ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 2, Issue 2, (Jul-Dec) 2025

Recent Cyberattacks in USA and India: A Comparative Analysis

Sandesh Waghmare
Student, Department of Computer Science
Christ College
Pune, India
sandesh.sameer@christcollegepune.org

Nisha More
Assistant Professor, Department of Computer Science
Christ College
Pune, India
nisha.more@christcollegepune.org

***Abstract*—-This research paper conducts a comparative analysis of recent cyberattacks in the United States and India and identifies knowledge gaps in the field of cybersecurity. Both countries have witnessed a lot of cyberattacks targeting critical infrastructure, government agencies, and private enterprises, exposing significant vulnerabilities in their cybersecurity frameworks. The types of cybersecurity domains and threats faced are listed, and an effective analysis of existing cy- cybersecurity measures in mitigating these threats is done. By comparing the strategies used by the USA and India, the research paper examines best practices for enhancing cybersecurity resilience. The findings underscore the need for a coordinated global effort to combat cyber threats and point out the importance of investing in advanced cybersecurity technologies and awareness programs to shield our digital ecosystems as a scope of the future..**

***Index Terms*—Cybersecurity, cyberattacks, ransomware, threat, phishing, CyBOK, HackerOne, DDoS.**

I. Introduction

A. Overview of Cyberattacks in the Digital Era

Cyberattacks have become a worrying and widespread trend in the digital age. Malicious acts come under Cyberattacks, such as data breaches, ransomware attacks, hacking, phishing etc. They attack traditional computer systems and critical infrastructure, as well as financial institutions, healthcare organizations, and government agencies. Over time, the number of information breaches has increased, hampering the operations and causing financial losses.

Factors including the rapid expansion of the digital realm, increased dependence on technology, and the extensive expansion of Internet of Things (IoT) devices have made it possible for the danger landscape to grow. Various factors, such as commercial or industrial espionage, activism, or state-sponsored cyberwarfare, might be the driving force behind cyberattacks. Even though cyber dangers are constantly evolving, it's crucial to get a sneak peek into how attacks are perceived, how they affect society, and what can be done to lessen them.

B. Highlighting the Significance of Understanding and Addressing Threats

Identifying and combating cyberthreats is easy. If the increasing number of cyberattacks is not promptly addressed, there could be serious repercussions, including monetary loss, damaged reputation, invasion of privacy, and even disruption of national security. The risk might vary from financial theft and loss of sensitive data to interruption of vital services for both individuals and organisations. Public safety, geopolitical stability, and essential infrastructure are all impacted by cyberattacks in the national context.

Given how linked the international economy is becoming, a breach anywhere in the world affects people and businesses well beyond the original target. Due to the interconnectedness of cyberspace, effective countering of cyber threats requires international cooperation and coordination. Additionally, the fast-paced nature of technological innovation

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 2, Issue 2, (Jul-Dec) 2025

has made it increasingly challenging to predict and defend against new attack vectors, leaving the public and private sectors susceptible.

II. Literature Review

A. Insight into the current cybersecurity ecosystem

The ever-evolving digital landscape in the United States and India has seen a rapid increase in the importance of cybersecurity in recent years. As these two nations become more interconnected and digitally dependent, understanding the current cybersecurity landscape is essential for comprehending the challenges and vulnerabilities they face.

B. Cybersecurity Landscape in the USA

In the United States, cybersecurity has assumed a central role in national security and economic stability. The country's extensive digital infrastructure is a lucrative target for a wide array of threat actors, including criminal organizations, hacktivists, and state-sponsored groups. Recent reports highlight the prevalence of cyberattacks targeting critical infrastructure, government institutions, financial services, and healthcare systems. Key agencies like the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) play vital roles in mitigating these threats. The USA's National Institute of Standards and Technology (NIST) has also developed the NIST Cybersecurity Framework to guide organizations in enhancing their cybersecurity posture.

C. Cybersecurity Landscape in India

India has seen comparable cybersecurity issues due to its rapidly expanding digital economy. Cybercriminals find it an appealing target due to the quick growth of digital payments, e-governance, and internet connectivity. Ransomware, phishing, and data breaches that impact both public and commercial organisations have become more common in India. In tackling these issues, the Indian Computer Emergency Response Team (CERT-In) has taken the lead. India's National Cyber Security Policy, which was introduced in 2013, also provides measures for strengthening the nation's cybersecurity capabilities.

