International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 14, Issue 3 [March. 2025] PP: 126-131

Cybersecurity in the Indian Scenario

Gaurav Singh Rana[1], Amardeep Singh[2], Manish Gupta[3], R. Chitra[4]

[1] Scientist B, [2, 3] Scientist E, [4]Director,
Central Soil and Materials Research Station, New Delhi

Abstract
In the ever-evolving world of digital innovation, the surge of emerging electronics and software technologies brings both unprecedented opportunities and formidable challenges, particularly in the realm of cybersecurity. Cyberattacks are becoming increasingly sophisticated. With the rapid growth of emerging technologies such as digital media, 5G, generative AI, and robotic automation processes, the incidence of cyberattacks is rising unexpectedly. Emerging technologies often create more opportunities for cyberattacks and data breaches. Developing countries, with relatively weak surveillance capacity, are most vulnerable to cyberattacks. India has witnessed rapid digitalization across nearly all spheres of public life, with over 1.2 billion phone users and more than 700 million Internet users—a number that continues to grow. The rapid growth of digital media has provided easy access to various online services even for the rural population of India. Initiatives such as Make in India and Digital India are creating a positive ripple effect across online services, including government and commercial services.

The study begins by establishing a clear understanding of various key elements of cybersecurity and highlighting its importance in the current digital realm. This paper aims to provide a comprehensive analysis of the current state of cybersecurity in India, including the government, private sector, and general public. It then examines the various cyber threats that individuals, the public, and the private sector in India face on a daily basis, including ransomware, malware infiltrations, phishing, and data breaches, among others. This paper also highlights the proactive steps that have been taken by Indian administrations. It emphasizes the importance of continuous efforts to improve cybersecurity, as well as cybersecurity education and awareness among individuals and various organizations. Additionally, this paper highlights various steps taken by the Indian government to strengthen cybersecurity.

Keywords:*cybersecurity, information and communication technology,cyberattacks,digital realm*

I. Introduction

As the world advances in the realm of digitalization, the threat of cyberattacks has grown, and India is no exception. Over the last few years, the cybersecurity landscape in India has become quite unstable. While spending on cybersecurity has increased significantly, the number of cyberattacks has shown no signs of slowing down. In Q1, 2024, 20% of internet users in India experience Cyberattacks [1]. Information and Communication Technology (ICT) has become ubiquitous among government ministries and departments across the country. Due to the lack of proper cybersecurity practices followed on the ground and the increased use of ICT, the attack surface and threat perception to government organizations have increased. Despite growing awareness among both private and public organizations in India, hospitals, oil and gas majors, banks, government organizations, telecom vendors, diagnostic labs, and even restaurant chains have become victims of cyberattacks.

Cybercrime is unique in its modus operandi compared to other types of crimes due to its distinct characteristics. Unlike traditional crime, cybercrime has no territorial boundaries, and identifying the criminals can be extremely challenging. The anonymity provided by ICT has created significant challenges for law enforcement agencies, government organizations, private organizations, and individuals affected by cybercrime. All segments of society, including individuals, the government, and private businesses, bear the impact of cybercriminal activities. The rapid digitalisations in India and increased connectivity have created new opportunities for cybercriminals to exploit vulnerabilities in ICT. Therefore, it has become necessary to analyse the nature of cybercrime in India, its various forms, and simultaneously take steps to resolve the issues created by cybercrimes.

A nation's legislative and regulatory frameworks pertaining to cyberspace, as well as its national cybersecurity strategy, need to be updated and developed with greater agility. As cybercrime knows no boundaries in digital realms, governments around the world have implemented legislation and established specialized law enforcement units and cybersecurity agencies to address it. The main aims are to discourage cybercriminals, speed up the investigation of cybercrimes, and ensure that offenders are held accountable for their illegal actions. Further, by raising awareness among the general public and adopting robust cybersecurity measures—such as creating and regularly changing strong passwords, avoiding pirated software, and implementing encryption and firewalls for networks and personal computers—government and private organizations, as well as individuals, can mitigate the risks posed by cybercrime.

