IJARSCT

ISSN (Online) 2581-9429

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

Impact Factor: 6.252

Volume 2, Issue 2, June 2022

Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic

Manasi Sutar[1] and Mayuri Talegaonkar[2]
Students, Department of MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Cyber Security performs a vital position within the area of facts era. Securing information has been certainly one of the biggest challenges in the present day [1]. The usage of the internet has made human beings and organizations vulnerable to outdoor assaults [3]. Cyber issues mainly affect the information technology domain which includes different types of malicious attacks such as spyware, virus, social, and engineering. In this COVID-19 pandemic, the use and dependency on Internet have grown exponentially. This paper examines how cyberattacks have accelerated at some point of this pandemic and shows how substantially they have got affected banking sector.*

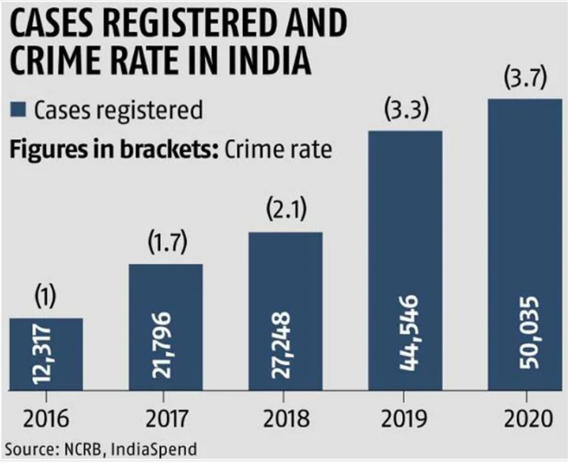
Keywords: Cyber Security.

I. INTRODUCTION

Cybercrime is a crime that is done using computer or network. An essential impact of cybercrime is monetary. Cybercrime can incorporate various kinds of benefit driven crime, including ransomware assaults, email and web extortion, and character misrepresentation, as well as endeavors to take monetary record, Mastercard or other installment card data.

Due to an increase in usage of digital devices Cybersecurity has become an important discipline of research. A attack can be planned or random, it can be by single intruder, multiple intruder or automated. The attack destroy computer or network, data theft, and more.

In today's era Cybercrime is one of the crucial issues for the Internet banking industry. The world is facing Financial terrorism in recent times. Protecting customers' private information is becoming challenging for the internet banking industry. A breach in any cyber protection results in financial and non-financial losses to the banking company and its clients, for this reason, cyber safety is important to protect against these breaches. Cybercrime is becoming a global problem as it have a serious economic impact. In the banking cyberspace securing sensitive information is a challenge. Due to this pandemic the banking world has evolved with cyber banking as it is a convenient way to do with technology. Our study is structured as follows. In section II, we have present a brief overview of the background study and try to understand increase in cybercrime. Section III is, about the research methodology use to research this topic.



Source: NCRB, India Spend

The essential goal of Cyber safety in banking is to shield the user's assets. As people go cashless, similarly actions or transactions are performed online. Individuals use their digital money like debit cards and credit cards for transactions that require to be safeguarded under Cyber protection.

1.1 Importance of Cyber Security in Banking Sectors

Cyber security isn't handiest restrained to IT enterprises, it's far critical for every single commercial enterprise. But, for banks, it holds important cost. Banks deal in millions of transactions on an ordinary basis. Hence, it's far very critical for banks to take protecting safety processes to protect their records against cyber assaults.

