Impact Factor (SJIF): 6.126 E-ISSN: 2583-1615, P-ISSN: 3049-3498

International Journal of Research in Academic World

Received: 02/August/2025 **IJRAW:** 2025; 4(9):46-53 **Accepted:** 13/September/2025

A Critical Review on Cyber Crimes, Challenges and Encountering the Risks & Problems by the Public and Bank Customers

[*1]V Sumalatha MSc., Applied Statistics., B.Ed., (Ph.D.) **and [2]Dr. S Srinivasa Padmakar** M.Com., M.B.A., M.Phil., Ph.D., PGDCA

[*1]Assistant Professor & HOD, Department Statistics (P.G), Keshav Memorial Institute of Commerce & Sciences, Hyderabad, Telangana, India.

[2]Retired, Visiting Professor and Academic Counsellor, Department of Commerce, Regional Study Centre, Khairatabad, Dr. B.R. Ambedkar Open University, Jubilee Hills, Hyderabad, Telangana, India.

Abstract

Cyber threats and crimes are shaking the public and various departments & organisations worldwide and the governments are facing many problems and it is a challenging task to the Cyber security agencies to protect the financial data and public transactions. Public and financial organisations are facing many problems with the cybercrimes losing crores of deposited amount from the banks. It is a regular phenomenon worldwide like corruption for looting public money attacking on their financial data using cyber and electronic equipment.

The cyber criminals are masters in using the emerging technology, I.T., A.I. and M.L., and gathering the contact number, bank account numbers, debit card and credits and e mail ids and Aadhar and PAN Cards and Passport-VISA ids of the public. It is a cyber-attack on the public ids, financial information. Trapping the public through their mail ids., creating the fake agencies of telephone dept., CBI., E.D., Banks, insurance, foreign affairs department, passport agency VISA Consulates. Calling the public randomly through their phone contact, create panic with fake police threatens, of CBI, ED., ACB attacks demanding amounts from the panic public with a hope of protecting public from those raids. These fake calls daily coming from unauthorised fake bank agencies, communication channels., Newspaper editors, Police. ACBs, C.B.I, & E. D to blackmail the targeted customers and the public. These are all fake organs make calls to the customers to blackmail them.

This paper will study and examine the nature, and scope of cyber threats, crimes. How they will target the public, their aim of attacks, and how the affected public will suffer and panic with cyber-attacks by the criminals. Their origin, their objective will be studied. Also studied and examined the cyber security agencies, local police facing the challenges, risks to protect the affected public. And to suggest the, remedial measures, and steps to alert and stop the cybercrimes is the main aim of the study. Secondary data will be the base to study the topic published from national and international journals and the data taken from cyber security agencies analysed through the graphic images, averages and the appropriate statistical tools and techniques.

Keywords: *Cyber threats, cyber-attacks, Cyber-crimes, targeted public, cyber security agencies, unauthorised fake agencies, Remedial measures to prevent cybercrimes, Artificial intelligence.*

Introduction

The topic, cyber security is a big challenging and hot topic today discussing worldwide. How to secure and safeguard the public, financial institutions, from the cyber threats, crimes and attacks from those cyber criminals. To be frank it is a largest worldwide network shaking the world threatening the targeted the customers effecting the privacy of the bank customer, government officials, insurance clients, etc. Unidentified cyber criminals thrown many challenges on the financial system of the country using the sophisticated emerging technologies.

Cyber security agencies, government security organisations try to control and prevent the cyber threats, crimes with traditional system of security will not give expected results. With the cyber-attacks, the business people, financial and commercial organisations, bank customers, government officials, merchant traders are mainly target by the cyber criminals.

The main weapon in their profession is threatening through the blackmailing on the weakness of the targeted customers using privacy phone calls, secret business financial contracts, corruptive trade practices of the government officials, hidden property accumulations, exceeding bank deposits of business people, secret honey traps etc. and political confidential meetings and illegal foreign country business dealings.

In these cases, mainly the cybercrimes will be done basing on privacy, and confidential phone calls through phone tapping of the targeted public, business people, govt. officials, conversations between two country officials. Secret cameras, security surveillance are also using to increase the cyber-crimes.

Adopting advanced scientific knowledge systems, AI driven technology, and computerised based technology, computerised data processing are the reasons to increase the

***Corresponding Author:** V Sumalatha

cybercrimes, as the cyber criminals also using advanced scientific technology, to capture the confidential financial data of the bank customers to make use of their criminal activities.

Fig 1: Cyber Security: Safeguarding Against Modern Digital Threats

The more we use the technical devices, AI driven technology, internet-based computer technology and advanced Smart, apple and android phone technology are also causing for the leakage of the data to the outsiders., due to unawareness of their usage. We have to protect our conversations, data, sharing the data with so many precautionary measures.

