JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY AND WAYS TO TACKLE CYBER CRIMES IN FINANCIAL INSTITUTIONS

1. Dr. Rajasi Dutta

State Aided College Teacher (SACT)
(Department of Commerce, Charuchandra College,
University of Calcutta, Kolkata, India)

2. Aditya Kumar

(Research Scholar)

Abstract

Cyber security has become a critical concern for institutions due to the increasing frequency of cyber threats. These threats not only pose a risk to the financial integrity of the institutions but also impact customer trust and the overall stability of the industry. To effectively combat cyber crimes, organizations must prioritize the understanding of internet threats and implementing measures that promote awareness and safety. This study aims to understand the need of cyber security and how it is important in these increasing stage of technology. By studying relevant articles this study also seeks to uncover the possible forms of cyber threats, policies to mitigate them and provide ways to tackle cyber threats so that governments, financial institutions., universities and other business can secure their confidential data and reputation.

Keywords – Cyber security, cyber crimes, financial institutions, ways to tackle cyber threats.

1. INTRODUCTION TO CYBER SECURITY

In the unexpectedly evolving technologies, cyber security has emerged as a crucial thing of contemporary-day society. As our reliance on generations deepens, so does the want to defend our virtual assets, records, and structures from cyber threats. Cyber security includes a wide variety of practices, technology, and techniques designed to guard against malicious activities within the virtual realm. At its core, cyber security goals to ensure the confidentiality, integrity, and availability of statistics and structures. Confidentiality entails stopping unauthorized access to touchy records, and

other confidential data. One of the essential activities of cyber security is to protect against unauthorized access. This entails enforcing strong authentication mechanisms, together with passwords, biometrics, and multi-element authentication, to make certain that the simplest legal people or structures can get admission to touchy data. Encryption performs an important function in safeguarding records at some point of transmission and storage, making it tough for unauthorized entities to access the content. As the virtual environment expands, so do the styles of cyber threats. Malware, along with viruses, ransomware, and Trojans, poses a considerable hazard to people and groups. Cyber security measures encompass deploying antivirus software, carrying out ordinary machine updates, and instructing customers to keep away from ability threats. Phishing attacks, wherein malicious actors try to mislead people into disclosing crucial records, are also prevalent. Cyber security efforts fight phishing via e-mail filtering, person education, and the implementation of protocols. Social engineering attacks, which control people to disclose exclusive records, are another area of study that calls for technological defences and individual awareness. Securing networks is a crucial thing of cyber security, regarding measures together with firewalls, malware detection and prevention structures, and virtual private networks (VPNs). These technologies help reveal and manage community traffic, locate suspicious activities, and create steady conversation to defend. In the world of cyber security, regular vigilance is vital. Threats evolve, and cyber attackers adapt their tactics, techniques, and procedures. Therefore, groups hire safety specialists who interact in moral hacking, penetration testing, and vulnerability exams to become aware of and deal with weaknesses earlier than malicious actors can take Governments and regulatory bodies play an important role in shaping cyber security rules and standards. Compliance with those policies is vital for groups to ensure the safety of their structures and the safety of all records. Additionally, global cooperation is also crucial in addressing cyber threats that go beyond country wide borders. The destiny of cyber security will likely see persisted improvements in technology, together with synthetic intelligence and gadget learning, that may enhance chance detection and reaction capabilities. However, with innovation come new challenges, and the cyber security panorama would require ongoing variation and collaboration to stay ahead of rising threats.

2. LITERATURE REVIEW

- **I-Chiu Chang, His-Ginn Hwang, David C. Yen, Hen-Yi Huang (2006)** investigated about factors affecting internet security implementation in different financial institutes in Taiwan. A survey of 573 CIOs revealed varying levels of concern for software systems, hardware security, executives' support, internal system users, organizational characteristics, and security policy.

- **Vuuren, Leenen, Phahlamohlaka, Zaaiman (2012)** founds that the South African government has approved a draft National Cyber Security Policy Framework in 2012, but needs a national cyber security governance structure to effectively control and protect its cyber infrastructure. Despite various structures, implementation is still in the early stages. A holistic approach to cyber security, involving

partnerships between business, government, and civil society, is crucial. This paper investigates government organizational structures for national cyber security control in selected countries and proposes a proposed approach for South Africa.

