Library Progress International
Vol.45, No.2, Jul-Dec 2025: P. 656-671

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

A Critical Study on Enhancing Cybersecurity in India's Healthcare Sector

[1]Mrs V B Malleswari, [2]Dr Anjali Dixit, [3]Dr Mithlesh Malviya

[1]Research Scholar Institution: School of Legal Studies and Governance, Career Point University, Kota, Rajasthan
Email Id: vbmalleswari@yahoo.com
[2]Associate Professor Institution: School of Legal Studies and Governance, Career Point University, Kota, Rajasthan
Email Id: anjalidixitlexamicus@gmail.com
[3]Assistant Professor Institution: School of Legal Studies and Governance, Career Point University, Kota, Rajasthan
Email Id: Mithlesh.malviya@cpur.edu.in

How to cite this article: Mrs V B Malleswari, Dr Anjali Dixit, Dr Mithlesh Malviya (2025). A Critical Study on Enhancing Cybersecurity in India's Healthcare Sector. Library Progress International, 45(2), 656-671

Abstract

The healthcare industry in India comprises both private and public institutions that offer essential services across urban and rural areas. This sector includes hospitals, pharmaceuticals, diagnostics, medical devices, medical insurance, medical tourism and telemedicine. Technological advances such as Artificial Intelligence (AI) have enhanced operations and services in this industry. AI is applied in hospitals for patient management and personalized treatment plans, in the pharmaceutical sector for drug discovery and in diagnostics for accurate medical image analysis. It also supports the development of smart medical devices, aids health insurance providers in risk assessment, improves patient recruitment in clinical trials, enables virtual consultations in telemedicine and streamlines medical tourism experiences. Nevertheless, these advancements have increased the risk of cyberattacks. In 2022, nearly 1.9 million cyberattacks on healthcare facilities exposed serious cybersecurity weaknesses. These attacks often involve ransomware, denial-of-service attacks, phishing, data breaches, malware and insider threats which disrupt operations and steal sensitive data.

To protect data, India has enacted laws and regulations such as the IT Act 2000, the NCSP 2013, The IT Rules 2021 and the DPDP Act 2023. Despite these laws and policies, the healthcare sector remains vulnerable, signifying that these are inadequate. This study therefore highlights need for improved cybersecurity in India's healthcare sector, recommending stricter law enforcement, investment in better security technology, efficient staff training to protect patient data, conducting regular security assessments and using advanced encryption techniques.

Keywords: Cyber Security, Healthcare Sector, Data Protection, Artificial Intelligence.

Introduction

India's healthcare sector, which includes hospitals, pharmaceuticals, diagnostics, medical devices, medical insurance, medical tourism and tele medicine, has seen notable improvements with the adoption of technologies like the Artificial Intelligence (AI) and Machine Learning (ML). AI being capable of mimicking human intelligence, offers great potential in healthcare (RajKomar et al, 2019)[1]. Whereas, ML helps analyze large data sets, reveal complex patterns and provide real-time insights. This improves clinical decisions, treatment strategies and resource management enhancing patient outcomes and overall healthcare efficiency (Esteva et al, 2017)[2]. AI helps in patient management and personalized treatment plans in hospitals, aids in drug discovery in the pharmaceutical sector and enhances accuracy in diagnostics (Obermeyer et al., 2016) [3].

1 Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347-1358.
2 Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with the deep neural networks. Nature, 542(7639), 115-118.
3 Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the future – Big data, machine learning, and clinical medicine. New England Journal of Medicine, 375(13), 1216-1219. doi: 10.1056/NEJMp1606181

In hospitals, AI is used for patient management and the creation of personalized treatment plans. For instance, Apollo Hospitals Group in India, introduced an automated patient monitoring system that quickly alerts experts to any signs of patient health deterioration. This system enhances timely intervention, improving patient management and outcomes (Apollo Hospitals, 2022)[4]. In the pharmaceutical sector, AI plays an important role in drug discovery. Corporations like Tata Consultancy Services (TCS) utilize AI to scrutinize through vast amounts of data for identifying potential new drugs ((Blackman J, 2024)[5]. This approach significantly reduces the time and cost associated with bringing new medications to the market, making the drug development process more efficient. Similarly, diagnostics field too has gained from AI advancements. For instance, diagnostic centers such as Dr. Lal PathLabs and Ibex Medical Analytics have introduced India's first AI platform 'Galen', which supports pathologists in cancer diagnosis and enhances the quality and speed of cancer tests (Healthcare MEA, 2021)[6]. Telemedicine platforms including Practo and mFine, depend on AI to offer remote consultations and health advice. This technology makes healthcare more accessible to individuals in remote areas, bridging the gap between patients and healthcare providers (Saha N, 2024) [7]. These advancements have not only improved efficiency within the healthcare system but has also enhanced the quality in providing care and access to patients across India (Junaid SB et al 2022)[8].