How to protect the A.I. technology, advanced scientific knowledge systems, advanced cell phone technology, computer internet based financial data from banks data usage of bank debit and credit card technology from the cybercrimes is the big challenge to the cyber security agencies and government police protection, to make this study and suggest the security measures, giving security alerts, preventive steps of the cybercrimes is the aim of the study.

The government organisations, banking and financial organisations, the local police force, insurance organisations, communication departments, educational institutions are continuously giving security alerts, to the public creating awareness on cyber threats attacks and the procedure of crimes followed by the cyber criminals to protect themselves in the banking and financial transactions.

Significance of the Study

Public and the various sections of people regularly doing their financial, business, property transactions with the government, commercial organisations and banking organisations, real estate agencies and from the insurance organisation making the conversations through the various communication networks and orally. In Olden days the public were attending all these transactions normally as usual without any problems, risks and challenges from their neighbours because they are all with some ethical standards, mutual understandings, and with mutual trusts.

But in some occasions, neighbours, surrounding people intentionally observe our financial and property transactions with suspected nature with harmful attitude Therefore, while doing their transactions, safety and security must be observed. Whether anybody observing them while doing bank transactions, withdrawal, deposits property transactions etc., must watch them carefully. Privacy should be followed while doing the financial transactions and property transactions.

As the days are changing increasing the population and decreasing ethical standards due to jealous and with harmful attitude developed among the people. There is a big gap between haves and have-nots developed among human beings. The illiterate without having proper education no proper employment opportunity will develop the jealous attitude towards employees, business people, bank customers.

This is the main reason to increase the cybercrimes rate in the country because the technology widely being used even by the low and less educated. It is easy way of earning without wasting their energy threatening the business people, employees and bank customers and landlords. They are using the technology for threatening the targeted customers through the communication networks, blackmail them with their human weaknesses affecting their privacy phone calls.

Cybercrimes, threats, and attacks are being done by the unidentified criminals, they unorganised using advanced scientific technology, computer technology and with emerging technology like artificial intelligence, Machine learning. They are appointing educated technicians for operating and for communicating with targeted customers and business people and bank customer blackmailing them to leak out their information.

To identify these people who are with suspecting nature, doing some mischievous and suspected activities keeping a close watch on them. Those cases are to be identified and recognised to deal and report them with local police, cyber security organisation.

Review of Literature

1. **Varunraj C. Kalse and Mohd. Farooque Khan (2025):** in their paper – "A Study of Cyber Security Management in online shopping-Marathwada region in Maharashtra", they studied the consumer perceptions on online shopping procedures and practices, awareness on using the ICT tools, technology security issues, quality of shopper's websites, on online payments security aspects, and trust worthiness of the organization systems. Moreover, they studied the cyber risks and challenges and trustworthiness of the material supplied by the shop dealers. They gathered the opinions of online customers opinions towards online purchasing process, and payments made through debit and credit cards. And how the card payment is safe to pay to the shop dealers without losing the customer confidential data. The main purpose their study to reduce the risk of cyber-crimes, while making online shopping doing online payments through debit and credit cards and get the secured shopping.
2. **Rami Shehab *et al* (2024):** In their paper "Assessment of Cybersecurity Risks and threats on Banking and Financial Services". They observed that technology adoption and adapting is inevitable in doing the bank transactions in these days. In this paper the authors mainly focused to study on the banking and financial institutions payment technology system escalating the cyber security attacks affecting the banking system, individual customers, and organizations. They studied more than 30 project studies and demonstrated how the cyber criminals continue to attack on the financial sector due to weakness loopholes in the organization infrastructure. They found that malware attacks are the most common threats to Banking and financial institutions. Finally, they concluded that the existing

Banking laws and acts are not sufficient to address the risks and cyber challenges as the cyber criminals adopting highly technology soft-wares, A.I. technology. Banking and Financial institutions must be updated with the technology to meet the upcoming and latest cyber threats and cyber-crimes.