- **Setiawan, Sastrosubroto (2016)** have conducted a study on "Strengthening the security of critical data in cyber space, a policy review" This study reviews about the policies for strengthening critical data sovereignty in cyber space of Indonesian Government. It reveals that many cyber security policies and regulations are not properly implemented and enforced, raising questions on cyber security awareness in Indonesia. The study proposes initial recommendations for securing National critical data in cyber space, including implementing regulations for data storage within the country. It also suggests necessary actions and further studies required to address the lack of proper implementation and enforcement of these policies.

- **R.K Goutam (2016):** Explained the importance of cybersecurity, he discussed that the growing volume and sophistication of cyber attacks on sensitive information and data, highlighting the insecurity of the internet for transmitting such data. It highlights the increasing prevalence of hacking and presents various methods of cyber attacks globally.

- **Ghosh (2022)** explained how cyber security has become a complex and rapidly evolving ICT concern, with increasing cyber attack incidents targeting people, companies, and governments. ICT is increasingly seen as a battlefield for strategic wars and a strategic asset for national security. This study examines cyber security's importance from India's perspective, enhancing the analysis of the field.

3. OBJECTIVE OF THE STUDY

Cyber security is a critical concern for Institutions due to the growth threat of cyber attacks. So it is important to study cyber security so that institutions can protect themselves from cyber risks and develop a robust cyber security framework.

This study will help in –

1. Exploring the importance of cyber security.
2. To identify various forms of cyber crimes.
3. Identifying the needs of cyber security in financial institutions.

4. NEEDS OF CYBER SECURITY

Cyber security is now taken into consideration as critical element of people and households, in addition to agencies, governments, academic establishments, and our business. It is vital for households and mother and father to defend the youngsters and own circle of relatives from online fraud. In terms of monetary protection, it's vital to stabilize our monetary data that can have an effect on our non-public monetary status. Internet is very critical and useful for faculty, students, personnel and academic establishments, has supplied masses of getting-to-know possibilities with the quantity of online risks. There is vital want for net customers to apprehend a way to defend themselves from online fraud and identification theft. Appropriate getting to know approximately the web conduct and

device safety outcomes discount in vulnerabilities and more secure on line environment. Small and medium-sized agencies also revel in diverse protection-associated demanding situations due to the fact of restrained sources and suitable cyber protection skills. The fast enlargement of technology is likewise developing and making cyber protection as hard as we do not gift everlasting answers for involved problems. Although we're actively combating and providing diverse frameworks or technology to defend our community and data, however, all of those offering safety for short time period only. However, higher protection knowledge and suitable techniques can assist us in defending intellectual belongings, change secrets and techniques and decrease monetary and reputational loss. Central, country and neighbourhood governments preserve large quantity of records and personal data on line in virtual form that turns into the number one goal for a cyber attack. Most of time governments face problems because of inappropriate infrastructure, lack of knowledge, and not enough funding. It is critical for the authorities and our bodies to offer reliable offerings to society, keep healthy citizen-to-authorities communications and safety of personal data.

5. IMPORTANCE OF CYBER SECURITY IN FINANCIAL INSTITUTIONS

Cyber security is paramount in monetary establishments because of the touchy nature of the facts they take care of and the important position they play within the economy. Here are numerous key reasons why cyber security is crucial in monetary establishments.