III. Research Design

To comprehensively understand the cybersecurity landscape, a mixed-methods research design was adopted. This design combines both qualitative and quantitative approaches to provide a holistic perspective. Data was gathered from multiple sources, including:

- Cyberattack Reports: An in-depth analysis of cyberattack reports, post-incident investigations, by which the tactics, techniques, and procedures were understood in recent cyberattacks.
- Government Documents: Government publications, policy documents, and cybersecurity strategies from the United States and India were reviewed to gain information of the approaches and initiatives taken to mitigate cyber threats.

A. Quantitative Analysis

Cyberattack data was analysed quantitatively, using statistical techniques, to find patterns and similarities in attack targets, vectors, and effects. This method offered a foundation for unbiased comparisons between the two nations.
Alper Ozcan, Emrah Donmez, and Ahmet Kasif conducted an online survey as part of their research paper in order to obtain an online poll for their study [1]. In the investigation, CyBOK version 1.0 was utilised. The first section of the form asks about degrees, roles, and graduation year, among other demographic enquiries. Participants were asked about their academic educations, their knowledge of the aforementioned subdomains of cybersecurity in the CyBOK, and the relative importance of each topic in the workplace.

It is evident from the scatter-plot graphic above that the sub-KA clusters are restricted. This suggests that respondents share a common view regarding the importance of the sub-KA and the educational attainment of a given KA. We do not, however, have a topic among the CyBOK KAs [2] that is heavily emphasized in university curriculum but receives little attention in reality. Conversely, the average learning rating is roughly 1 out of 4, suggesting that college education is often subpar.

ISSN (Online):3048-5088
International Journal of Advancement and Innovation in Technology and Research (IJAITR)
Volume 2, Issue 2, (Jul-Dec) 2025

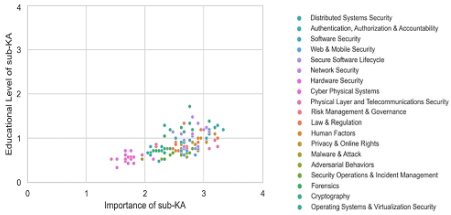

Fig. 1: Respondents' Perceptions about Importance vs Learned Topics in University by Sub-Knowledge Awareness (KA)

This observation, however, is not negative. It is challenging for university curricula to adequately handle the wide range of cybersecurity concepts and challenges. The majority of universities thus focus on giving graduates the fundamental skills that employers demand. Students must therefore acquire the requisite experience as they progress in their careers.

B. Qualitative Analysis

The qualitative information was gathered from cybersecurity experts' films. The specialists' findings offer a deeper comprehension of the arbitrary elements of cybersecurity. In this part, recent cyberattacks in the US and India are analysed, providing a comparative viewpoint on the types, targets, and consequences of these attacks. By closely examining the details of these instances, this analysis seeks to find similarities and contrasts between the assault methods and strategies used in the two countries

1) Types of Attacks:

- **Data Breaches:** Cybercriminals and threat actors target organizations to gain unauthorized access to sensitive data. This data is often used for financial gain or to undermine the reputation of the victim.
- **Ransomware Attacks:** Ransomware attacks have become significantly more common. Attackers threaten the availability of data by encrypting it and then demanding a ransom in return for the decryption key.
- **Phishing Campaigns:** Attackers use social engineering techniques to trick people and organisations into disclosing private information or downloading malicious software, a tactic known as phishing that is still commonly used today.
- **State-Sponsored Attacks:** Nation-state actors engage in cyber espionage and cyber warfare, targeting government agencies and critical infrastructure to gain strategic advantages or disrupt operations.

C. Similarities and Differences in Attack Vectors and Tactics

Although the cyber dangers faced by both countries are comparable, there may be differences in the specifics of these attacks. The use of well-known attack vectors, like phishing, is one area where there are typically similarities. However, targets and reasons might vary. Comprehending these similarities and distinctions is essential for developing efficacious cybersecurity tactics and reducing risks at the domestic and global tiers.

1) Targets:

- **Government Agencies:** Both nations have witnessed cyberattacks on government institutions, affecting national security and public services.
- **Critical Infrastructure:** Attacks on critical infrastructure, such as energy grids, water treatment facilities, and transportation systems, have exposed vulnerabilities that can have far-reaching consequences.
- **Healthcare:** The healthcare sector has become a prominent target, particularly amid global health crises, threatening patient data and the delivery of medical services.
- **Private Sector:** Private companies across industries face constant threats, with financial institutions and technology firms being prime targets.