3. **Hasibul Hossain, Nikhil C, Nath and other (2025):** In their paper Title – Cybercrime as a Threat to the Banking Sector: A Perspective from the commercial Banks in Bangladesh", they confirmedly opined that that the Cyber and technology related crimes are increasing day by day all over the world due rapid digital technology and Cyber related threats increasing all over the world. The I.T. Professionals, governments, legal enforcement authorities, software technicians are widely using the technology. Cybercrime threats becoming serious challenge and with risk to the developing countries. Recently the banking sector in Bangladesh is facing serious challenge, cyber threats problem. This paper mainly focused to highlight the risks and types of various cyber-crime in the banking sector by taking snow ball sampling technique and qualitative research techniques for their study. Interview method also been adopted to study, and establish the cyber threats in banking sector. They suggested certain measures to reduce and control cyber security threats and to strengthen the banking sector technology to overcome the cyber-crime challenges.
4. **Report on Cyber Security and Resilience 2024 FDIC:** The Federal Deposit Insurance Corporation (FDIC) submits a report on cyber security and resilience to the committee on financial Services of the House of Representatives and the senate Committee on Banking. The FDIC is the Primary federal regulator. The report discusses FDIC actions to strengthen the cyber security aspects in the financial services sector. This committee widely discussed on various cyber-crime issues and recommended with certain measures and precautionary steps. Information sharing about cyber threat information among financial institutions and face the situation with suitable measures. And Training of Officials on the updated technology controlling cyber threats. Collaborating with the other government organizations in strengthening cyber security also recommended.
5. **Bank Quest:** The Journal of Indian Institute of Banking & Finance Vol, 89 No.1 (2018): On the Cyber Security in Banks:

This journal consisting of various research paper and articles of on the banking cyber security risks and challenges.

The cyber security concerns in banking have always been the main Prime focus area of the" discussion and negotiations. The serious consequences of cyber-crimes have certain alerts the bank with strict vigilance in tightening of the security measure with a view to creative awareness among about cyber security in banks and sharing the knowledge to the readers.

The article with the title on "Cyber security in banks by Mr. Burra Butchi Babu, a senior Expert, institute for development and Research in Banking Technology (IBRBT). He opined that the cyber threat is a worldwide phenomenon and banks also are not exempted and moreover, the cybercrimes more will happen in banking transaction on the bank customers because they do the financial transaction ins banks with their bank deposits, various aspects, different varieties of bank cyber security threats in his paper.

The article written by Mr. Mukhopadhyay with title "A simple Banker into Bank's Cybersecurity: understand the task, the role", in this paper he has discussed in depth on the various cyber security challenges, and recommended various measures.

Another article written by Mr. Rajendran chairman, Digital security Association of Indian on "Banking IT's Security'' he has well explained the technical and legal aspects of cyber security and the importance of cyber security aspects, besides the cyber risk insurance as a measure of relief to the cyber security victim customers.

Summary of Review of Literature

Cyber security threats in different fields are world Phenomenon and the banking sector also has not exemption and moreover majorly badly affected and suffered with the cyber risk by the bank customers. Some of the authors widely discussed the seriousness of the cyber security problem with consequences. Some authors were observed that the more advancement in technology, A.I and machine learning also causing more opportunities and avenues to the cyber criminals. They are following more advanced technology thank banking and financial organizations throwing challenges to banks and bank customers.

Statement of the Problem

Using advanced challenge by the cyber criminals is a big challenge that should be avoided. Technology is available everywhere and to anybody avoiding to certain section of the people may not be possible but can guess what technology they are using and create awareness among victims. Super advanced technology must be adopted overcoming the challenges thrown by the cyber criminals. Banking authorities, insurance authorities and commercial organization also must create awareness and cyber security opportunities to their customers and give alerts continuously. Cyber security threat risk holders must be provided with insurance package.

Objectives of the Study

i). To Study on the possibilities of cyber security threats, challenges in Banks, financial institutions, commercial organization.

ii). To Study on the effects, serious consequences of the cyber security threats and various security risks and challenges to the banks, and bank customers

iii). To Study on cyber security measures, suggestions and recommendation overcoming the risks and challenges.

Conceptual Frame Work

1. **Possibilities of Cyber Security Threats, Risks, Challenges in Banks Insurance and Commercial Organization – Types of Cyber Threats, Risks.**

i). Banking sector plays an important role in the economic growth and development of the nation, since 1990, as a part of financial sector reforms and L.P.G. (Liberalization Privatization and globalization) adopted Information technology and insisted to habituate the technology with computerization and I. C. Tools in its day to day administrative, accounting portfolio activities, and for the customer bank transactions (V. Rajendran…Bank Quest)

ii). Banking in India today running on electronic technology devices like computerization, I. C. Tools. And with the support of electronic software and hardware in automation process.