- **Protection of Financial Data:** Financial establishments keep sizable quantities of touchy facts, such as non-public and monetary records of clients, account details, transaction records, and proprietary enterprise records. Cyber security measures are important to guard this information from unauthorized access, theft, or manipulation.
- **Prevention of Financial Fraud:** Financial establishments are high targets for cyber criminals searching to perform fraud schemes, which include identification theft, account takeover, price card fraud, and fraudulent twin transfers. Strong cyber security defences assist in locating and securing fraudulent activities, protecting the organization and its clients from monetary losses.
- **Preservation of Trust and Reputation:** Trust is most important within the monetary sector. A cyber security breach can seriously harm a financial organization`s recognition and erode the trust of its clients and stakeholders. By making an investment in study cyber security measures, establishments exhibit their dedication to protective records and retain the consider in their clientele.
- **Compliance with Regulations**: Financial establishments are challenge to strict regulatory necessities regarding facts, safety, and privacy, which include the Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR). Compliance with those rules necessitates the implementation of complete cyber security measures to guard consumer information and keep away from regulatory penalties.
- **Mitigation of Operational Risks:** Cyber security threats pose operational dangers to monetary establishments, such as disruptions to enterprise operations, downtime, and monetary losses as a result of cyber attacks. By proactively enforcing cyber security controls, establishments can mitigate those dangers and ensure continuity in their operations even in the face of cyber threats.
- **Protection in opposition to cyber threats:** Financial establishments face an infinite number of cyber threats, such as malware, phishing attacks, ransomware, insider threats, and allotted denial-of-service (DDoS) attacks. Effective cyber security defences, which include firewalls, intrusion detection structures, endpoint safety solutions, and worker education programs, are crucial for figuring out and thwarting those threats.
- **Safeguarding Digital Transactions:** With the upward thrust of online banking, cellular payments, and virtual transactions, monetary establishments need to ensure the safety of those virtual channels. Cyber security measures, which include encryption, stable authentication mechanisms, and transaction

tracking structures, help guard virtual transactions from interception, tampering, or unauthorized access.

6. VARIOUS FORMS OF CYBER CRIMES

Cyber crime incorporates a huge variety of unlawful activities devoted to the usage of computers, networks, and virtual technologies. These crimes can target people, businesses, governments, and vital infrastructure, posing sizeable monetary, social, and safety risks. Here are diverse kinds of cyber crimes.

- **Malware Attacks:** Malicious software (malware) is designed to infiltrate and damage computers without the user's consent. Types of malware consist of viruses, worms, Trojans, ransomware, spyware, and adware. Malware can compromise the integrity, confidentiality, and availability of facts and structures.
- **Phishing and Social Engineering:** Phishing includes the usage of misleading emails, messages, or web sites to trick people into revealing non-public facts, which include login credentials, monetary details, or social safety numbers. Social engineering strategies control human psychology to advantage unauthorized access.
- **Identity Theft:** Cyber criminals steal non-public facts, which include names, addresses, social safety numbers, and monetary facts, to impersonate people for fraudulent purposes. Identity robbery can cause monetary losses, broken credit score scores, and reputational damage for sufferers.
- **Online Fraud:** Online fraud encompasses diverse schemes geared toward deceiving people or corporations for monetary advantage. Examples consist of funding scams, credit card fraud, public sale fraud, false online stores, and romance scams. Cyber criminals take advantage of vulnerabilities in online structures to defraud victims of cash or treasured assets.
- **Data Breaches:** Data breaches contain unauthorized access to the data saved via the means of corporations or people. Cyber criminals may also take advantage of vulnerabilities in networks or structures to steal personal facts, which include patron records, monetary facts, highbrow property, or exchange secrets and techniques. Data breaches can bring about monetary losses, reputational harm, and criminal results for affected parties.
- **Cyber extortion**: Cyber extortion includes threatening people or corporations with damage until they pay a ransom. Common kinds of cyber extortion consist of ransomware assaults, wherein malware encrypts the victim`s facts till a ransom is paid, and dispensed denial-of-service (DDoS) assaults, wherein attackers disrupt on line offerings till a ransom is received.
- **Cyber bullying and Harassment:** Cyber bullying refers to the usage of virtual technologies, which includes social media, messaging structures, or on line forums, to harass, intimidate, or humiliate people. Cyber bullying could have extreme mental and emotional consequences for sufferers, leading to anxiety, depression, or even suicide in intense cases.
- **Cyber Espionage and Cyber Warfare:** Nation-states and state-backed actors have interaction in cyber espionage to steal sensitive data, highbrow property, or authority's secrets and techniques from different international locations or corporations. Cyber war includes the use of cyber assaults to disrupt or sabotage the vital infrastructure of adversaries, which includes electricity grids, communique networks, or monetary structures.
- **IoT (Internet of Things) Exploitation**: With the rise of linked gadgets, cyber criminals aim to exploit vulnerabilities in IoT gadgets to gain unauthorized access to, release assaults on, or steal data. IoT exploitation can cause privacy violations, data breaches, and disruptions to vital infrastructure.