Here are some reasons why cyber security is crucial for banks:

- Loss to Customers - When a bank confronts a cyber-attack, it no longer only influences the bank's reputation but also causes loss to its client's assets. Normally, while a person loses cash because of card fraud, it may be retrieved from the bank. But, in instances like information infringement, it takes time to retrieve the funds, which is very stressful for customers. To keep customer's statistics secure, every financial institution needs to execute cyber protection methods which could shield their customers' information.
- Bank's Reputation - Data infringement is a vital problem for banks, as it results in dropping user's information. If the customers' facts of a financial institution are breached, then it becomes tough for clients to trust within the financial institution. Data breaches generally occur due to vulnerable cyber protection methods. Thus, it is required to have cyber security requirements for banks to evaluate the present-day security measures and shield crucial statistics.
- Digitization - As we realize, almost the entirety has been digitized now. From ordering merchandise to making meetings and sending money, we accept as true with on diverse virtual platforms. This makes it incredibly critical for banks to increase their banking capabilities used by clients, as hackers can hastily get right of entry to banking apps if proper cyber safety strategies are not applied.

II. REVIEW OF LITERATURE

Simran,et.al, they have recognized study and examine the loopholes existing in the Indian Banking Sector to control the fake exercises and to have the option to take restorative activities, accordingly upgrading the safety efforts of this area.

Liaqat Ali, et.al, mentioned that impact of cyber threats in Internet banking services and had enhance customer focus when coping with Internet banking offerings. By their manner of survey, it's far crucial to recognize and discover the security issues and Internet banking clients need to be privy to those strategies and strategies used by computer fraudsters.

Seema Goel (2016), found that technical elements of several styles of cybercrimes concerning the banking and financial area and their related affects. Additionally, she identifies the risk vectors assisting those cybercrimes and broaden measures to aid inside the combating the resulting cyber-attacks in order that such assaults may be better avoided in the future for superior safety.

A.R. Raghavan and Latha Parthiban (2014), they tested the exclusive kinds of cybercrimes which plague the banking area and the motives of the cyber criminals in the back of such acts. The economic loss inside the banking area is huge throughout the globe each in phrases of combating the cyber-attacks and on improvement of machine.

Soni R.R. and Soni Neena (2013), they showed a bigger share of private and overseas banks in frauds related to Internet banking, ATM, cards and different digital banking. Banking cyber frauds in the country are the end result of introductory segment of banking technology like ATM, Internet banking, mobile banking, EFT and so on which want time for humans, market and technology to get matured. Regulatory framework also receives more potent by revel in.

III. RESEARCH METHODOLOGY

The facts used is absolutely secondary in nature i.e., from assets published, printed media, magazines and journals.

Objectives of the study:

- To examine cybercrimes and its implications at the Banking Sector.
- To understand the seriousness of online cyber threats available to Internet banking enterprise.
- To understand the effects of cybercrime and its reasons.
- To degree the scope of protection and its implementation in Internet banking sectors.

- To analyse and use the preventive measures available to manipulate frauds.

IV. OVERVIEW OF INTERNET BANKING IN INDIA

Most of the Indian banks have launched their net banking and mobile banking web sites to facilitate the customers with on line availability of almost all banking merchandise. Internet banking is now a not unusual mode of stable and handy banking services.

Internet Banking, additionally known as net-banking or online banking, is an digital charge device that permits the purchaser of a bank or a financial institution to make economic or non-economic transactions online thru the internet. This carrier offers online access to almost each banking service, historically to be had thru a neighbourhood branch including fund transfers, deposits, and online bill payments to the clients.

Web banking can be accessed by any person who has enlisted for internet banking at the bank, having a functioning ledger or any monetary foundation. Subsequent to enrolling for web based financial offices, a client need not visit the bank each time he/she needs to profit a financial help. It isn't simply helpful yet in addition a protected strategy for banking. Net financial gateways are gotten by interesting User/Customer IDs and passwords. Internet banking may be accessed through any individual who has registered for online banking on the financial institution, having an energetic bank account or any economic institution. After registering for online banking centres, a patron need not go to the bank every time he/she wants to avail a banking provider. It is not simply convenient but additionally a steady technique of banking. Net banking portals are secured by means of specific User/Customer IDs and passwords.

There are three purposeful levels of Internet banking which can be informational, communicative and transactional. Under informational level, it's been identified that banks have the advertising records about the bank's products and services on a standalone server. Communicative level of Internet banking lets in a few interplays between the bank's structures and the consumer. Transactional level Internet banking allows bank clients to electronically switch budget to/from their bills, pay payments and conduct different banking transactions on-line.

