International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13 Issue 2, February, 2024, Impact Factor: 8.285

Virtual Banking Frauds: Facet, Motives, Trend and Suggestive Measures

Garima Dahiya

Research Scholar (Pursuing Ph. D. in Deptt. of Management Studies from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat)
under the guidance/ supervision of Prof. Rajbir Singh

ABSTRACT

The Indian banking system is well regulated and supervised under the ambit of Reserve Bank of India; it involves moral principles, financial prudence and good governance. The Indian Banking Sector has been at par with the rapid advancements in technology, emerging trends andchanges. This spur in technology has given the banking sectors immense opportunity as well as significant challenges in the form of cyber-attacks. The proliferation of online transactions in the form of NEFT (National Electronic Fund Transfer), RTGS (Real-Time Gross Settlement), ECS (Electronic Clearing Service) and mobile exchanges further gave the hackers a chance to exploit the people. This technological development endangers the virtual world, by making people and organizations prey of cyber-crimes. With the rise of virtual crimes, banking sector becomesthe hub of theft, phishing, PC infections, hacking and so on. Given this environment the paper aims to examine the technical aspects of various types cybercrimes concerning Indian Banking System and it also focuses on prevailing trend, motives behind cybercrime while providing certain valuable suggestions to curb the cybercrimes in banking sectors in India.

INTRODUCTION

Banking plays an important role in the evolution of market economy of any country. In today's world we cannot envision the economic development of any nation without the growth of their banking sector. Economydefines the prosperity of a nation and the banking sector is regarded as the cornerstone of that economy. Fordaily monetary transactions, people started using cash payment, cheques or demand drafts. This trend eventually led to a modern payment system in the formof debit cards or credit cards.

On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998, Information and Technology was introduced in the Indian banking sector. This call gave impetus to the online transactions which further paved the way for insurgence of innovative advancements such NEFT (National Electronic Store Exchange), RTGS (Constant Gross Settlement), ECS (Electronic Clearing Administration) and transportable exchanges which facilitates in saving time, efforts and money.

Like any other invention, technology has proven to be a double-edged sword with its own advantages and risks involved. It has direct impact on a bank's operationswhich exacerbate credit risks and market risks. Given the increasing dependence of customers on e-banking channels to perform their day-to-day transactions, these security risks can undermine public confidence in the use of online channels which can increase the reputational risk for the banks.Faulty technological implementations can also increase strategic risk in the terms of strategic decision making based on inaccurate information.

Banking system strives to provide better customer facilityusing information technology but cybercrime remains a risk. Whatever is available online is highly susceptible to be attacked by cyber criminals.

Cybercrimes result in huge monetary losses not only to the customers but to the banks also which affects the economy of a nation. Non-monetary cybercrime occurs when viruses are made and spread on other computers or insider business information is leaked online.

The most common of it is phishing and pharming. This paperexplores various problems faced by Indian banking sectorbyadopting the electronic banking.

REVIEW OF LITERATURE

To better understand of the subject matter is very necessity to have a look on some of the works which have been done in this regard.

Siaw I, Yu A (2004), identifies who can leverage competitive benefits from the internet are confronted with significant business potential. The impact of internet in banking industry and internet banking as a source of competitive advantage has becoming challenging issues for both business managers and academics.

Jaishankar, K., (2008), he has developed a theory called 'Space Transition Theory'to explain the causation of crimes in the cyberspace. He felt the requirement for a separate theory of cybercrimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon of cybercrimes.

Wada and Odulaja (2012), discussed that Cybercrime policy issues and provide insight into how cybercrime effects on E-banking from a Nigerian perspective. Social theories were used to explain causation with a view of guiding policy makers on behavioral issues that should be considered when formulating policies to address Cybercriminals activities in Nigeria

Balasubramanian et al (2014),studied the success of Information System in e-banking and its security risks. 52 respondents were scrutinized and foundthat customers have fear that information sent by them through internet is not protected, they also have threat of their bank's website getting hacked. The customers have the fear of the malware attacks too. The customers have their doubts about the security system of being reliable for online banking services.

Khan, M. N. et al (2015), identified and explored ways and means of the major concerns inhibiting the adoption of IB in India. The research targeted 400 bank customers from the Delhi NCR (National Capital Region). Multiple regression & Correlation analysis were used to analyze the data. The study found that awareness and safety & security would bring about positive changes in usage of IB and the issues of comfort, satisfaction, physical presence would bring negative impacts on intentions of usage of IB. They suggested that the banks should focus on strategic consumer groups to maximize their revenues from IB and concluded that concerns had a significant impact on the adoption of IB by customers.