I.T and I. C. Tools Security issues, cyber threats, risks

and challenges are the major problems to the banks and bank customer from the out-side cyber criminals who are also using advanced technology software to trap the bank customers.

iii). "Now a days cyber criminals do not rob with weapons on bank with premises and on staff with guns. But they are attacking with the highly sophisticated weapons with the support of keyboard and mouse and software" (V. Rajendran., Bank Quest) hacking the banking systems and on customer financial information system, and Management Information systems.

iv). According to Burra Buchi Babu, author of an article "Cyber Security in Banks" for Bank Quest, his observations on cyber security were shared as follows.
Cyber security attacks are carried continuously on various financial institutions, insurance organization., especially banking sector organizations are their target for their attacks, Banks were developed many apps to facilitate the customers for their banking services, utility, digital payments, Many, new customers are now habituating to the banking apps. Through them, customers are getting benefits, banking services.

v). Now the cyber criminals are targeting internet banking, mobile banking and on different apps, designed by the banks for customer services and unauthorizedly enter into those and performing malware functioning misguiding the bank customers to capture their valuable financial information.

vi). According to the above author, during 2014, 2015 and 2016, total cyber security incidents 44679, 49455 and 50362 respectively'' were recorded increasing year by year by Phishing, skimming ATMs causing heavy losses for banks as per the 'Computer Emergency Response Team (CERT)'.

vii). "The evolution of cybersecurity is a story of continuous adaptation, driven by the rapid advancement of technology and the parallel emergence of increasingly sophisticated cyber threats" …. Nachaat Mohammad.

viii). Banks have taking precautionary measurements for the malware functioning misguiding customers for the capturing valuable financial information of the banks account of the customers. Banks are now planned a decade back the Cybercrime Risk Insurance to compensate the cybercrime victims, but still, they are in dilemma in its implementation.

ix). The cyber criminals are continuously targeting the bank customers approaching the customer through unidentified phone numbers, on the name of the banks creating some hopes to the customers for certain benefits., they collect, capture and gather customer bank account details, card details, ATM pass words, OTP passwords.

x). Reserve Bank of India had provided many guidelines on information security, e Banking, Technology Risk Management and cyber frauds through the IB-CART, CERT-IN NCIIP helping banks in disseminating and foster sharing information associated with physical and cyber fraud threat incidents with suitable solutions.

xi). Moreover the I.T. Act 2000 and with subsequent further amendments focused on digital signatures, E Governance, Justice delivery system, offences and penalties. Still there is a need to redefine cyber-attacks and to further solutions.

xii). According to the author Sri Buchi Babu, B, observation, "Cyber criminals caused unprecedented levels of disruption of I.T. services with relatively simple I.T. tools and cloud services.

xiii). Cyber security attacks by the criminals capturing the bank I.T. devices by unauthorized entering and doing malware functioning disrupting the I.T. services misguiding the bank customers causing heavy losses by capturing the financial and customer account, card information.

xiv). Reserve bank of India wide in the circular dated 2nd June 2016 issued comprehensive guidelines on cyber security measures to ensure cyber security/resilience frame work in banks, the following are some of the features mentioned in the above RBI guidelines.

a) Banks must have a separate approved board framing on cyber security Policy on broader I.T. Policy/I.S. Policy of a bank. Banks to establish cyber risks in real time through the Security Operations Centre and make continuous monitoring.
b) Cyber Security Crisis Management Plan should immediately be designed as a part of overall strategy.
c) Commercial bank branches must share Cyber-crime incidents information with R.B.I continuously for monitoring and controlling purpose.
d) Banks should create and conduct the awareness programs to all related stakeholder by creating cyber security cell to deal with customer grievances.