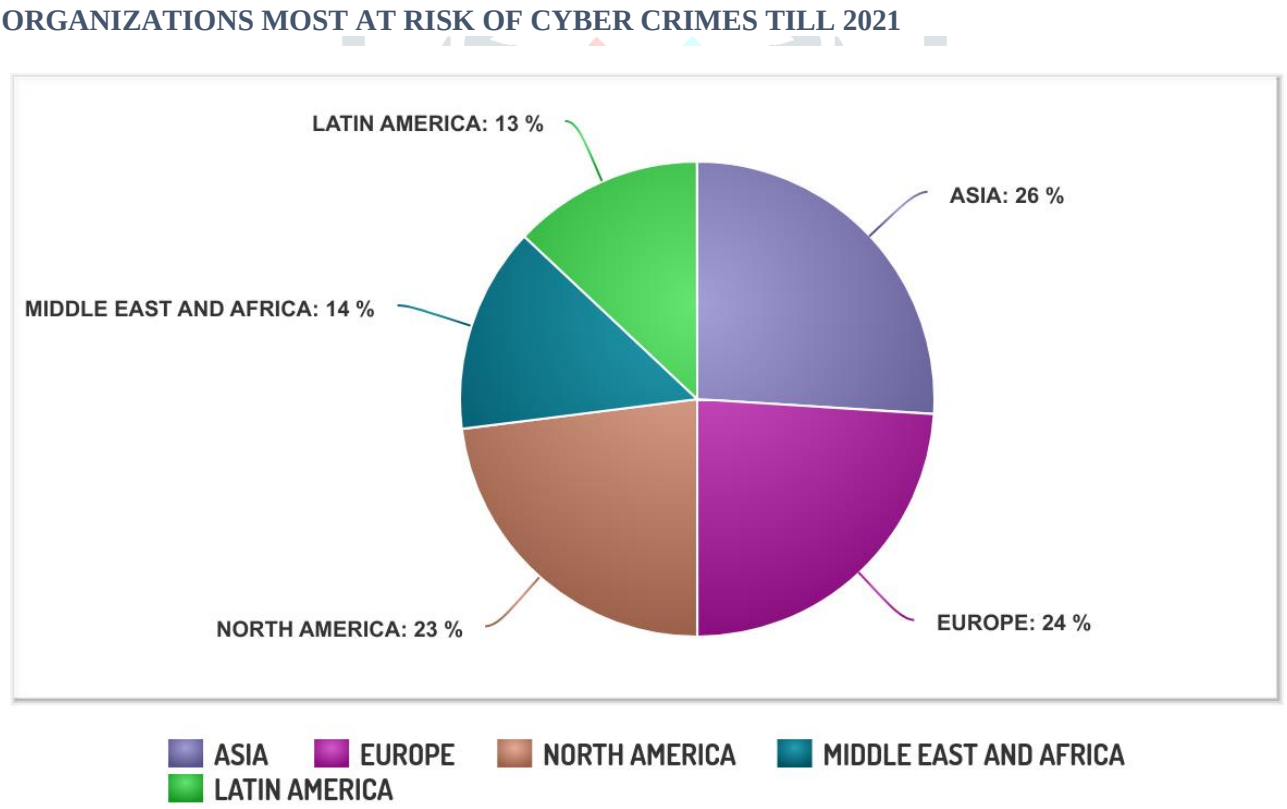
7. NATIONAL/INTERNATIONAL SCENERIO OF CYBER ATTACK

➢ **Countries having the strongest cyber security till December 2023**

- Poland (90.83)
- Estonia (85.83)
- Ukraine (80.83)
- Latvia (79.17)
- United Kingdom (75.00)

