INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 16 | ISSUE - 3 | APRIL – 2026

A STUDY OF CYBER SECURITY SYSTEM IN INDIA IN PRESENT SENARIO

Dr. Maneesha Sharma
Assistant Profesor, Supervisor, Law Department, Monad University, Hapur, U.P.

Shefali Kaushik
Research Scholar, Law Department, Monad University, Hapur, U.P.

ABSTRACT:

Cybersecurity is the activity of defending systems, networks, and programs from digital threats. These intrusions are frequently intended to access, modify, or delete sensitive information; extract money from users via ransomware; or disrupt normal corporate activities. The term "cyberspace" referred to the vast expanse of the internet. Cybersecurity is also a set of laws put in place to protect the cyber realm, which refers to the internet. Cybercrime refers to a set of organised crimes that target both cyberspace and cybersecurity. This paper attempts to present an overview of cybersecurity. It defined cybersecurity, improved cybersecurity in Nigeria, and reduced and eradicated cybercrime. This study used primary sources such as cases and statues, as well as secondary sources such as textbooks, journals, and articles. The study concluded that cyber security is a serious issue in Nigeria, and there has been no improvement in the laws governing cybercrime, which is still prevalent in the country and around the world. A search is a quest for evidence to support an argument. Thus, the critical literature evaluation establishes a foundation for study while also filling research gaps with new perceptions and awareness of a compelling case. Cybersecurity safeguards internet-connected systems, networks, and data from digital threats by providing confidentiality, integrity, and availability (the CIA trinity). As people rely more on technology, they confront new hazards such as malware, hacking, and unauthorised access. Technical measures, policy, and user knowledge are all essential components of effective defence..

KEYWORDS: *Cybercrime, Cybersecurity, Cyberspace, Digital, Technology.*

INTRODUCTION:

Cybersecurity is the process of protecting systems, networks, and data against digital threats while also encouraging responsible and sustainable technology use. In today's linked world, cybersecurity not only secures information, but also helps environmentally friendly digital growth by minimising wasteful practices and system misuse.

Cybersecurity is the activity of defending systems, networks, and programs against digital threats. These intrusions are typically intended to access, change, or delete sensitive information; extract money from users via ransomware; or disrupt normal corporate activities.

Implementing effective cybersecurity safeguards is especially difficult today, as there are more devices than humans, and attackers are becoming more creative.

A good cybersecurity posture has numerous layers of protection dispersed throughout the computers, networks, applications, or data that one wishes to safeguard. A unified threat management gateway system within an enterprise can automate cross-product integrations and accelerate important security operations processes such as detection, investigation, and remediation. To build an effective cyber defense, people, processes, and technology must all work together.

Types of Cyber Security:

Effective cybersecurity involves multiple layers of protection throughout an organization's IT infrastructure. Key types include:

- AI security
- Critical infrastructure security
- Network security
- Endpoint security
- Application security
- Cloud security
- Information security
- Identity security

AI Security:

AI security refers to cybersecurity methods that safeguard AI applications and systems against cyberthreats, cyberattacks, and malicious activity. Hackers may use prompt injection, data poisoning, or other malicious approaches to fool AI tools into disclosing sensitive information. They also employ AI to quickly generate malicious code and phishing scam content.

Critical infrastructure security :

Critical infrastructure security safeguards the computer systems, apps, networks, data, and digital assets that a society relies on to ensure national security, economic health, and public safety. In the United States, the National Institute of Standards and Technology (NIST) provides a cybersecurity framework to assist IT providers and stakeholders in safeguarding critical infrastructure.5 The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) also offers guidelines.

Network Security :

Network security is to prevent unauthorised access to computer networks and systems. It has three primary goals: to prevent unauthorised access, to identify and interrupt ongoing cyberattacks and security breaches, and to ensure that authorised users have secure access to their network resources.

Endpoint security :

Endpoint security defends users and endpoint devices (desktops, laptops, mobile devices, cellphones, servers, and others) from cyberattacks. Organisations are also implementing unified endpoint management (UEM) solutions, which enable them to protect, configure, and manage all endpoint devices from a single console.