D. Impacts

- **Financial Losses:** Organizations suffer financial setbacks due to data breaches, ransom payments, and disruption of business operations.
- **Reputational Damage:** Data breaches erode trust, damage reputation, and result in potential legal and regulatory consequences.

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 2, Issue 2, (Jul-Dec) 2025

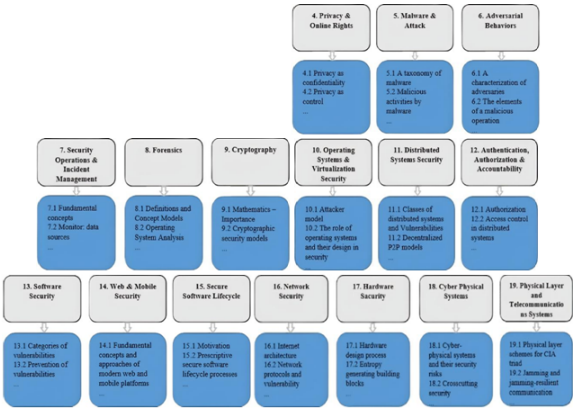

Fig. 2: The charts illustrate the complete overview of the cybersecurity domains.

- **Service Disruption:** Critical infrastructure attacks can lead to service outages, affecting public safety and daily life.
- **National Security Concerns:** Attacks on government agencies and infrastructure pose national security risks and can have geopolitical implications.

IV. Top 5 Cyberattacks in the USA

A. Rackspace Ransomware Attack

When consumers encountered difficulties attempting to access their Exchange environment on December 2, 2022, Rackspace Technology discovered that the problem was actually a ransomware attack. [3].

No indications of the theft of any sensitive user data have been found thus far. According to security analysts, the ransomware attack's root cause was an unpatched version of the Exchange cluster that gave the attackers access to the ProxyNotShell vulnerability. [4].

B. Cisco faces an attack by UNC2447, Lapsus$, & Yanluowang

In late May, Cisco announced that their corporate network was penetrated by the UNC2447 cybercrime gang, Lapsus$ threat actor group, and Yanluowang ransomware operators. The actors attempted to blackmail them by threatening to post 2.75GB of stolen material online. [5].

Researchers found throughout the investigation that an attacker had gained access to the personal Google account where the victim's saved browser credentials were synchronised, compromising the credentials of a Cisco employee.

C. Uber's Internal Systems were breached by a Teenager

The internal systems of Uber were breached on September 15, 2022. In addition to having complete administrator access to the company's AWS Web Services and GCP accounts, the attacker gained access to the HackerOne and Slack accounts. [6]

The initial assault was a social engineering scheme directed at Uber staff members. In addition to temporarily disabling several of its internal systems due to the attack, Uber is currently conducting an investigation. [7]

D. Sensitive NATO Data Leaked After Cyber Attack

According to a Portuguese news outlet, the Portuguese Department of Defence was the target of a cyberattack on September 8, 2022, which resulted in the release of classified NATO papers that are sold on the dark web. [8]

According to an examination, the material was sent via unprotected channels. Created to obtain sensitive data, it was deployed via a botnet and exfiltrated in a manner that made it undetectable. [9]

E. Russian Hacktivists, Killnet, Take Down US Airport Websites

Hackers who support Russia claimed credit for breaking into multiple airport websites in the United States. Just another DDoS attack by the infamous hacker collective "Killnet" against US airport websites. [10]

In 2022, during Russia's invasion of Ukraine, the pro-Russian hacker collective Killnet launched many distributed denial of service (DDoS) and denial of service (DoS) attacks against private businesses and government organisations across the globe.

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 2, Issue 2, (Jul-Dec) 2025

V. Top 5 Cyberattacks in India

A. ICMR Data Breach

The Indian Council of Medical Research (ICMR) has been the target of multiple cyberattack attempts. One of these breaches involved a "threat actor" using X to advertise the database for sale on the dark web [11]. 81.5 million Indian individuals' personal information was reportedly stolen from the ICMR's COVID-19 testing database.