➢ **Organizations most at risk of cyber crimes:**

- Asia (26%)
- Europe (24%)
- North America (23%)
- Middle East and Africa (14%)
- Latin America (13%)



▪ **FIGURE - 1** Source – aag-it.com/.com

CYBER SECURITY IN INDIA

Last year, on November 30, the internet site of the Indian Council of Medical Research (ICMR) confronted round 6,000 hacking tries in 24 hours. This befell every week after 5 servers of the All India Institute of Medical Sciences (AIIMS) were hacked with the aid of using ransomware. A predicted 3 terabytes of information changed into encrypted. The hackers had made it not possible for AIIMS to get entry to its personal information.

On October 31, 2023, in a huge information breach, data of over 81.5 crore Indians with the ICMR have been offered at the dark web.

One such notable cyber attack was the breach of the Unique Identification Authority of India Aadhaar database, which exposed the personal information of millions of Indian citizens. This breach raised serious concerns about the security of India's national identity card system and the protection of citizens' personal data.

Separately, the Massachusetts Institute of Technology (MIT) Technology Review Cyber Defence Index (CDI) 2022/23 ranked India at No 17. MIT`s CDI is the `first-of-its-kind` annual comparative rating of the world`s 20 biggest and maximum virtual economies on their guidance against, cyber security threats, every other “India struggles, inspite of a digitally ahead authorities and the world`s biggest IT-enabled provider sectors. This effective tech pressure lacks essential infrastructure, has bad countrywide virtual financial system adoption, and susceptible cyber security regulation. Despite cyber attacks and requires cyber security legal guidelines and a committed ministry, India has opted out,” ET quoted the file as saying. The growing variety of cyber attacks has referred to as for a cyber security regulation and the established order of a committed ministry. Despite having the second one maximum variety of lively net customers after China, India represents best 6% of the worldwide cyber security jobs.

It is seen that cyber security is a critical concern in India, as the country has experienced significant growth in its digital infrastructure and technology adoption. With a population of over 1.3 billion people, India has become one of the world's largest internet user bases, making it a prime target for cyber threats. The Indian government has recognized the importance of cyber security and has taken several initiatives to enhance its cyber resilience. These initiatives include the establishment of the National Cyber Security Coordination Centre and the release of the National Cyber Security Policy. Moreover, India also faces unique challenges in terms of cyber security, including the rapid digitization of government services and financial transactions, as well as the increasing use of mobile devices for banking and other online activities.

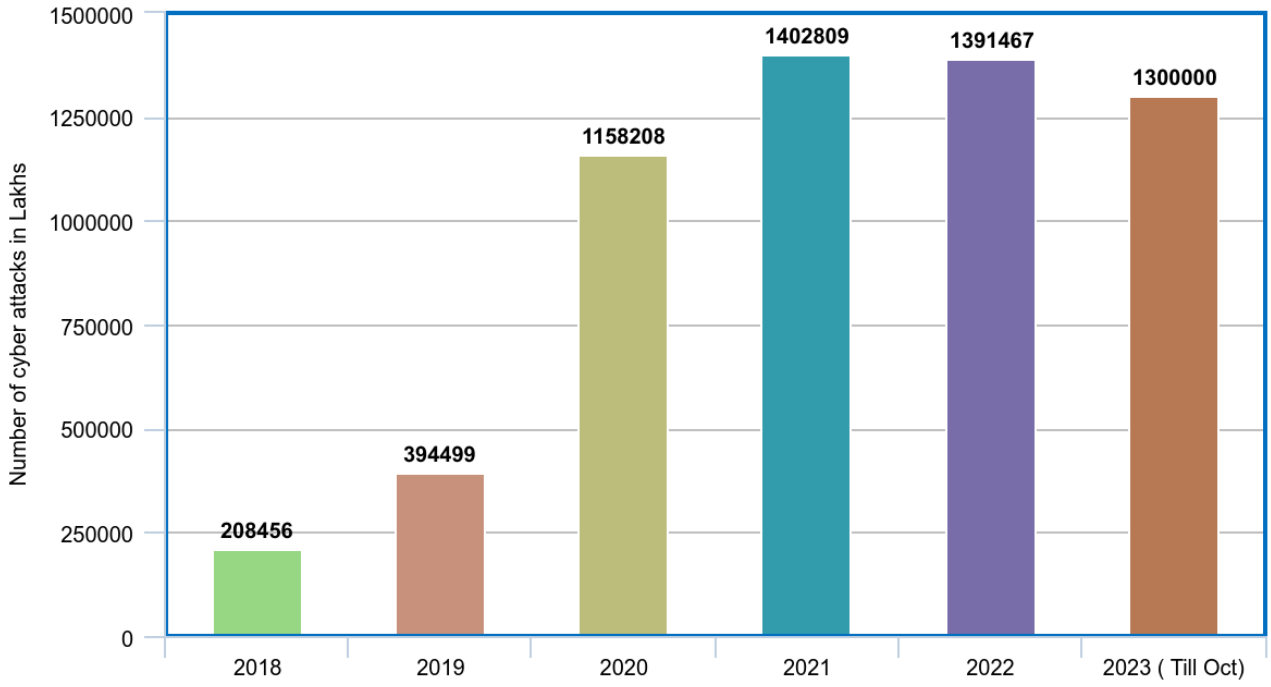
Like many countries, India is also suffering from increasing cyber crime. In 2018-208456 cases were reported, in 2022, in the first two months, there were 212485 reported cyber crimes, more than the entire 2018.