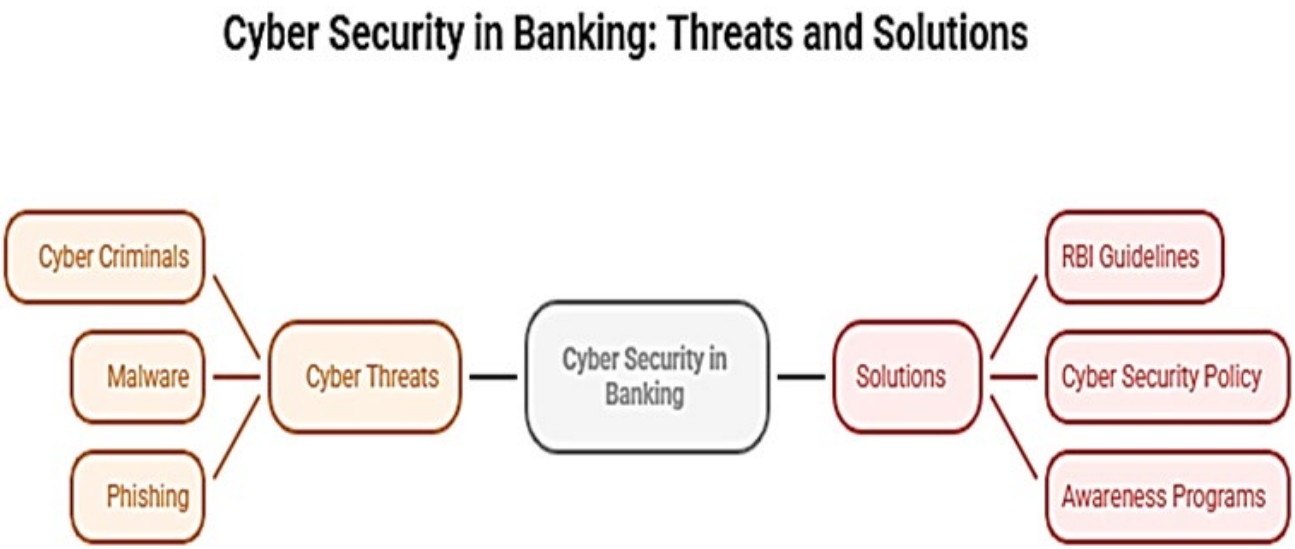

Fig 2: Cyber Security in Banking: Threats and Solutions

2. Varieties and Types of Security Threats, Risks and Challenges

The following are the various types of security threats and risks

Phishing the data attacks of the customers, capturing unauthorized gathering the information from the customers. Spoofing, E Mail Attacks, Malware, third party services, Spam calls, unwanted calls., Point of sale attacks through…capturing card numbers, OTP pass words, card information. Phishing, Cookies, Hacking, cracking and spoofing and cyber security threats.

Banks are more vulnerable to cybercrime securities than other business. Online payment fraud, A.T.M machine fraud, electronic debit, credit card frauds, net banking transaction frauds, Unwanted fraud mails, crimes, fraud embedded links and denial of Service (DOS) attacks.

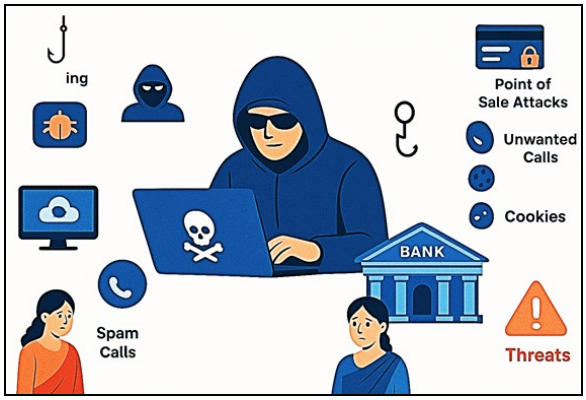

Fig 3: Cybercrime Threats Targeting Banking and Financial Customers

And internet logging attacks, software fraud, spamming and Spyware. Link between Customer happiness and bank security unfavorable. Fake phone call frauds on the name of banks, financial and insurance organization. Strategic cyber security threats, and attacks by the cyber-criminals targeting particular type of customers, senior citizens, illiterate rural women, illiterate street business people.

"These financial crimes are increasingly using Artificial intelligence to create fraudulent or fake alternate document, audio files, video recordings leading to increasing number of fraud cases. The generative A. I. tools allow malicious actors as realistic images (2024 Report on Cyber security and resilience FDIC).

The following current, and emerging operational resilience and cyber security threats to the banking Sector as per the "Cyber Security and Financial system Resilience Report"

i). **Ransomware:** The frequency and severity of ransomware attacks continue to increase targeting all sizes of organizations in the financial sector.

ii). **Denial of Service (DoS):** It attacks in a variety of shapes and sizes and call for different mitigations.

iii). Artificial Intelligence: The banking sector and financial organization sector new fraud and cyber security related to threat from cybercriminal culprits using advanced technology Artificial intelligence A.I. The usage of A.I has the potential to reduce the costs and increase efficiencies, improve products and services and performances, strengthen the risk of management. A.I. has also present challenges including the operational risks.

iv). **Taking Over Accounts:** Cyber criminals have used several ways to gather unauthorized access to the financial information or to take over the control of customer accounts, These, attacks are very popular and becoming more sophisticated

v). **Supply Chain-cyber Risks:** Cyber-criminal culprits are increasingly and continuously exploits using widely I.T. systems and services to conduct malicious cyber activities affecting thousands of customers including government agencies.

vi). **Geopolitical Cyber Threats:** These type of threats and risks are exploring political potential cyber-attacks in response to the unprecedented economic sanctions. These tensions highlight the importance of heightened threat monitoring, greater public private sector information sharing and safeguarding and disruptive attacks targeting the financial sector.

Fig 4: Banking Sector Cyber Threats

Impact of Cyber Attacks, Threats on Public Financial Dealings:

Rapid growing of technology, like A.I. and I.T., Internet, which are really facilitating for the cyberattacks and cyber threats, implementing the tools and software for attacking the bank customers. Public and business people, insurance clients,

spreading rumors and request the bank customers, insurance clients to update the KYC norms unauthorizedly.