Application Security:

Application security (AppSec) is the process of identifying and repairing vulnerabilities in software to prevent unauthorised access, modification, or misuse. Modern application development methodologies (such as DevOps and DevSecOps) incorporate security and testing into the development process.

Cloud Security:

Cloud security protects an organization's cloud-based infrastructure, such as apps, data, and virtual servers. In general, cloud security follows a shared responsibility paradigm. The cloud provider is responsible for the security of the services they supply as well as the infrastructure that supports them. The customer is responsible for safeguarding the data, code, and other assets they store or run in the cloud.

Information Security :

Information security (InfoSec) safeguards an organization's critical information (digital files and data, paper documents, and physical media) from unauthorised access, use, or alteration. Most cybersecurity-related InfoSec measures focus on data security, which is the safeguarding of digital information.

Identity security:

The goal of identity security is to protect digital identities as well as the systems that handle them. It comprises procedures like identity verification, access control enforcement, and unauthorised access prevention. According to the IBM X-Force 2025 Threat Intelligence Index, identity-based assaults account for 30% of all intrusions, making them the most common access point into corporate networks.[2]

History of Cyber Security:

William Gibson created the phrase "cybersecurity" in 1983 with his novel Neuromancer. Three years later (1986), the United States passed "The Computer Fraud and Abuse Act." Digital criminal behaviour was new and unregulated, necessitating methods to mitigate these risks. Justice.gov explains, "As technology and criminal behaviour continue to evolve, however, it also remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law"[3]

Cybersecurity is becoming increasingly important as people rely more on computer systems, the Internet, and wireless network technologies like Bluetooth and Wi-Fi, as well as the proliferation of smart devices and other devices that make up the 'Internet of Things'.

Because of its complexity, both in terms of politics and technology, cybersecurity is one of the most pressing issues in today's globe. Where did it all start? We look at the history of cybersecurity, from its beginnings to the present.

1970s: ARAPNET and the Creeper.

Cybersecurity originated in the 1970s, when researcher Bob Thomas wrote Creeper, a computer software that could walk across ARPANET's network while leaving a breadcrumb trail.

The 1980s saw the birth of commercial antivirus

Commercial antivirus was born in 1987, despite contradictory claims about who invented the first antivirus product. Andreas Lüning and Kai Figge developed their first antivirus solution for the Atari ST, along with Ultimate Virus Killer, in 1987.

1990s: The world gets online

As the internet became more widely available, more people began to share their personal information online. Organised crime outfits viewed this as a possible source of revenue and began stealing data from individuals and governments via the internet. By the mid-1990s, network security threats had grown tremendously, necessitating the mass production of firewalls and antivirus programs to protect the public.

In the early 2000

criminal groups began funding professional cyberattacks, while governments tightened laws against hacking, resulting in harsher penalties for individuals responsible.

2021: The Next Generation

The cybersecurity sector is rapidly expanding. Statista forecasts that the worldwide cybersecurity market will reach $345.4 billion by 2026. Ransomware is one of the most common dangers to an organization's data security, and it is expected to grow.[4]

Legal Provisions Related to Cyber Security:

The Information Technology Act of 2000 :establishes India's cybersecurity architecture. It addresses hacking, identity theft, and cyber terrorism and imposes penalties for violations. Cyber security is enforced by specific parts, such as Section 66 (hacking) and Section 67C (intermediary retention of sensitive data).

Digital Personal Data Protection Act, 2023.

The purpose of this Act is to protect persons' personal data by regulating how it is processed. The key provisions include:

Consent Mechanism: Before processing personal data under Section 4, organisations must obtain explicit consent.

Section 5 mandates that information be gathered only for defined, legitimate purposes.

Data Localisation: Section 17 requires some sensitive personal data to be maintained in India.[5]

B.N.S. 2023:

This cybercrime prevention act is primarily concerned with cyber frauds involving identity theft and other sensitive information theft.

Companies Act (2013):

When the Companies Act was passed in 2013, the legislature ensured that all regulatory compliances were addressed, including e-discovery, cyber forensics, and cybersecurity diligence. The Companies Act establishes standards for the responsibilities of corporate directors and leaders in confirming cybersecurity commitments.

Information Technology (Amendment) Act, 2008:

It targets cybercrime and electronic commerce by establishing a legal framework for data security, digital signatures, and cyber activities.