1. Cybersecurity

Cybersecurity is the practice of protecting internet-connected systems, programs and networks from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processesand government services. There are currently more devices than humans, making it extremely hard to implement efficient cybersecurity safeguards, and attackers are getting more innovative.

2. Most Common type of Cyber Attacks

A. **Ransomware attack:** Ransomware is a type of malware that blocks access to the system or encrypts its data, hereby forbidding users from accessing their system or files [2].The malware is designed to exploit security vulnerabilities that neither the IT department nor the system's manufacturer has fixed. Ransomware can occasionally attack single or multiple targets to block access to System or files[2].

B. **Whale-phishing attack:** If a targeted "whale," i.e., a high-level executive or official, downloads ransomware, he or she is more likely to pay the ransom to prevent news of the successful attack from getting out and damaging their reputation or that of the organization. Whale-phishing attacks can be prevented by carefully examining emails and their attachments and links, and with the cybersecurity education and awareness among individuals[3].

C. **Malware attack:** It aims to exploit internal weaknesses of the system with the goal of steal, modify, and destroy information and/or physical components of the system[4]. It can also obtain unauthorized access to the system without the end user's knowledge.Most malware type can be classified as virus, worms, Trojan, hybrid malware, adware spyware etc.

D. **Trojan horses:** Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. When the user executes the presumably genuine program, the malware within the Trojan can open a backdoor into the system, allowing hackers to penetrate the computer or network[5].

E. **Session hijacking:** Session Hijacking is an attack which is basically used to gain the unauthorized access between an authorized session connections[6].Session hijacking sometimes called cookie hijacking, cookie side-jacking, or TCP session hijacking occurs when an attacker takes over your internet session..[6].
Numerous additional types of cyber-attacks exist.

3. Cyber Security Goal

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. To achieve this, there are three fundamental goals of cybersecurity

i. Protect the confidentiality of data
ii. Preserve the integrity of data
iii. Promote the availability of data to approve users only.

These three form the confidentiality, integrity and availability (CIA) triads, the basis of all security programs.This model also refers as availability, integrity and confidentiality (AIC).For data to be completely secure, all of these security goals must come into effect.

i. Confidentiality

Confidentiality is the "prevention of disclosure of information from unauthorized user".Information has confidentiality when it isprotected from disclosure or exposure to unauthorized individuals or systems [4]. Various tools can be used to maintain confidentiality, such as access control, authentication, authorization, encryption, and physical security and others.

ii. Integrity

Integrity is the "prevention of modification of information from unauthorized user.Information has integrity when it is whole, complete, unmodified oruncorrupted[4].Tools used to ensure integrity include checksums, backups, and error correction codes and others.

iii. Availability

Availability is the “right information accessed by right person at the right time”. Availability enables authorized users, people, or computer systems to access information without interference or obstruction andto retrieve it in the required format[4]. Tools used to ensure availability include physical protection and computational redundancies and others.

To achieve these three goals, the following steps can be taken:

- Policies should be updated regularly to handle risks, based on previous assessments.
- Categorize the importance of data and apply security measures, such as encryption and two-factor authentication, accordingly.
- Provide access based on position and precedence, with the goal of keeping backup data safe.
- Determine the method and policy of security safeguards for each threat.
- Monitor each breach activity and manage data accordingly.
- Keep access control lists and other file permissions regularly updated.
- Use backup and recovery tools and services, and keep applications and systems regularly updated.
- Use access control, version control, security control, data logs and checksum.
- Keep data recovery plan in case of data loss.
- Use preventive measures, such as redundancy, failover, and RAID.

It has a lot of positive aspects. As the name implies, it provides network or system security, and as we are all aware, safeguarding anything has several benefits. It provides safeguarding, such as the protection of personal data as well as data related to government and private organizations. It hampers illegal access to confidential and important data, and it secures society from cyber-attacks.