In the pandemic, figures rose more sharply, with crime jumping from 394499 cases in 2019 to 1158208 in 2020 an d 1402809 in 2021 between Q1 & Q2 in 2022 Cyber crime in India increased by 15.3x% when Indian organizations experienced a ransom attack in 2021.

The most common form of cyber crime in India is financial fraud. This accounted for 75% of cyber crime from 2020 to 2023.

According to Reserve Bank of India reports, India's financial sector faced more than 13 LAKH cyber attacks between January and October 2023. This means that banks and non-banking institutions faced around 4,400 cyber attacks every day this year.

NUMBER OF CYBER CRIMES IN PAST 6 YEARS IN INDIA



▪ **FIGURE - 2**

Source – statista.com

8. WAYS TO TACKLE CYBER SECURITY RISK FOR YOUR ORGANIZATION

- **Employee Training and Awareness Programs -** Employee training and awareness programs are crucial for reducing cyber crime. These programs act as a human firewall, educating employees to identify phishing attempts, malware, and social engineering tactics. By understanding these red flags, employees are less likely to fall victim to scams and more likely to report suspicious activity. Training also promotes secure data handling practices and fosters a culture of cyber security within the organization. These combined efforts significantly reduce the risk of data breaches, financial losses, and reputational damage for businesses.

- **Adopting Advanced Threat Detection Systems (ATDS)** – It acts as a powerful shield against cyber crime. These sophisticated systems go beyond traditional security measures by continuously analysing network traffic and user behaviour for unusuals. This allows them to identify even the most hooded cyber attacks, including zero-day threats that haven't been flagged yet. By catching threats early and enabling faster response times, ATDS significantly reduces the potential damage from cyber crime, protecting sensitive data and minimizing business disruptions.

- **Strengthening Authentication Procedures** - Strengthening authentication procedures acts as a powerful gatekeeper against cyber crime. Traditional methods like usernames and passwords are increasingly vulnerable. By implementing stronger authentication methods, organizations make it significantly harder for unauthorized individuals to gain access to sensitive systems and data. This includes:
  - **Multi-Factor Authentication (MFA)**
  - **Strong Password Policies**
  - **Biometric Authentication**

- **Regular Security Audits and Compliance Checks** - Regular security audits and compliance checks act as a double shield for financial institutions against cyber crime. These expert assessments uncover vulnerabilities internal teams might miss, allowing for early patching and a reduced attack surface. Additionally, compliance checks ensure adherence to data security regulations, preventing hefty fines and reputational damage. This multi-pronged approach not only deters attackers but also builds customer trust, ultimately reducing the risk of cyber crime.