The Information Technology Rules, 2011, were enacted to supplement the IT Act by providing precise instructions on many aspects of cyber law.

The National Cyber Security Policy (2013) presents a strategy framework for protecting the country's cyber environment. The key objectives include creating a secure and resilient cyberspace for individuals, enterprises, and the government.

The IT Rules, 2021

Enhance laws governing digital media and social networking sites. They require due diligence on intermediaries, including grievance redressal systems and the hiring of compliance officers. The regulation of digital content and OTT (Over-The-Top) platforms to ensure compliance with content standards.

The Digital Personal Data Protection Act (2023):

The DPDP Act 2023 is a comprehensive law that aims to protect personal data in the digital environment.

Case Study Related to Cyber Crime:

In Sharat Babu Digumarti v. Govt. of NCT of Delhi (2017) SCC 18

In this case it was determined that Chapter XI of the IT Act, including Sections 67-67B, serve as a comprehensive code for offences related to electronic obscene and pornographic material. Sections 67, 67A, and 67B of the IT Act should be interpreted in a way that suppresses mischief and promotes remedies. This ensures that the legislative intent of penalising cyber-offences against children and the use of obscene/pornographic material through electronic means is not undermined by a narrow interpretation of these provisions.[6]

Just Rights For Children Alliance v. S. Harish (2024 SCC OnLine SC 2611)

The Supreme Court reversed the verdict of the High Court and reinstated criminal proceedings against the respondent. The Court ruled that the High Court erred in quashing the criminal proceedings without reviewing the chargesheet and other evidence. As a result, the judgement and order were set aside. The Court clarified the ambit of the POCSO Act and IT Act, including the possession, consumption, and transmission of CSEAM.[7]

Justice K.S. Puttaswamy vs. Union of India (2017) - The Privacy Judgment

Citation: (2017) 10 SCC 1

Raju Kumar Paswan vs. State of Bihar (2025): In a unanimous and historic ruling, the nine-judge bench concluded that the Right to Privacy is a basic right guaranteed by Articles 14, 19, and 21 of the Constitution. The Court clearly rejected previous decisions in M.P. Sharma and Kharak Singh, which held otherwise.8

A.Shankar @ Savukku Shankar vs. State Of Tamil Nadu (2025):

A recent Supreme Court case involves allegations handled by a cybercrime police station.[9]

Ananya Kumar vs Union Of India (2024):

A public interest litigation (PIL) filed before the Delhi High Court to address the police's ineptitude in invoking IT Act provisions in cybercrime cases rather than only IPC.[10]

Faizan Ansari vs. Union of India (2024):

Jharkhand High Court case about the formation of ISIS-aligned cyber groups, with an emphasis on "stealthy cyber security measures" such as the usage of VPNs.

Patna High Court case concerning the hacking of an informant's identity and the transmission of obscene videos.[11]

True cybersecurity is based on ground-level knowledge rather than top-down control. In this essay, Roel Gloudemans, Director IT Risk & Compliance at Conclusion, discusses how a culture of responsibility makes organisations more robust to new challenges.

Cyber security awareness transforms compliance from a reactive exercise into a proactive culture. When everyone—from leadership to interns—understands their role in protecting data and systems, security becomes second nature. By aligning with ISO 27001 and NIS2, you build not just compliance, but trust.

REFERANCES:

1) https://www.geeksforgeeks.org/cybersecurity
2) https://www.ibm.com/think/topics/cybersecurity
3) https://www.tracesecurity.com/blog/articles/a-brief-history-of-cybersecurity
4) https://cybermagazine.com/cyber-security/history-cybersecurity
5) https://thelegalschool.in/blog/cybersecurity-and-data-privacy
6) In Sharat Babu Digumarti v. Govt. of NCT of Delhi (2017) SCC 18
7) Just Rights For Children Alliance v. S. Harish (2024 SCC OnLine SC 2611)

8) Justice K.S. Puttaswamy vs. Union of India (2017) - The Privacy Judgment Citation: (2017) 10 SCC
9) A.Shankar @ Savukku Shankar vs. State Of Tamil Nadu (2025)
10) Ananya Kumar vs Union Of India (2024)
11) Faizan Ansari vs. Union of India (2024)