Cybersecurity delivers various protections, such as protection from information theft, defence of workstations from theft, a sense of security for internet users, protection of sensitive and important personal information, and a reduced chance of PC freezing. It protects individuals from financial loss and defamation. It also protects individuals from cyber-attacks.

Cybersecurity make network secure, it enhance network security. Establishing strong cybersecurity protocols can greatly enhance an organization's defence against cyberattacks. To protect sensitive data and information, these precautions entail implementing cutting-edge technologies like firewalls, encryption, and multi-factor authentication.

4. Cybersecurity Initiative by India

In today's high-tech digital realm, the best way to safeguard an organization's IT infrastructure is to maintain appropriate cybersecurity measures and regularly update cybersecurity guidelines. Not only do these risks harm corporations, but they also harm government institutions. The adoption of cybersecurity measures by the Indian government would mitigate these risks and help maintain a secure online environment for citizens as well as for the various organizations. The Indian government has launched a number of programs and policies to combat cybersecurity issues in the country in order to address these issues.

- **The Indian Computer Emergency Response Team (CERT-In):**In order to manage cybersecurity problems and plan incident response actions, the CERT-In is essential. In India's cyberspace, it serves as the main organisation for incident response, vulnerability management, and security management[7].
- **Cyber Swachhta Kendra:**The “Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. It is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections[7].
- **Cyber Surakshit Bharat:** The Cyber Surakshit Bharat was introduced by the Ministry of Electronics and Information Technology (MeitY) in collaboration with the National Electronic Governance Division (NeGD) to augment the government's vision of "Digital India." The purpose of this campaign is to raise public awareness of current cybercrimes and India's cybersecurity issues[7].
- **National cybersecurity policy [7]:** The Data Security Council of India (DSCI), led by Lt. General Rajesh Pant, created the National Cyber Security Strategy in 2020. The research focused on 21 areas to guarantee India’s cyberspace is safe, secure, trustworthy, resilient, and dynamic.In 2022, the Parliament was presented with the updated National Cyber Security Strategy 2021, which adopts a comprehensive approach to addressing national cyberspace security issues[7].
- **National Critical Information Infrastructure Protection Centre:** NCIIPC, a unit of NTRO, is an organization of the Government of India created under Section 70A of the Information Technology Act, 2000 (amended in 2008)[8].

○ Vision: To facilitate a safe, secure, and resilient information infrastructure for the critical sectors of the nation.

○ Mission: To take all necessary measures to facilitate the protection of critical information infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation, or destruction through coherent coordination, synergy, and raising information security awareness among all stakeholders.

5. Need for Cybersecurity in India:

The significance of cyberspace in India is expected to continue expanding with the vision of a trillion-dollar digital economy [14]. Indians have adopted mobile broadband like fish to water, thanks to low-cost smartphones, affordable tariffs, and increased availability of audio-visual content in Indian languages. With this rapid growth of digitalization, cybersecurity and safety have become imperative issues for India.India has witnessed the total number of Internet subscribers increase from 88.1crore at the end of March 2023 to 95.4crore at the end of March 2024, registering a quarterly growth rate of 8.3% [9].

Internet penetration rate in India from 2014 to 2024

The internet penetration rate in India rose over 52 percent in 2024, from about 14 percent in 2014, which is presented in figure 1 [10]. Although these figures seem relatively low, it meant that more than half of the population of 1.4 billion people had internet access that year. This also ranked the country second in the world in terms of active internet users.