Like that they will get all the bank account details, Pan Card details, Aadhar card details, credit card and debit card details security password of the customer. Public and bank customers feel that the calls received from banks are really requesting and they will disclose all the confidential cards details numbers, passwords to those unauthorized callers

They are getting the telephone numbers from the telephone network operators, Aadhar card and pan card details of the customers and ask the customers to link up both Pan card and Aadhar to insurance policy and bank accounts and to the voter card also.

Fig 5: Cybercriminals Exploiting Customer Trust for Financial Fraud

During the linkage process the confidential cards information is now disclosed openly to so many agencies. These details are available with private agencies SIM card telephone operators, They, are selling to outsiders and later they will be in the hands of cyber criminals, once they reached all the details, they will start the game threatening and blackmailing the public and bank customers.

They will do the reputational damage to the public, customers, teacher, bank people, catching their weaknesses, black mailing them and threaten them to handover the police custody, digital arrest, online police enquiry, threatening through the official phone calls,

They demand the cash, directly, or transfer the bank cash from their account. Or directly drawing the funds from the customer bank. Without the customers' knowledge.

Loss of deposited amount from their customers bank account director asking the customers to press the link or processing

By Damaging the brand image of the product manufactured and traded by the business individuals and manufacturers for the sake of competitors.

Directly stealing the public money from the bank accounts unknowingly through catching the account, Aadhar and pan account number from outside agencies.

According to an internet-based study report, *"Cyber Crime cases rapidly increased significantly between 2020-2025 in India showing a jump from 3,94,000 cases in 2019 to more than 1.4 million cases in 2021 and with over 1.2 million cases reported in mid-2025"*.

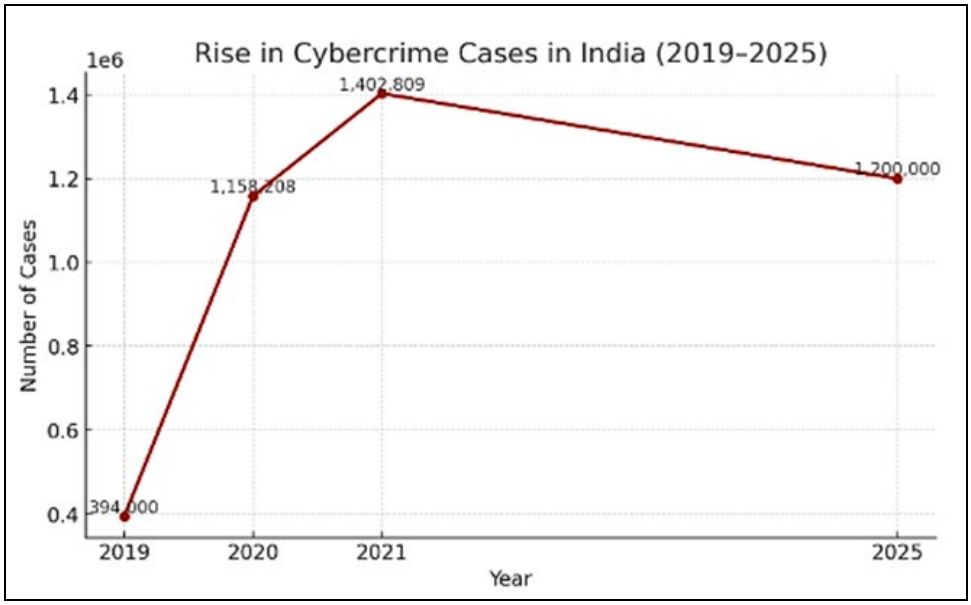

Fig 6: Trend of Cybercrime Cases Reported in India (2019–2025)

Major Cyber Threats

Major cyber threats during this period included financial fraud, data capturing using A.I based technology by cyber criminals to develop sophisticated attacks.

Other Types of Cyber Threats

i). Financial Fraud (individual bank transaction and financial institutions)
ii). Confidential financial Data capturing (2020 Solar Winds Supply chain hack)
iii). Social Engineering & Impersonation (Fake Police case, CBI case, ED cases, Fake court Trials and digital arrests.)
iv). Artificial Intelligence (AI) in Attacks (AI merged formidable tool)
v). Malware and Vulnerabilities (Trojan, Infectors and other Novel threats)

Rising Number of Cases

In the 2019 year 3,94,499 cases., in the 2020 year: 11,58,208 cases. And in the 2021 year: 14.02,809 cases