The victims' names, ages, genders, residences, passport numbers, and Aadhaar card numbers were among the information found on the dark web, according to Resecurity, a security firm that discovered it on October 23, 2023. A [12] Cyber Attack on the Indian Power Sector A cyberattack in October 2020 targeted the Indian electricity industry, causing a blackout in several areas of Mumbai, including ports and airports such as Jawaharlal Nehru Port, VOC, and Tuticorin. The country's vital infrastructure was found to have vulnerabilities as a result of this catastrophe. In [13], because of the incident's sophistication, attackers will take advantage of any vulnerability, underscoring the necessity of ongoing surveillance and quickted nature of the incident shows adversaries will exploit any weakness, reiterating the need for constant monitoring and rapid response. Overall, the event serves as an important lesson to reinforce collaboration at all levels to ensure critical national infrastructure remains secure.

B. DDoS Attack on G20 Website

A large DDoS (Distributed Denial of Service) attack on vital digital infrastructure caused significant disruptions at the G20 Summit 2023, which was hosted in India. [14] The goal of the attack was to disrupt the event's seamless functioning by overloading government websites and communications channels.

Although the incident highlighted cybersecurity vulnerabilities and raised concerns about the growing potential of cyberattacks at significant world events, authorities acted quickly to contain the damage.RailYatri Data Breach RailYatri, a well-known website for railway information in India, had a huge data breach in 2023 that revealed private user information. Cunning cybercriminals broke into the platform's database and stole travellers' personal information, including phone numbers and email addresses. More than 31 million user records were stolen and were discovered being sold on the dark web. The hacked database had personal information such names, email addresses, phone numbers, mailing addresses, UPI IDs, travel information, and payment records. [15] The incident has made many very worried about the cybersecurity of Indian Railways and the RailYatri platform. It also made it clear how much the country has to improve its cyber defences to properly protect its growing internet population.Ransomware Attack on AIIMS

Cybersecurity attacked AIIMS (All India Institute of Medical Service) on November 23, 2022. This attack made it harder for patients and clinicians to get primary care services, such as billing, discharge, and patient admission systems.

According to an investigation by responsible parties, five of the AIIMS servers were impacted and almost 1.3 TB of data was stolen [16].

The Computer Emergency Response Team (CERT) has put out the "India Ransomware Report H1-2022," which talks about the most recent methods and tactics used by ransomware attackers and gives specific advice on how to respond to and stop ransomware attacks. [17]

VI. Steps to Improve Cybersecurity Awareness

A. Education and Training:

Cybersecurity training and education programs are very important for creating a workforce that can handle cyber threats. These programs might include a wide range of activities, such as formal education at schools and colleges, on-the-job training, and certifications.

a. Academic Programs: Colleges and universities that provide degrees and classes in cybersecurity. Through these programs, students learn about cyber risks, how to effectively protect themselves, and the skills they need to keep systems and data safe. [18]

b. Certifications: Professional certifications like Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager

ISSN (Online):3048-5088
International Journal of Advancement and Innovation in Technology and Research (IJAITR)
Volume 2, Issue 2, (Jul-Dec) 2025

(CISM) give experts a clear path to becoming skilled in cybersecurity. [19]
c. Training Employees: Companies need to regularly teach their employees about the best ways to protect themselves online. (Workshops, lectures, and practice cyberattacks are all examples of things that could happen.)
d. Awareness Campaigns: There should be campaigns inside the company to teach employees about the latest cyber risks, social engineering techniques, and security rules.

B. Public Awareness Campaign:

To protect society at large, public awareness campaigns are needed to protect society at large. Ultimately, these campaigns should reach out to citizens of all ages, raising awareness of common cyber threats and best practices to avoid them. Government Initiatives: Government organisations can warn the public about cybersecurity threats by starting national awareness campaigns. Community gatherings, social media outreach, and ads are a few examples of these campaigns.
School Programs: Schools may teach kids and teenagers how to stay safe online by incorporating cybersecurity education into the curriculum[20].
Online Resources: By offering websites, hotlines, and online tools, users can learn how to stay safe online and report cyber occurrences.Research and Development:

VII. Collaboration:

To keep ahead of changing threats, it is imperative to invest in cybersecurity research and development. This level covers both the development of new tactics to counteract cyber intrusions and technology breakthroughs.

A. Innovation Centres:

Establishing cybersecurity-focused research and innovation centres. These centres collaborate with academia, industry, and government to develop solutions.

B. Threat Intelligence Sharing:

Investing in research that focuses on stemming threats, vulnerabilities, and attack patterns. The findings can be shared with relevant stakeholders to enhance defenses..

C. Incident Response Research:

Research on the infected is also about improving incident response, which assists organizations in effectively dealing with and recovering from cyber-attacks.