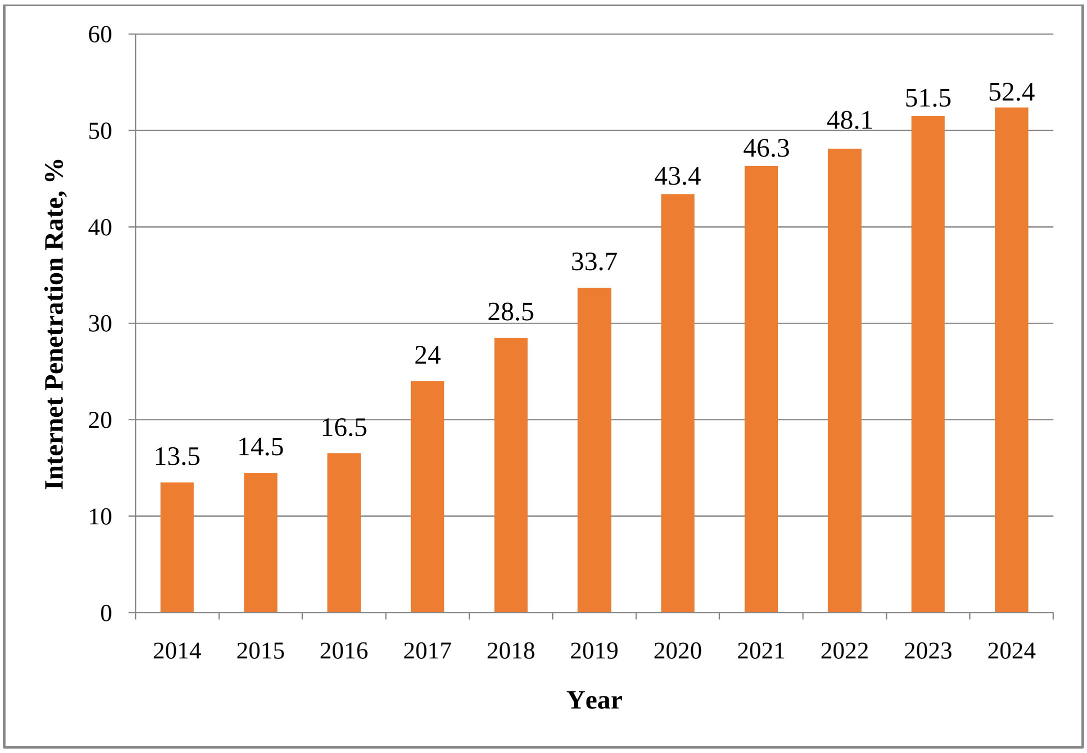

Figure1: Internet penetration rate in India from 2014 to 2024

(Source: www.statista.com)

Growth of Digital payments in India

Digital payments have significantly increased in recent years, as a result of coordinated efforts of the Government with all stakeholders. The Minister stated that the total digital payment transactions volume increased from 2,071 crore in FY 2017-18 to 13,462 crore in FY 2022-23 at a CAGR of 45% and crossed 10,998 crore during current financial year till 27.11.2023 [11]. The details of the progress made in the number of digital payment transactions during the last three years and current year are presented in Table 1:

Table 1: Digital payments in FY2023-24 cross 10,998 crore as on 27.11.2023

Financial Year	Target (in crore)	Achievement (in crore)
2020-21	5,500	5,554
2021-22	6,000	8,839
2022-23	13,233	13,462
2023-24 Till 27th Nov'2023	18,000	10,998

(Source: https://pib.gov.in/)

India currently ranks second with just under half of its population **(49.15%)** using the internet - that accounts for **692 million** people [12],which is presented in figure 2.