Karim, S. S. (2016), emphasized on evolving a conceptual framework regarding the issues of cyber-crime in the banking sector of Bangladesh. She focused on the concept of the crimes happened in banks and the financial sector-namely Automated Teller Machine (ATM) frauds, E-Money Laundering, etc. She suggests that by applying the modernized technology and appointing skilled human resources and devices cyber-crime can be minimized from the banking transactions.

Goel, S. (2016), revealed that technical aspects of various types of cybercrimes concerning the banking and financial sector and their related impacts. Additionally, she identifies the threat vectors supporting these cybercrimes and develops measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security.

Ali, L. et al (2017), discussed the effect of cyber threats in Internet banking services and given level of customer awareness when dealing with Internet banking services. Moreover, they identified various security issues faced by banks and Internet banking customers.

Leung, R. (2018) analyzed Cybersecurity laws in the UK, USA, Hong Kong, and Singapore. He suggests that for retail banks indulging in e-banking services educating their customers about the basics of mitigating Cybersecurity risks is as important as checking their systems, controls, and processes are sufficiently resilient.

Simran et al (2018), have studied and analyzed the loopholes existing in the Indian Banking Sector to take corrective actions, thereby enhancing the security measures of this sector by curbing virtual threats.

Bhardwaj, A. S. (2019), Five classifications of algorithm are used: NB, K-mean, Artificial Neural Network, DT and DNN. The set of data to be extracted is huge, so a vital task is the pre-processing and processing of null values. The Artificial Neural Network and DNN can be useful to detect and analyze crime using past crime databases to predict future crimes from the enormous amount of data. Data mining algorithms can be preferred when data is monitored, and deep learning techniques can be used when data is multi model, enormous and unmonitored.

Soundarya, C. and Usha, S. (2020), The ARIMA model is widely used to make forecasts, but it is predictable. RNN model is used for cybercrime violation detection and evaluation of the pattern of the incident. The findings reported in this research are associated with validated attack data on the reliability of the SARIMAX and Compared to the

SARIMAX model, the prediction accuracy of the RNN model, both of SARIMAX and RNN models can achieve a reasonable forecast in terms of actual situations. There are several interesting aspects that are available for serious investigation.

Rahaman, H. A. (2020), Data mining procedures and algorithms are applied for pre-processed data to detect or predict fraud and remove noisy, incomplete, missing values. Three classification algorithms are used: DT, K-means and clipping method. This study introduces a descending algorithm for Big Data anomaly detection using K-means algorithms. To detect the anomalies posed in the monitored and unmonitored data collection, the suggested algorithm is used. With the clustering method, using big data analytics reduces the investigative time and helps to recover the secret information.

Al-khater, W. A. et al (2020), Cybercrime can be defined like any crime carried out using a computer or other communications platform to give people fear and alarm, or to hurt, damage, and destroy property. Cybercrime can be defined in two ways, one of them is computer-assisted and the other is computer focused. Crimes including in computer-assisted are child porn, theft, cyber-bullying and money laundering. Whereas, website defacement, hacking and phishing is included in focused cybercrimes.

Statement of the Problem

One of the most important tasks is to analyse and understand thoroughly the nature and the intensity of the given problem. Today, information technology has emerged as anindispensable part of the Indian Banking system. The impetusgiven to non-cash-based transactions all over the world has resulted in the tremendous growth of online payment system, which further led to the significant increase in cybercrime across all sectors among nations. Due to the proliferation of this crime, institutions face a significant challenge to prepare against these attacks. National Crime Records Bureau (NCRB), Ministry of Home Affairs released the 70th edition of the annual 'Crime in India' report which states that a total of 65,893 cases were registered under cyber-crimes, showing an increase of 24.4% in registration over 2021, crime rate under this category increased from 3.9 in 2021 to 4.8 in 2022. This research paper attempts to study the concerns of cybercrimes in e-banking sector by highlighting most common type of cyber-crime along with the prevailing trends in these crimes. There is a need to analyses the nature of such crimes so that appropriate preventive measures may be devised.

Objectives of the Study

As far asthe objectives of the study are concerned, there are four objectives that are set out to examine the problem thoroughly. These are:

1. To identify the various cybercrimes in e-banking sector in India.
2. To study the motive behind cybercrime in India.
3. To analyse the prevailing trend in cybercrime in India.
4. To provide the preventive measures to control the cybercrimes in India.