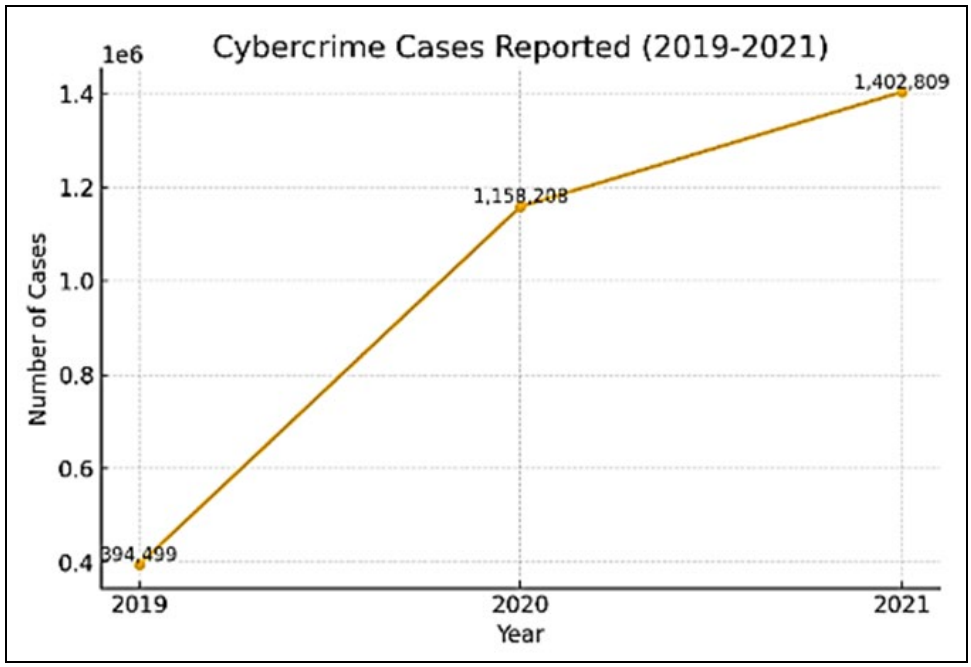

Fig 7: Rising Trend of Cybercrime Cases in India (2019–2021)

3. Case Study Reports on Cyber Security Aspects Suggestions, Recommendations:

(Times of India 15th Sept 2024) reveals the following observations

Dealing with cyber threats, crimes and providing cyber security is a big challenging task to the government, security agencies, banking and financial organizations. Emerging technologies not only for security agencies but cyber culprits also using actively. With those heavy financial losses incurred to the public yearly.

- **Cyberabad & Hyderabad (2023–24):**
  - Cyberabad registered 5342 cases in 2023 and 5500 cases in 2024.
  - Hyderabad registered 2140 cases, and Rachakonda 1500 cases.
  - Victims across Telangana lost ₹1085 crore (May 2023 – April 2024).
- **Types of Crimes:**
  - Over 50% of cybercrimes are investment scams.
  - Daily victim loss: ₹3.3 crore in Telangana.
  - Responding to unsolicited messages was a major factor in financial fraud losses.
- **Detection & Recovery:**
  - In Hyderabad (2023): Only 51 of 2735 cases resolved.
  - In Cyberabad: 168 cases detected, with ₹233 crore lost, and ₹46 crore recovered.
  - Nationally, only 16% of cases solved, and 3% of stolen funds recovered.
- **Nationwide Cases (2021–2025):**
  - 2021: 4.5 lakh cases.
  - 2022: 10,29,026 cases.
  - 2023: 15,96,493 cases.
  - 2024: 22,68,346 cases (36.37 lakh incidents of financial fraud reported via CFCFRMS).
  - 2025 (mid-year): ~12.5 lakh cases already recorded.

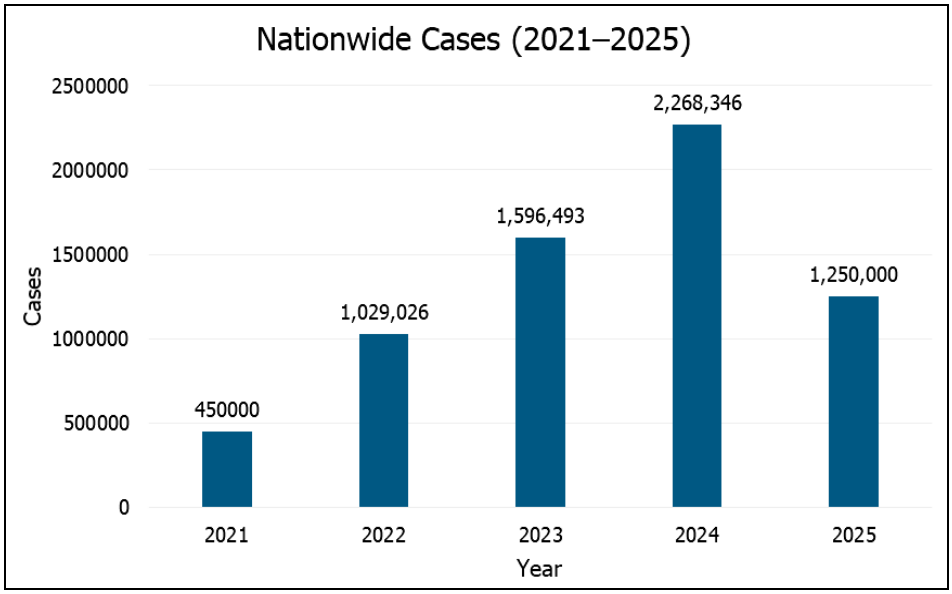

Fig 8: Nationwide Cases (2021-2025)

- **Financial Losses:**
  - 2023: ₹7465.18 crore lost.
  - 2024: ₹22,845.73 crore lost (a 206% increase).