- **Building a Culture of Cyber Resilience** - Building a culture of cyber resilience acts as a hidden armour against cyber crime. It empowers everyone, not just IT specialists, to be vigilant. Regular training educates employees to spot threats and report them. Open communication fosters a safe space for employees to voice concerns. Having a plan for cyber attacks minimizes damage. This cultural shift, with strong leadership backing, makes it much harder for cyber criminals to infiltrate the organization.

- **Leveraging AI for Enhanced Security Measures** - Leveraging artificial intelligence (AI) injects intelligence into our fight against cyber crime. AI-powered security solutions are like tireless cyber soldier, constantly analysing vast amounts of data to identify unusual and potential threats. These systems can detect sophisticated attacks. By automating threat detection and enabling faster response times, AI significantly reduces the window of opportunity for cyber criminals, minimizing damage and protecting sensitive data. This translates to a more proactive and effective defence against the ever-evolving landscape of cyber crime.

- **Partnerships with cyber security firms –** Partnering with cyber security firms strengthens an organization's defences against cyber crime. These firms offer a wealth of expertise and advanced tools. They can help organizations:

- Identify vulnerabilities:
- Implement advanced security solutions
- Stay updated on threats
- Incident response
- By combining their internal security efforts with the expertise of cyber security firms, organizations can create a more dependable defence system, significantly reducing the risk and impact of cyber crime.

- **Implementing Encryption Practices** - Implementing encryption practices throw a wrench into cyber criminals' plans. The encryption of data makes it unreadable without a decryption key. This adds a crucial layer of protection, especially for sensitive information like financial records, personal data, and intellectual property. Even if cyber criminals manage to steal encrypted data, it remains useless without the key, significantly reducing the risk of data breaches and financial losses for individuals and organizations.

9. CONCLUSION

In this paper we have detailed about the need and importance of cyber security. It is found that it is crucial for any organization to develop an alert system that effectively implements and integrates big data technologies into their system. Cyber crimes are increasing day by day and have a negative impact of cyber crimes. India faces increasing cyber threats due to its rapid digitization of government services and increasing use of mobile devices. Study found that there are various ways to tackle cyber threats that can create awareness among organization and customer, helping to prevent massive losses. Also the various forms in which cyber criminals can stole credential data and other important information that can cause serial damages to the institution or the whole industry. Conclusively, the study on cyber security in financial institutions highlights the increasing number of cyber crimes in organizations, and nations.

10. REFERENCES

1. I-Chiu Chang, His-Ginn Hwang, David C. Yen, Hen-Yi Huang (2006). Empirical study of the factors affecting internet security for the financial industry in Taiwan, *Telematics & Informatics Volume 23, Issue – 4,* 343 – 364.
2. Vuuren, Leenen, Phahlamohlaka, Zaaiman (2012). An Approach to Governance of Cyber Security I South Africa, *International Journal of Cyber Warfare and Terrorism (IJCWT),* 2(4), 13-27.
3. Goutam R.K (2016). Importance of Cyber Security, *International Journal of Computer Applications, Volume 111, 14* – 17.
4. Setiawan, Sastrosubroto (*2016).* Strengthening the security of critical data in cyberspace, a policy review, *International Conference on Computer, Control, Informatics and its Applications.*
5. Ghosh K. (2022). Cybersecurity in Digital India, *International Journal for Multidisciplinary Research (IJFMR),* 1 – 7.
6. "Ways to tackle cyber security risk for your organization" *https://www.upguard.com/blog/reduce-cybersecurity-risk/*
7. "Incidents of cyber attacks across India from 2015 to 2022" *https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/*
8. "State-Sponsored Cyber Attacks Against India Went Up by 278% Between 2021 and September 2023" *http://thewire.in/*
9. "Latest cyber crime statistics (2024)" *https://aag-it.com/the-latest-cyber-crime-statistics/*
10. "Online Safety is Everyone's Responsibility – Yes that means you" *https://blogs.cisco.com/security/online-safety-is-everyones-responsibility-yes-that-means-you/*