predictive models in response to them is the primary cause for alarm. But in the past few months, cybercrime has been seen as one of the top five hazards by financial institutions throughout the world.

Hackers acquired the personal information of approximately 2.9 million credit card clients from high-profile UK banks like Barclays and Santander by breaking into the banks' software maker systems, causing the businesses to suffer significant financial losses. While this situation is certainly concerning, it is not unique to the United Kingdom. Similar attacks have emerged in the United States in recent years, and to mitigate their effects, authorities there have developed a programme called Quantum Dawn. Unfortunately, most systems lag behind new cybercriminal technologies, necessitating the creation of a system capable of adapting to and neutralising any threats it encounters. What is needed now more than ever is a reliable system of defence that can deal with attacks before, during, and after they happen.

WAY FORWARD TO CURB THE PROBLEM

The RBI has instructed banks to make that grievances in this respect are handled & any consumer liability is substantiated within the 90-day time frame allowed by the bank's Board-approved guideline. Several actions have been taken to raise awareness about cyber-attacks, including the publication of a handbook for teenagers/students, the publication of data security best practises for state officials, the organisation of information security safety & security events, the distribution of messages on cybercrime via short message service (SMS), radio campaigns, and publicity on prevention of financial fraud & cyber safety suggestions through the social media channels of the Indian Cybercrime Coordination Centre.

The banking industry supports nation's economy. The consumer and the bank need to be informed of the potential dangers and the measures that can be taken to reduce them. To ensure the smooth execution of its cyber security plan, the Indian government formed the ISTF, with the National Security Council serving as its coordinating body. CERT-In is the government organisation in charge of handling cyber-attacks. Jurisdiction is a major problem in the fight against cybercrime. Every region of the world is vulnerable to cybercrime. Everyone, no matter where they live, should be able to report and investigate cybercrimes.

Complaints about cybercrime can currently be filed at local police stations or special cybercrime cells in India. Cybercrime monitoring cells have been established in many Indian states. Victims of cybercrime may be unable to report the incident in some cases due to factors including their location (being too far from the appropriate reporting authority), their lack of familiarity with the appropriate reporting authority, or concerns over their own privacy. With the absence of a standard method for reporting cybercrime online, many incidents may go unreported. There is also no centralised referral process for complaints related to cybercrime to reach national, state, or municipal law enforcement organisations. The IT Act has to be updated to include a definition of cybercrime as well as a list of circumstances in which it will have extraterritorial jurisdiction. The Cyber Laws of India need to be incorporated into the IT Act to make it more comprehensive. There needs to be more clarity and explicitness on the responsibility of the intermediaries.

CONCLUSION

There are several effects of cybercrime in banking industry such as financial loss, infringement, legal consequences and sabotages and theft to important data of an individuals. In India, there are several laws enacted in order to curb or protect the rights of netizens in the current world. Indian financial institutions has taken up an initiative to make every citizens knowledgeable about these kinds of cyber-attacks. In furtherance to this, they have started advertising cautious information in televisions, newspapers as well as radio.

Online services are becoming more and more popular among Indian consumers because of their extraordinary simplicity, cost savings, and quickness. Financial institutions are now offering consumers tempting discounts in an effort to increase the frequency of cashless transactions in order to reduce operational costs. Therefore, it may be concluded that a dynamic technical environment and improved attacker skills are outpacing economic institutions' cyber security measures to combat cybercrime.

These kinds of risks, which were mentioned in the project, are thought to be able to be reduced to some extent after making sure and estimating upon the proper checks on all the problems and involving all the stakeholders in order to solve this major problem relating to the technological growth in developing countries like India. In this way, we can in some ways ensure that India is safe and secure online.

Today, hackers may be found all around the globe in great numbers. Even though there are many public and private organisations trying to track out cybercriminals, every one of us has a responsibility to take steps to safeguard our accounts and personal information. Moreover, the illiterate should be educated on the use of computers, the internet, and credit and debit cards. As these cybercriminals often operate from a remote location, it can be challenging to track them down. To protect ourselves, we need to stay vigilant and use strong, one-of-a-kind IDs and passwords whenever we're online. Finally, I would like to stress the importance of staying safe online by only visiting reputable, encrypted sites.

REFRENCES:

1. David Bainbridge, "Hacking. The Unauthorised Access of Computer Systems; The Legal Implications." MODERN LAW REVIEW 236–45, (http://www.jstor.org/stable/1096193
2. A Karakasiliotis, "An Assessment of End-User Vulnerability to Phishing Attacks." 6 JOURNAL OF INFORMATION WARFARE 17–28, (Mar. 2, 2023, 10:49 PM), https://www.jstor.org/stable/26503466
3. Patricia L Bellia, "Spyware and the Limits of Surveillance Law." 20 BERKELEY TECHNOLOGY LAW JOURNAL 1283–1344, http://www.jstor.org/stable/24116655.
4. Brian F Caminer, "Credit Card Fraud: The Neglected Crime." 76 THE JOURNAL OF CRIMINAL LAW AND CRIMINOLOGY 746–63, https://doi.org/10.2307/1143521.
5. N.P Singh, "Online Frauds in Banks with Phishing", The JOURNAL OF INTERNET BANKING AND COMMERCE, (Mar. 3,2023,11:13AM), https://www.icommercecentral.com/open-access/online-frauds-in-banks-withphishing.php?aid=38493
6. Aditya Narang, "Rise Of The Growing Threat Of Cyber Frauds Due To Digital Payments", THE TIMES OF INDIA, https://timesofindia.indiatimes.com/gadgets-news/rise-of-the-growing-threat-ofcyber-frauds-due-to-digital-payments/articleshow/92968264.cms
7. "Prevention of Cyber Crimes", THE MINISTRY OF ELECTRONICS & IT - PRESS INFORMATION BUREAU, https://pib.gov.in/PressReleasePage.aspx?PRID=1845321
8. Neeta Chabra, Cyber Crimes In Banking Sector, 6 AAY' INT'L IN' RES' JOU'L 3 (2019).
9. S. Kalpana, Cyber Crime: A Growing Threat To Indian E-Banking Sector, 7 JOU'L EMR' TEC' INN' RES' 967 (2020).
10. Dr. Umamaheswari K., Impacts of Cyber Crime on Internet Banking, INT'L JOU'L ENG'