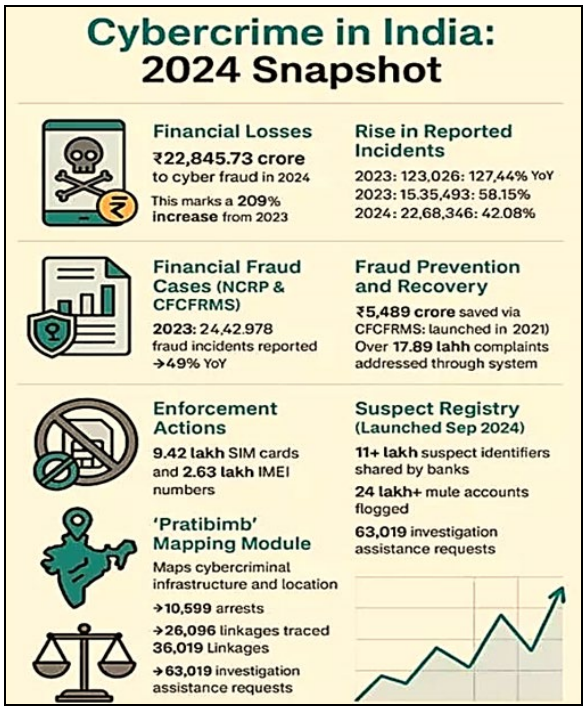

Fig 9: Cybercrime in India: 2024 Snapshot

Source References

- Times of India (TOI)
- PTI News Agency Reports
- Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)
- Ministry of Home Affairs (Parliament Report)
- MIT Sloan Case Study by Sanjana Shukla, George Wren & Dr. Keri Pearlson

Suggestions & Recommendations

i). Government should avoid the insisting Aadhar. PAN, id cards, phone nos. e mail ids for the public transaction. They are all reaching and side-tracking cyber-crime culprits. They misusing and threatening the public looting public money.

ii). Telephone operators issuing Duplicating Sim cards to other persons who applied on behalf of original sim card holder. This should be avoided.

iii). Bulk sale of telephone numbers should be avoided from the telephone operators to so many organizations, customer care centers, individuals, real estate owner, without the prior permission of customers. Whoever applied for their business activities. Customer are receiving unwanted calls daily. It is a big problem.

iv). Customers and public must safeguard their financial information bank-debit/credit card, bank account details, nos. and the security password and should not disclose to anybody including family members.

v). Bank people must not disclose the financial data account detail to anybody if any make id cards on the name of fake police, ACB CBI, IT dept. ED, GST tax authorities approached for checking account details, and to open lockers in the bank without the customer consent & presence. When they approached, bank people must call the customer and take the written consent.

References

1. Peng Liu, Tao Lio *et al*. Published by Penn State Cyber security Lab.
2. Nachaat Mohammad (2025) – Artificial Intelligence and Machine learning in Cyber Security – A deep dive into State-of-the-art techniques and future paradigms. From Homeland Security Department Rabdan Academy Abu Dhabi UAE vide in Doi. Org/10.1007/s10115-025-02429.
3. Cyber Management Alliance (2023) – The Impact of Artificial Intelligence on Cyber Security – It's a Newsletter.
4. World Economic Forum AI Governance Alliance Collaboration with the Global Cyber Security Centre, University of Oxford (2025) – "Artificial Intelligence and Cyber Security Balancing Risks and Rewards – White Paper published in January 2025.
5. Steve Wilson, Contrast Security (2023) – "Cyber Security and Artificial Intelligence: Threats and Opportunities" published by Contrast Security in 2023.
6. Mariam Aldhamer (2023) – The Impact of Artificial Intelligence on the future of Cybersecurity. Published by Multi-knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ) vide issue 71 in 2024.
7. Sanjana *et al* (2020) – A Case Study on "Cybersecurity Management of A. I Systems: Managing an attempted Breach at E-Fortress" p.no.1-19.
8. Threat Landscape Report (2025) on cyber threat predictions on Cyber Security: Key Benefits, Defense, strategies & future Trends.