VIII. Conclusion

With the world growing more connected, especially in the U.S. and India, cybersecurity has become even more crucial in order to protect ourselves and our organizations. Recent cyberattacks highlight the growing threats faced by individuals, businesses, and governments, which are rising alongside technological progress. Since breaches can have a lasting impact, keeping data safe is critical too. What's needed to counter these is government programs, public awareness campaigns, and international cooperation. Investment in cybersecurity research and legislation is what helps keep us ahead of the competitors. Hence, to create a safe digital future, we need a coordinated, pro- active approach.

References

[1] Catal, C., Ozcan, A., Donmez, E. et al. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ Inf Technol 28, 1809–1831. https://doi.org/10.1007/s10639-022-11261-8 (2023).
[2] Vahid Garousi, Gorkem Giray, and Eray Tuzun. 2019. Understanding the Knowledge Gaps of Software Engineers: An Empirical Analysis Based on SWEBOK. ACM Trans. Comput. Educ. 20, 1, Article 3, 33 pages. https://doi.org/10.1145/3360497 (2020).
[3] Rackspace: Ransomware Attack Bypassed ProxyNotShell Mitigations, Kelly Jackson Higgins Weblink: https://www.darkreading.com/cloud-security/rackspace-ransomware-attack-microsoft-exchange-server-zero-day-exploit (2023)
[4] Natalie Silva: Update on Recent Cybersecurity Incident – Rackspace Technology (2022)
[5] Cisco Suffers Cyber Attack By UNC2447, Lapsus$, & Yanluowang, Jason Firch News Writer Weblink: https://purplesec.us/breach-report/cisco-cyber-attack/ (2024)

ISSN (Online):3048-5088

International Journal of Advancement and Innovation in Technology and Research (IJAITR)

Volume 2, Issue 2, (Jul-Dec) 2025

[6] Sharma, Ujjwal & Kalekar, Samruddhi.: Dissecting the Uber Security Breach: Root Cause Analysis and Mitigation Strategies. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY. 15. 715-720. 10.5281/zenodo.13368425 (2024).

[7] Uber Investigating Breach of Its Computer Systems, Kate Conger and Kevin Roose Weblink: https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html (2022)

[8] Sensitive NATO Data Leaked After Cyber Attack on Portugal's Armed Forces, Jason Firch News Writer Weblink: https://purplesec.us/breach-report/nato-data-leaked/ (2024)

[9] NATO investigating breach, leak of internal documents, AJ Vicens News Writer Weblink: https://cyberscoop.com/nato-siegedsec-breac/ (2023)

[10] HC3: Analyst Note January 30, 2023 TLP: CLEAR Report: 202301301200 (2023).

[11] Understanding the Massive ICMR Data Breach Incident Report, Alles Technology Weblink: https://www.linkedin.com/pulse/understanding-massive-icmr-data-breach-alles-technology-d6cdf (2023)

[12] List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached, IT Governance Weblink: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023 (2024)

[13] Mr. Ujjawal Upadhyay.: Analyzing Information Support Force (ISF) of China and Its Impact on India. CENJOWS, New Delhi Issue Brief IB/13/24 (2024).

[14] https://www.hindustantimes.com/technology/16-lakh-ddos-attacks-per-minute-on-g20-website-during-summit-govt-101704293255773.html (2024)

[15] Guru Baran.: RailYatri Data breach – Over 31 Million Users Data Exposed https://cybersecuritynews.com/railyatri-data-breach/ (2023)

[16] All India Institute of Medical Sciences (AIIMS), Delhi: Cyberattack Puts Digitalization Under Scanner IMIB Journal of Innovation and Management 2(2) 299–306 (2024).

[17] Delhi AIIMS ransomware attack carried out by hackers from China, Hong Kong: Report, Harshit Sabarwal Weblink: https://www.wionews.com/india-news/attack-on-aiims-delhi-server-carried-out-by-chinese-hackers-report-543044 (2022)

[18] Research and analysis Cyber security skills in the UK labour market 2020 https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020

[19] Closing the cybersecurity skills gap, Rebecca Vogel https://search.informit.org/doi/abs/10.3316/informit.093144667545339 (2016)

[20] Alrabaee, S. & Manna, R.: Boosting Students and Teachers Cybersecurity Awareness During COVID-19 Pandemic. In: 2021 IEEE Global Engineering Education Conference (EDUCON). pp. 726-731.Academic Programs (2021).