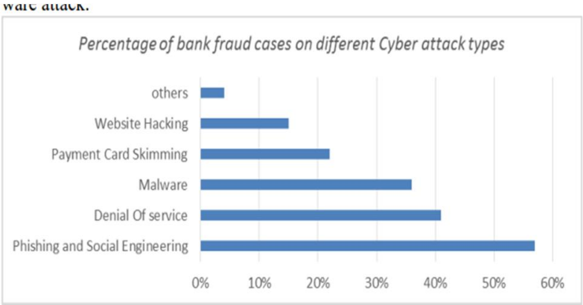
V. CYBER CRIME IN INTERNET BANKING

Top Cyber Security Threats Faced by means of Banks

- **Credential Stuffing:** Using Someone else identity is one of the not unusual cyber-crimes. In this sort of cyberattack, stolen account credentials which includes usernames and passwords are used to advantage unauthorized get entry to to money owed through massive-scale automated login requests. These lists are to be had due to breaches and may frequently be bought on the darkish web. In this kind of fraud, the hacker does no longer must play the password guessing game. The hacker uses an automated process where he can log hundreds to hundreds of thousands of breached password and usernames the use of automated gear.
- **Internet of Things (IoT) Exploitation:** Internet of factors, or IoT, devices can check with the swiftly developing quantity of physical gadgets capable of connecting to the internet. Unsecured Internet of Things (IoT) devices which include DVRs, domestic routers, printers and IP cameras are vulnerable to assault, when you consider that they're frequently no longer required to have the equal level of safety as computer systems. To breach a monetary organization, attackers will target insecure devices to create a pathway to different systems. Once they have entry from the IoT device, they have got full get admission to the complete community, together with all patron data.
- **Pharming:** Pharming is carried out through the net. When a patron logs in to a bank's website, the attackers hijack the URL in this type of way that they're routed to any other internet site this is fake however appears just like the financial institution's authentic internet site.
- **ATM Skimming and Point of Sale Crimes:** Installing a skimming device atop the system keypad to appear as a actual keypad or a device made to be affixed to the card reader to appear as part of the device is a tactic for compromising ATM machines or POS structures. Malware that without delay steals credit card records can also be established on those gadgets. Skimmers which might be efficaciously set up in ATM machines retrieve non-public identification variety (PIN) codes and card numbers, which are then copied to perform deceitful transactions.
- **Malware based-attacks:** This assault is most risky cyber threats to banking industry. In this attack malicious

code is created. The variety of malware attacks in the banking industry is on the upward thrust these days. Zeus, Spyeye, Carbep, KINS, and Tinba, are some of the most well-known banking malwares. Nearly every virus has characteristics: one, it secures a backdoor access into the gadget, and the alternative, it steals a user's credential information.

- **Phishing:** In phishing assault hacker try to benefit patron private information like pin, credit card variety, password, and so forth. In Phishing an electronic mail is ship to consumer that appears to be from a regarded organization like banks or from a famous website.
- **Dos Attack:** In this attack community and offerings are shutdown that effect the burden pace of a bank's internet site. DDoS attacks arise when multiple systems flood the bandwidth or sources of a focused gadget.



VI. TECHNOLOGY LANDSCAPE

The pace of digitization of monetary transactions in India maintains to gather pace. It is expected 7 that noncash payment transactions, which these days constitute 22 percent of all purchaser payments, will overtake cash transactions by 2023. It is envisioned that the entire payments carried out through virtual charge contraptions may be in the variety of USD 500 billion by 2020, which is about 10 times of contemporary degrees. The era infrastructure keeps to accumulate, with one hundred crore mobile connections in the united states of America, of which 24 crores are of cell phone customers. The variety of smartphones is expected to increase to fifty-two crore by way of 2020. Around 90 percent of all gadgets are net enabled and the number of net users is ready to double to nearly 650 million by 2020 from the erstwhile 300 million in 2015.