Research Design

Research design is an important and integral part of any research work. The focus of the paper has been on describing the various cybercrimes and the preventive measure to overcome this issue. The research design that has been chosen for the study is descriptive and the secondary data source has been used to collect data through web-sites, books and journals. The period of the study was till December 2023.

Limitations of the Study

Any work is not complete in itself; this work too has its own limitations. This paper focuses on the cybercrimes related only to thee-banking system in India. It neither covers the whole financial sector nor e-banking sector of any other country. All aspects, area and measures covered are limited to theInternet Banking users only.

Conceptofe-Banking

E-Banking, also known as online banking or virtual banking or internet banking is a system which facilitatesmonetary transactions like transfer of funds, payment of loans, accepting deposits and withdrawal of cash electronically with the internet. e-banking is not an old concept in India.The acknowledgment of the beginning of internet banking services in India goes back to the ICICI bank. City bank and HDFC bank started with internet banking services in India in 1999. Government of India and Reserve Bank of India took several other proposals for the development of Internet Banking in India. The government of India passed the IT act 2000 with the effect from October 17/2000 which gives lawful acknowledgment to e- transaction and other means of electronic commerce.

E-banking includes Internet Banking, Mobile Banking, RTGS, ATMs, Credit Cards, Debit Cards, Smart Cards etc.

Concept of Cybercrime

The word '**cyber**' is synonymous with computer, computer systems and computer network. Thus, it can be said that cyber-crime occurs when any illegal activity is committed using a computer or computer resource or computer network. Douglas and Loader have defined cyber-crime as a computer mediated activity which is conducted through global electronic networks that are either considered illicit or illegal by certain parties. Neither crime nor cyber-crime has been defined in IPC or Information Technology Act, 2000 (hereinafter referred as IT Act), but only provides punishment for certain offences.

Lord Atkin says: "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime"

According to **Josh Wepman** "Cybercrime is one of the fastest growing crimes at international level"

CYBERCRIMES RELATED TOE-BANKING

1. **Hacking**: Hacking is an action committed by an intruder by accessing our computer system without our permission. Hackers are primarily computer programmers, who have a superior understanding of systems and commonly misuse this knowledge for tricky reasons. They are usually technology experts who have expert-level skill set in one particular software, program or language.
2. **Virus**: Viruses are computer programs which will spread like a biological virus or infect a computer, file or other systems on a network. They interrupt the computer operation and affect the database either by altering it or by removing it altogether. They just reproduce until they consume up all available memory in the computer.
3. **Logic bombs**: Logic bomb, also called as "slag code", is a horrible piece of code which is intentionally inserted into software to execute a malicious task when generated by a specific event.
4. **Denial-of-Service attack**: Attack is obvious attempt by attackers to deny service to prospective users of that service.
5. **Phishing**: This technique is used for removing confidential information such as credit card numbers and username passwords. Phishing is typically carried out by email tricking. The malware would have installed itself on the computer and stolen private data.
6. **Data diddling**: Data Diddling is an unlawful altering of data before or during entry into a computer system, and then altering it back after processing is completed. Using this technique, the attacker may change the expected outcome and is difficult to track.
7. **Keystroke Logging or Key logging**: Key logging is a process by which attackers' record actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that aim at computer's operating system and are "installed" via a virus. These are very dangerous because the fraudster captures user ID and password, account number, and anything else that has been typed by the user.
8. **Spyware**: Spyware is a technique to stolen online banking credentials of the users for fraudulent activities. Spyware works by capturing information either on the computer while it is transforming between the computers and websites.
9. **Watering hole**: "Watering hole" cyber fraud is a branch arising from phishing attacks. In watering hole a malicious code is injected onto public web pages of a website which is visited only by a small group of people. In a watering hole attack situation, when the victim visits the site injected with malicious code by attackers the information of such victim is then traced by the attackers.
10. **Credit Card Redirection and Pharming**: Pharming is associated with the words, 'farming' & 'phishing'. In Pharming a bank's URL is hijacked by the attacker in such a manner that when a customer log in to the bank website they are redirected to another website which is false but looks like an original website of the bank. Pharming is done over Internet and Skimming is another method which occurs usually in ATMs.
11. **DNS Cache Poisoning**: DNS servers are deployed in an organization's network to improve decision response by caching before obtained query results. Poisoning attacks against a DNS server are made by exploiting exposure in DNS software. That causes the server to wrongly validate DNS responses that ensure that they are from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request.