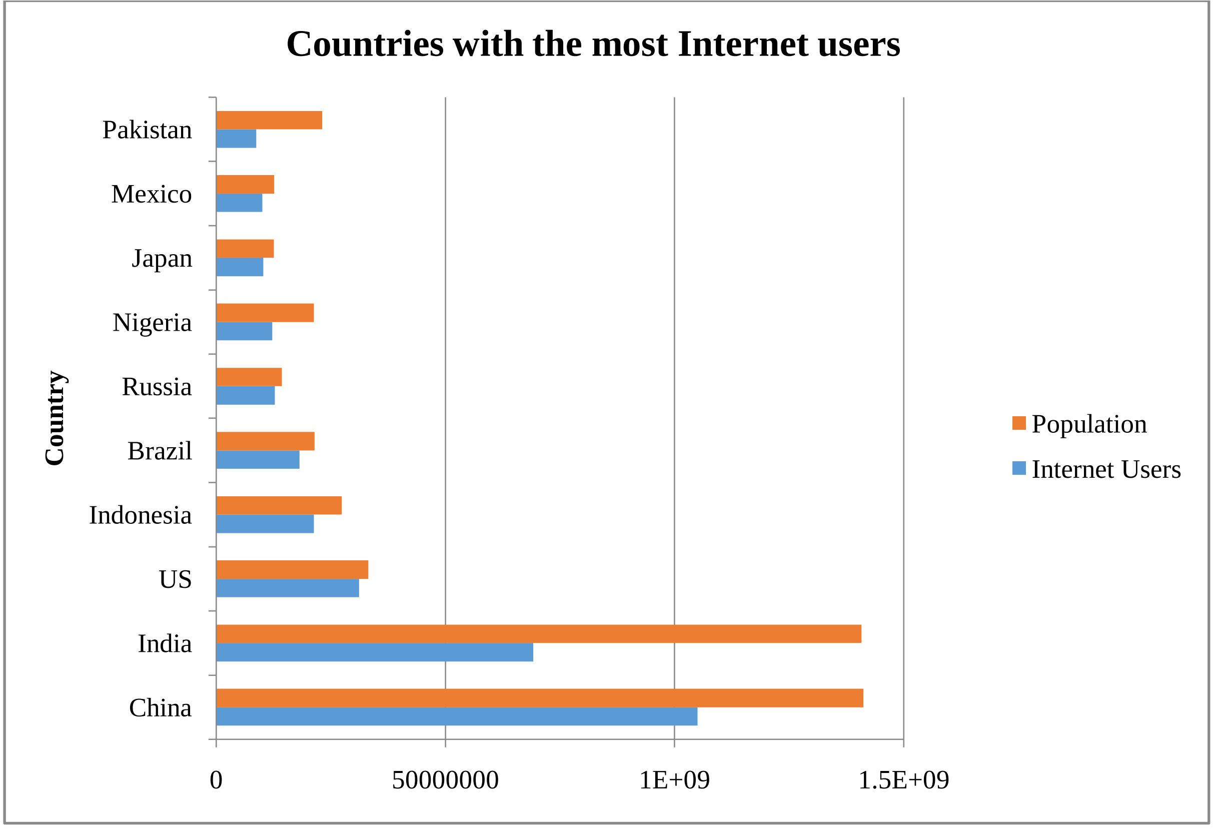

Figure 2: Countries with the most Internet users
(Source: https://explodingtopics.com/blog/countries-internet-users)

India's cyber security workforce

An estimated 4 million professionals are needed to fill the growing cybersecurity workforce gap. At the same time, Fortinet's 2024 Global Cybersecurity Skills Gap Report found that 80% of Indian organisations indicated that the cybersecurity skills shortage creates additional risks for their organizations [13].

According to the data, the digitalization rate in India is significantly high. More than half of the population of India is using the internet. India is in second place on the list of internet users in the world. The total volume of digital payment transactions has increased significantly. This data clearly indicates that India is a rapidly growing country, particularly in the field of the digital economy. It is crucial for India to prioritize cybersecurity due to the rising threats of cyberattacks and the country's growing reliance on digital technology. By implementing robust cybersecurity safeguards, India can defend its vital IT infrastructure, secure the privacy and personal data of its citizens, and guarantee the ongoing growth of its digital economy.

II. Findings

- The internet has significantly penetrated rural India, making it essential to spread cybersecurity awareness in these areas.
- India has taken several initiatives to improve cybersecurity.
- There is a significant gap between the demand and supply of cybersecurity professionalsin India.
- There is low awareness of cybersecurity among the general public, which is a major cause of cybercrime.
- Overall, to achieve the vision of a trillion-dollar digital economy [13], India requires digital inclusion from every corner of the country. As a result, cybersecurity has become crucial for India. Therefore, it is necessary to address the issue of cybersecurity to continue digitizing and integrating into the global economy.