Meanwhile, the Aadhaar enrolments retain to attain saturation tiers, with states already reporting 100% insurance. Eight This has significant implications for KYC simplification, but additionally in similarly proliferation of offerings like Aadhaar Enabled Payment System (AEPS). Nine As mentioned earlier, the PMJDY money owed extended the financial inclusion time table, with nearly 18 crore accounts being in semi-urban/rural areas. It needs to be kept in mind that most of those account holders will be new to the banking processes and the technology infrastructure underlying it, making them vulnerable to social engineering and other cyber-attacks.

A critical component within the thrilling increase of the charge atmosphere become Indian FinTech businesses, which are scaling up in variety and class. These corporations are likely to leverage generation and establish interfaces with banks and the Aadhaar database. Some of the active regions encompass payment systems, peer to see and move border transactions in addition to cell PoS processing; robo-advisory and brokerage for personal finance control; crowd-funding, P2P lending, opportunity creditors and market places; and credit score scoring, analytics and risk control.

These new applications are anticipated to introduce complexities inside the interfaces among structures, which can gift cyber vulnerabilities, and records security troubles. Moreover, as FinTech groups embark on data-based differentiation, the troubles of information privacy and patron safety will become more and more vital. FinTech companies will no longer simplest have get right of entry to to sensitive monetary information approximately customers, however are possibly to acquire personal consumer records of their quest to recognize more approximately the patron. Interfaces and APIs that facilitate seamless data hops with a couple of applications may also be maximum prone and create potentialities for malware propagation, in case of cyber-attacks. Developing sturdy defence mechanisms and techniques to deal with these worries might be an imperative for the FinTech area, simply the manner it's miles for incumbent banks and economic establishments.

People are an increasing number of making their non-public information available publicly. Today there is an extraordinary amount of private records available with Government and private region players. Digital India, Aadhaar and the telecom initiatives have brought to the already growing pool of personal statistics with numerous public and private gamers to pursue their activities. Lack of knowledge of the security and privacy implications might also have already ended in publicity of large amount of records.

Publicly to be had non-public sensitive records can pose a hazard for Indians because the majority of the populace are digital immigrants, and, therefore, at risk of misuse of their facts. Individuals are time and again sharing and transmitting their personal statistics for numerous activities. Aspects such as the purpose for accumulating private information, how will this facts be used, security mechanisms put in area for shielding such records, for a way lengthy will this statistics be stored and what will be the technique for destroying such facts, are not acknowledged through the character nor have those components been defined uniformly inside the rules and tactics. India does no longer have a particular law specializing in facts protection.

VII. ONLINE CRIMES AND ONLINE ATTACKS

Every area and location inside the world, inclusive of commercial enterprise to training are dealing with the demanding situations of on-line assaults and crimes into their structures. We have labelled the mentioned cyber-attacks and online crimes for the 2 nations states: USA (+1) and India (+91) in context of the last five years' data. Many of the web attacks nevertheless cross unreported due to numerous motives, say complexity of situation and unknown state of the victim worldwide.

7.1 United States of America

We all are acquainted with the present-day state of affairs of submit-COVID era and the continuing vaccination around the world. The “stay-at-home” orders and “no mask no provider” at the moment are taglines at many locations [5]. Although this current scenario has left road crime to be decreased, online crime appears to be increasing. Like the relaxation of the international locations around the sector, the United States additionally shift to the digital (online) international by means of upgrading numerous security features. This online shift creates new possibilities for offenders to engage in diverse online crimes, as hundreds of thousands of humans start work / examine from domestic.

We are living within the technology of uncertainty, and we cannot measure every feasible online crime nor expect cyber victimization as social distancing continues however, we are able to practice counter measures (security features) and theories (from the preceding studies of clients) to assist us to counter the submit-COVID scenario. Even customers these days slightly perceive the form of assaults he/she faced online, the scope and dimensions of online crimes and online assaults vary sometimes and nation to nation. Identity theft and customer fraud are the main motive that agencies face everywhere within the states.