TIME LINE AND EVOLUTION OF CYBER THREATS IN THE FINANCIAL SECTOR(Deloitte, 2020)

1971: Discovery of the first virus (Creeper and Reaper)

1988: The first 'Denial-of-Service'(DoS) attack: 'The Morris worm'

2005: 40 million card accounts of a US-based leading global payments company exposed in a security breach

2008: A major US-based MNC lost tens of millions of dollars to an international network hacking group

2010: ATM "jackpotting": An employee installed malware on a US-based multinational investment bank's 100 ATMs and stole US$ 0.3million in over seven months

2011: 0.36 million card details exposed as hackers exploited a URL vulnerability in a US-based financial services organization.

2012: 'Flame', the first most complex malware

2016: India's major attacks:

- In the case of Canara Bank, when in Aug 2016, a hacker from Pakistan, attacked and defaced the bank's site by inserting a malicious page and tried to block some of the bank's e-payments.
- Union Bank of India also became the victim of an attack in July 2016. Cyber thieves nearly stole USD 171 million from its Nostro Account. The attackers reportedly gained entry using spear-phishing, using spoofed RBI IDs.

2017: World's biggest ransomware attack: 'WannaCry' and 'Notpetya' cyberattack (costing at least US$ 10 billion) affecting banks, ATM network, and card payment systems.

2018: A Pune-based leading co-operative bank lost US$ 13.8 million in cyber-attacks; Canara Bank ATM servers were targeted in around mid-2018. According to sources, more than 300 user's ATM details were hacked by attackers and wiped off 20 lakh rupees from various bank accounts.

2019: Hackers attacked the server of co-operative Indian bank and stole US$ 0.1 million; internal leak led to stealing of US$ 4.1 million from a Mumbai-based co-operative bank

2020: The COVID-19 outbreak:

- Banks and FSI cyberattacks increased 238% during Feb-Apr 2020.
- About 40,000 cyberattacks attempted by global hackers on India's IT and banking in the last week of June 2020.

Cybercrime in India (2020-2022)

2020	2021	2022	Rate of total Cybercrime
50035	52974	65893	4.8

Source: NCRB "Crime in India" report 2022

- Crime rate is calculated as crime per one lakh of population
- Population source: Report of Technical group on population projections, National Commission on Population, MOHFW

NCRB Report shows that in States and UTS, cybercrime has seen a 24.4 percent increase from 2021 to 2022. Digital India has led to an increase in the usage of cashless transactions, digital money.

The continued increase in penetration of inclusive banking through the **Pradhan Mantri Jan Dhan Yojana** (PMJDY) with the total number of accounts crossing 29.18 crore, brought the uninitiated and new users into the fold of banking services (Saravade N. and Bhalla A., 2020).

Moreover, the exponential growth in online payments in India, with total digital payment market expected to grow to USD 1 trillion by FY23 and the **post-demonetization** emphasis on building a cashless economy highlighted the need for strengthening and bolstering financial cybersecurity.

RBI in its **financial stability report** pointed out that the banking industry remains a target choice for cyber-attacks especially post the **COVID-19** pandemic induced lockdown there has been an increased incidence of cyber-threats. ("Banking industry is the target of choice for cyberattacks: RBI"2020).As per **PwC's Global Economic Crime Survey**, cybercrime has jumped to the second position as the most reported economic crime and financial institutions are prime targets (Rivera K. and Rohn C., 2020).

Most Prevalent Types of Cybercrime As Per NCRB Report 2022

Type of Cybercrime	No. of incidents
Credit card/Debit card	1665
ATMs	1690
Online Banking Fraud	6491
OTP frauds	2910

Source: NCRB "Crime in India" report 2022

- Crime rate is calculated as crime per one lakh of population
- Population source: Report of Technical group on population projections, National Commission on Population, MOHFW

NCRB report states that among all the prevailing types of frauds in cybercrime arena, online banking frauds contributes the most. Lack of customer awareness, deficiency in employees' training and digital education, insufficient legal measures, inadequate digital infrastructure further aggravates the problem of cyber-attacks. As per the information reported to and tracked by **Indian Computer Emergency Response Team (CERT-In)**, a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively ("Over 2.9 lakh cyber security incidents related to digital banking reported in 2020",2021).