III. Conclusion:

In conclusion, with the rise of digital India, cybersecurity has become a major concern. The rate of growth of cyber-attacks has increased significantly, which clearly indicates that more needs to be done to strengthen the posture of cybersecurity in India and to lessen the rising fear related to cyber-attacks among citizens. India has taken several steps, but much remains to be done. India should implement strong data protection laws, ensuring compliance with international standards, and emphasize the use of encryption technologies to secure sensitive personal data. Cybersecurity measures need to be updated regularly. Developing a comprehensive cybersecurity policy that is followed by all government and private organizations is essential. This policy should also provide guidelines for incident response and recovery. There should be strong collaboration between the government and private sector to identify and mitigate cybersecurity risks. With the advancement of new technology, cyber-attackers are becoming more innovative, so it is necessary to increase investments in research and development of cybersecurity to come up with new creative and innovative ideas to identify and mitigate cybersecurity issues. It is also important to increase cybersecurity awareness; the government should launch a national cybersecurity campaign to educate the public, small businesses, and other vulnerable segments of the population about cyber risks and threats, including schools, small and medium-sized businesses, and individuals.

References:

[1]. "2024 Cybersecurity Outlook," (Jul. 8, 2024). Available at: https://www.dsci.in/resource/content/2024-cybersecurity-outlook (Accessed: 27 August 2024).

[2]. Manuj Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," in: Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), July 2023.

[3]. VaishnaviBhavsar, "Study on Phishing Attacks," International Journal of Computer Applications, 0975, December 2018.

[4]. C.P. Gupta, K. K. Goyal, Cybersecurity: A Self-Teaching Introduction

[5]. Dr. JeetendraPande, Introduction to Cyber Security. Haldwani: Uttarakhand Open University, School of CS & IT.

[6]. Baitha, A. K., "Session Hijacking and Prevention Technique," International Journal of Engineering & Technology, March 2018.

[7]. "Government Initiatives for Cybersecurity in India,". Available at: https://ccoe.dsci.in/blog/the-role-of-government-initiatives-in-tackling-cybersecurity-challenges-in-india (Accessed: 27 August 2024).

[8]. "National Critical Information Infrastructure Protection Centre,". Available at: https://nciipc.gov.in/RVDP.html (Accessed: 27 August 2024).

[9]. "Indian Telecom Sector Records Remarkable Growth in 2023-2024," (Aug. 20, 2024). Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2046870#:~:text=Surge%20in%20Total%20Internet%20Subscribers,in%20the%20last%20one%20year. (Accessed: 27 August 2024).

[10]. "Internet penetration rate in India from 2014 to 2024," (May 15, 2024). Available at: https://www.statista.com/statistics/792074/india-internet-penetration-rate/ (Accessed: 27 August 2024).

[11]. "Total digital payment transactions volume increased from 2,071 crore in FY2017-18 to 13,462 crore in FY2022-23 at a CAGR of 45%," (Dec. 11, 2023). Available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1985240 (Accessed: 27 August 2024).

[12]. "Countries with the Highest Number of Internet Users," (May 7, 2024). Available at: https://explodingtopics.com/blog/countries-internet-users (Accessed: 27 August 2024).

[13]. “Fortinet Annual Skills Gap Report Reveals Growing Connection Between Cybersecurity Breaches and Skills Shortages in India”, (Aug 12, 2024) Available at:https://www.crn.in/news/fortinet-annual-skills-gap-report-reveals-growing-connection-between-cybersecurity-breaches-and-skills-shortages-in-india/#:~:text=An%20estimated%204%20million%20professionals,additional%20risks%20for%20their%20organizations (Accessed: 27 August 2024).

[14]. “Report on India’s Trillion Dollar Digital Opportunity Released”, (Feb 20, 2019), Available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1565669 (Accessed: 27 August 2024).