The quantity of data breaches and cybercrime is a modern and rising hassle (as COVID-19 resulted in 600 % upward thrust in on-line crime worldwide) within the United States (and everywhere in the international). The five maximum commonplace cyber-assaults (despite the fact that there exist extra than 05 kinds of attacks) skilled via US corporations, furnished by using Statista reports, consist of phishing (38%), community intrusion (32%), inadvertent disclosure (12%), stolen gadgets or facts (eight%), and machine misconfiguration (5%) in 2019 [5].

7.2 India

As we realize that many countries of the sector had been affected by the COVID-19 pandemic, India is also certainly one of them. In this pandemic all places of work, services (import-export etc) get stopped. Employees of companies do their working from home (WFH). In this disastrous scenario where the CORONA virus increases every day; the web crime and cyber-attacks are also at their height. The cybercrime and protection record of Statista indicates Uttar Pradesh country as maximum cybercrime instances with greater than 2 million USD fee of statistics breach in 2020. During the lockdown period, the online criminals and hackers do online frauds in extraordinary approaches (almost 300% rise in cyber-attacks, without elaborating the attacker’s profile) [5]. Here are some kinds of cyber-attacks utilized by them as follows:

(a) Corporate Ransomware attacks
(b) Cyber Stalking

DOI: 10.48175/568

(c) COVID family research and COVID vaccine

(d) WFH approach and accessing of VPN

In the pandemic era, there are numerous methods utilized by online criminals in place of the above list. India (with many internet customers) has visible a 37% increase in cyber-attacks within the first sector (Q1) of 2020, compared to fourth zone (Q4) of 2019 [5].

VIII. ISSUES AND CHALLENGES

During COVID-19 pandemic, individuals are powerless against network protection as there is increase of online exercises for example, e-learning, telecommute, internet shopping and others. In this Morden world, it is hard for everybody to remain up to date about the new gadgets and how to remain safe on the web. Beside this many people avoid to update their devices as they think updating will consume more memory. This type of devices become more vulnerable to cyber security as the hacker can easily hack not updated device. Phishing attacks is increasing during COVID-19 pandemic. Attackers can easily trick people to give them some important information or their credential data such as username, password and credit card numbers by sending official bank email. The finance sector is adversely affected since there billions of transactions occurring online. A survey among financial institutions by the Financial Services Information Sharing and Analysis Centre (FS-ISAC) finds a substantial rise in phishing, suspicious scanning and malicious activity against webpages for WFH staff to access the network. Bank employees who are not professionals in technology will not know how easily cyberattack scan take place.

As Bank are moving their data on cloud, they need to ensure that cloud assets and data are secured and meet compliance. Implementing security on cloud is one of the big challenges for banking sector as modern cloud deployments are tremendously complex. Bank application is becoming famous in this pandemic as they are easy to use. Online application uses API and api can be easily hacked using advanced methods that include SQL injection, cross-site scripting, and deploying automatic scripts known as “bots”. These types of attacks are damaging and costly, detecting and preventing these attacks is becoming challenging.

IX. FINDINGS AND SOLUTIONS

Many organizations and monetary establishments are nevertheless exposed to different risks. Following technique will help them to manage the risks-