According to **Kaspersky's telemetry**, when the world went into lockdown in March 2020, the total number of brute force attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase. The numbers in India went from 1.3 million in February 2020 to 3.3 million in March 2020 (Shinde S. and Alawadhi N., 2021).The **IBM Security Data Breach Report of 2022** states that, for the fiscal year of 2022, the average data breach costs in India have reached a record high of ₹17.5 crores (₹175 million) rupees, or around $2.2 million, which is an increase of 6.6% from 2021, and a staggering 25% from the average cost of ₹14 crores in 2020.Sharing at a press conference, **Indian Cyber Coordination Centre** CEO Rajesh Kumar said, a whopping Rs. 10319 crores were lost to online frauds across the country between April 2021 and December 31, 2023. Moreover, the complaints on NCRP rose by 61% to 15.6 lakhs in 2023 from 9.66 lakhs in 2022. Currently cybercrime rate in India (reported cybercrime complaints in NCRP per lakh population) in 2023 was 129.**Financial frauds** accounted for 75% of cyber-crime in India from Jan 2020 to Jun 2023, with nearly 50 per cent cases related to UPI and internet banking, according to a study by an IIT Kanpur-incubated start-up.

Motives of Cybercrime In India, 2022

Personal Revenge	857
Emotional motives like anger	792
Fraud	42710
Extortion	3648
Causing disrepute	1902
Prank	173
Sexual exploitation	3434
Political motive	165
Terrorist activities	6
Inciting hate against country	34
Disrupt public service	70
Sale Purchase of illegal drugs	11
Developing own business	1068
Spreading piracy	89
Psycho or pervert	2
Steal information	137
Abetment to suicide	4
Others	10796
Total	65893

Source: NCRB "Crime in India" report 2022

- Crime rate is calculated as crime per one lakh of population

- Population source: Report of Technical group on population projections, National Commission on Population, MOHFW

Amongst the various inspirations for perpetrating a cybercrime, Monetary benefits remains the consistent winnerfrom the past many years surpassing the other motives including sexual exploitation, causing disrepute and developing own business.

About 30 crore people are vulnerable to phishing attacks in India, of which 5 lakhs potentially fall prey to scamsters, a top official of cloud communications firm Tanla Platforms said at the Mobile World Congress in Barcelona ("Around 5 lakh people potentially fall victim to phishing scams in India: report", 2023). These are the reported incidents and do not comprise the incidents that went unreported and/or unnoticed.

Banks all over the world are increasingly becoming the main target of distributed denial-of-service (DDoS) attacks which are launched sometimes as a part of a plan to confuse the security professionals from the crippling resources, meanwhile they carry out another dangerous activity simultaneously like insertion of virus, malware, or tampering with IT infrastructure. Such ahacking activity is embedded with a secret agenda known as Advanced Persistent Threat which is a new kind of threat gaining momentum now a days in the globe. In some cases, where the hackers are not able to attain some valuable data, they land up causing disrepute to the banks by defacing website of the given bank as a revenge. Sensitive information viz., leaked credit card/debit card numbers, online bank account details, OTPs, passwordand administrative access to servers are online sold for money.

Suggestive Measures

The digitalised world has become vulnerable to a new threat which is pervasive and underestimated. That's why this risk has become unevaluatedand remains unexamined. Year after year these attacks are draining the organisations of their money, reputation and trust, yet the cumulative efforts needed to tackle these attacks are not in place. Concrete measures to resist these frauds should be the priority of every government, businesses and organisations. As world is moving online, these security measures need to be stronger than ever to be able to protect virtual information and infrastructure. Just like the threats, such security measures should be far more cryptic,sophisticatedand updatedfrom time to time. To protect against online frauds, caution should be taken while opening web links or attachments from random senders, software should be updated timely, and any unauthorized activity in the bank account or credit card should be monitored, all the advisories of government and banks should be adhered too, moreover, all the scams and thefts should be immediately reported.An action Plan should be followed for cyber security:

- **Secure internal network**: organisation's network should be distinct from the public internet by setting user authentication mechanisms, firewalls and web filtering proxies. Additional monitoring and security measures, such as anti-virus software and intrusion detection systems, should also be used to detect and stop malicious software or unauthorized accesses.
- Develop strong password: Two-factor authentication methods, are safer than using just passwords for authentication. One common example is a One Time Passwords which are sent to respective mobile phones should be used in conjunction with static password. Moreover, strong password policies which suggest strong and complex passwords should be encouraged.
- **Encrypt sensitive data**: Encryption should be used to protect any information that is considered sensitive, plus all regulatory requirements on information safeguarding should be exercised. Different encryption solutions should be employed under different circumstances.
- •**Regularly update all software**: All systems and softwareshould be updatedtimely, as and when upgrades become available. Automatic updating services can be used especially for anti-virus applications.
- **Set safe web browsing codes**: Internal network should only be able to access those services and websites that are essential to the business and only by the employees with their respective passcodes. Web proxy can be employed to make sure that malicious or unauthorized sites cannot be accessed from internal network.
- **Create Safe USBsguidelines**: Employees should never put any unknown flash drive or USBs into their computer.

CONCLUSION

Cyber-attacks around the world are happening at a greater rate and intensity than before. Not only individuals, banks and businesses but also governments are being under radar. Thecyber attackers are becoming highly sophisticated while adapting latest technology. Recently, the financial world particularly the banks are being targeted for monetary gains. In today' world managing cyber risk has become the need of the hour. A cyber-safe environment needs awareness among public, training among staff at all the levels.Banks need to gain the trust of their stakeholders so that any attack or heist can be reported and addressed to resist future crimes. Banks should also focus on creating a cyber resilience atmosphere where best cyber safety techniques and cyber hygiene should be promoted. To make clients' bank account safer, all financial institutions should follow certain security guidelines as when suggested by government and RBI.

Customers should be advised to take all precautions while dealing electronically; they should never share personal information like PIN number, passwords etc. with anyone, including employees of the bank. PIN or password should be changed regularly should never be reused on every application. Customers should also be instructed to not provide sensitive account-related information over unsecured e-mails or phones. Safe cyber practices can go a long way in creating a cyber-safe environment.

REFERENCES

[1]. Al-khater, W. A. et al, ―Comprehensive Review of Cybercrime Detection Techniques, vol. XX, 2020, doi: 10.1109/ACCESS.2020.3011259.
[2]. Ali, L. et al (2017), The effects of cyber threats on consumer behavior and e-banking services,7(5), 70-76.
[3]. Around 5 lakh people potentially fall victim to phishing scams in India: report (2023, March 3). Economic Times.
[4]. Banking industry is the target of choice for cyberattacks: RBI (2020, July 27). Economics Times BFSI.com
[5]. Bhardwaj, A. S., Deep learning architectures for crime occurrence detection and prediction, vol. 5, no. 2, pp. 822–824, 2019.
[6]. Deloitte, (2020), Cybersecurity in the Indian banking industry: Part 1 report.
[7]. Goel, S. (2016), Cybercrime: A Growing threat to Indian banking sector, 5(12), 552- 558.
[8]. Khan, M. N. et al (2015). Adoption of Internet Banking in India: Issues and Concerns. International Journal of Electronic Commerce.
[9]. Over 2.9 lakh cyber security incidents related to digital banking reported in 2020 (2021, Feb 4). Hindustan Times.
[10]. Rivera, K. and Rohn, C. (2021). Fighting fraud: A never-ending battle.PwC's Global Economic Crime and Fraud Survey 2020.
[11]. Rahaman, H. A., A Proposed Model for Cybercrime Detection Algorithm Using A Big Data Analytics, vol. 18, no. 6, 2020.
[12]. Ricky, L. (2018). Cyber Security Regulations in the Banking Sector: Global Emerging Themes. The London School of Economics and Political Science.
[13]. Saravade, N. and Bhalla, A. (2020). Emerging trends and challenges in cyber security. Reserve Bank Information Technology Private Limited.
[14]. Shinde, S. and Alawadhi, N. (2021, April 6). India becomes favourite destination for cyber criminals amid Covid-19. Business Standard.
[15]. Siaw I, Yu A (2004), An analysis of the impact of the internet on competition in the banking industry, using porter's five forces model. International Journal of Management 21: 514-522.
[16]. Simran et al (2018), Cybercrime: A Growing threat to Indian banking sector, 5 (1), 926- 933.
[17]. Soundarya, C. and Usha, S., ―Analyzing and Predicting Cyber Hacking with Time Series Models, no. 7, 2020.
[18]. Sultana, S. K. (2016). Cyber Crime scenario in the banking sector of Bangladesh. The Cost and Management, 44(2).
[19]. Wada &Odulaja (2012), Assessing Cybercrime and its Impact on E-Banking in Nigeria Using Social Theories, 4 (3), 69-82.