- **Integrated safety as against layered defence:** As BFSI is a particularly regulated sector, banks invest time, cash and effort in deploying best-in- breed generation, which, lamentably, turn out to be strolling in silos and are tough to control collectively. Moving toward included protection, where all components speak and working together, is vital. [8]
- Multi-factor authentication: Multi-factor authentication (MFA) is a verification method in which access is only given once a consumer gives extra login credentials. Login credentials can consist of passwords, opts, or fingerprints. When establishing MFA, make sure that login credentials do not come from a comparable resource (passwords) as this can diminish security. MFA is a need for banks as it consists of an additional layer of protection when looking to get right of entry to important facts. [7]
- **Become smarter and intuitive with machine learning and big data analytics:** Considering the modern-day digitization power, there may be an exponential increase inside the records relevant to the BFSI zone. Analytics is the important thing factors in leveraging cyber resilience. A new technology of protection analytics solutions has emerged which can be able to save and analyse huge quantities of security facts in real time. [8]
- **Move from safety as a fee, to protection as a plus:** The mindset of seeing security as a cost needs an overhaul. The risks associated with protection threats and the capability effect to business ought to make groups see the blessings of proactive safety. [8]
- **Investing in Next Generation give end-point safety:** Traditional signature primarily based solutions are now not sufficient on their own and are prone to zero-day attacks. Banks and other economic establishments need to put money into generation that could recognize and save you the practices and moves utilized in exploits. [8]

- **Assess Cloud Security:** Review your cloud infrastructure regularly to make certain it's up to date. Assess your cloud security's current state, high-quality practices, and compliance requirements. To stable cloud structures and infrastructure, you possibly can use multifactor authentication. [9]
- **Monitor Cloud Security:** To automate the risk detection and guard in opposition to potential threats one could use a vulnerability management tool before they come to be a hassle. [9]
- **Disaster Recovery Plan:** Having an alternate plan to guard the records, help you to minimize downtime after a disruption and avoid facts loss. This may be applied simplest in case you backup your information frequently. [9]
- **Consumer Awareness:** It is one of the key elements where the person must be made aware of now not revealing their person credentials to everybody. They need to testify to the cyber protection cell in case of any questionable trends in their operations or of their bank account as fast as viable. [7]
- **Respond and Recover capabilities:** It is not a question 'if' an organisation would be attacked, it's far a question 'when. Organizations need to be prepared in identifying such attacks and not only respond, but recover with the least damage. [8]
- **Prioritize risk-based safety:** Risks are dynamic and 100% prevention isn't always practical. A danger-primarily based approach gives a clear roadmap for the business enterprise to consciousness its attempt and investment where it subjects. It is prudent to categorise the chance related to each gadget and cognizance on the efforts hence. [8]

X. CONCULSION

Cyber security in banking is something that can't be negotiated with. With the progress in digitalization within the financial enterprise, it has grown to be extra willing to hackers. Hence, there needs to be fool proof cyber safety that doesn't negotiate with the safety of user's and bank's statistics and cash.

The wave of technological advances and virtual innovation during the last decade has rapidly converted the BFSI region, making economic offerings greater efficient and easily on hand to all people. From making purchases, payments, and withdrawals to crowdfunding, making an investment, and applying for loans, human beings can now avail a plethora of banking offerings digitally, all from the comfort in their homes. Recent government statistics testified the boom in digital transactions in India—more often than not led with the aid of UPI—climbed near 90 percent, from 232,000 to over 430,000 among FY19 and FY21, and projected to account for nearly 71.7 percentage of usual charge quantity through the give up of 2025.

While RBI and the Government are taking proactive steps to warfare cyber-assaults, they are also evolving with newer generation developments like cryptocurrencies and blockchain. This steadily will increase the need for cybersecurity as a part of the design architecture proceeding to hit upon the stemming assaults in real-time, in place of repairing the damage.

REFERENCES

[1] A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies
[2] Impacts of Cyber Crime on Internet Banking
[3] The Impact of Cyber Security issues on Businesses and Governments
[4] COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19
[5] A review and analysis of online crime in pre and post COVID scenario with respective counter measures and security strategies
[6] Cyber Frauds in the Indian Banking Industry
[7] Cyber Security in Banking Sector - Top Threats & Importance
[8] Emerging trends and challenges in cyber security
[9] 4 Biggest Cyber Security Threats for Indian Banking Sector
[10] Cybersecurity Issues and Challenges during Covid19 Pandemic

DOI: 10.48175/568