Nonetheless, after the integration of technology into healthcare, few started using these computer applications for harmful purposes, either for personal gain or to help others. This misuse led to the rise of "Cyber Crime," which refers to illegal acts by using computers (Priya et al, 2020) [9]. Subsequently the Indian health sector is facing cyber threats and attacks. By 2017, India began seeing a rise in data breaches, which increased by 7.9% by 2022. During 2022, the healthcare sector faced around 1.9 million cyberattacks, with India experiencing about 6,935 attacks per week which is much higher than the global average. The cost of data breach on an average in India reached INR 4,552 ($64), making India the fourth most targeted country globally (Showkat, Ahmad et al, 2022)[10]. These incidents highlight the critical importance of enhancing cybersecurity in the healthcare sector to safeguard sensitive data and ensure the resilience of healthcare systems. This paper critically examines these cyber crimes within the Indian healthcare sector, focusing on recent cyberattack trends, existing cybersecurity measures and the impact of legal frameworks, while acknowledging the limitations imposed by the evolving nature of cyber threats.

1.1 Significance of the Study

Healthcare facilities across urban and rural areas keep huge amounts of confidential patient data, that includes patient identification information, medical histories and financial details (Gliklich, R et al, 2019)[11]. However, India's healthcare sector encompassing both public and private institutions is increasingly vulnerable to cybersecurity threats[12]. This critical data requires robust protection to prevent breaches and misuse, ensuring patient privacy and compliance with legal

[4] Apollo Hospitals. (2022, October 11). Apollo Hospitals has launched an automated AI based real-time rapid-response patient monitoring system, Enhanced Connected Care. Apollo in the news.
[5] James Blackman, Four in five using AI, says TCS – as it brings gen AI and IoT support for enterprises, RCR Wireless News, July 16, 2024, https://www.rcrwireless.com/20240716/ai-ml/industrial-ai/four-in-five-using-ai-says-tcs-as-it-brings-gen-ai-and-iot-support-for-enterprises.
[6] Healthcare MEA. (2021, November 26). Dr. Lal PathLabs, Ibex partner to deploy AI-powered cancer diagnostics in India. https://www.healthcaremea.com/dr-lal-pathlabs-ibex-partner-to-deploy-ai-powered-cancer-diagnostics-in-india/
[7] Saha N. (2024, June 24). Innovative telemedicine startups of India promising connected healthcare. Digital Health News. https://www.digitalhealthnews.com/innovative-telemedicine-startups-of-india-promising-connected-healthcare
[8] Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., Abdulkarim, M., Shuaibu, A. N., Garba, A., Sahalu, Y., Mohammed, A., Mohammed, T. Y., Abdulkadir, B. A., Abba, A. A., Kakumi, N. A. I., & Mahamad, S. (2022, October 3). Recent advancements in emerging technologies for healthcare management systems: A survey. Healthcare (Basel), 10(10), 1940. https://doi.org/10.3390/healthcare10101940. PMID: 36292387; PMCID: PMC9601636.
[9] Priya Rao, Abhay Kumar Tiwari. Laws Related to Cyber-crime in India. Research J. Engineering and Tech. 2020;11(2):41-44. doi: 10.5958/2321-581X.2020.00007.0
[10] Showkat, Ahmad & Dar, Showkat & Naseer, Ahmad & Lone, Naseer. (2022). CYBER CRIME IN INDIA. Sambodhi (UGC Care Journal) Vol-43 No.-04 https://www.researchgate.net/publication/357839318_CYBER_CRIME_IN_INDIA

11 Gliklich RE, Leavy MB, Dreyer NA, editors. Registries for Evaluating Patient Outcomes: A User's Guide [Internet]. 4th edition. Rockville (MD): Agency for Healthcare Research and Quality (US); 2020 Sep. Available from: https://www.ncbi.nlm.nih.gov/books/NBK562575/

12 Chandwani, R., Edacherian, S., & Sud, M. (2023). National Digital Infrastructure and India's Healthcare Sector: Physician's Perspectives. The Qualitative Report, 28(2), 360-386. https://doi.org/10.46743/2160-3715/2023.4964

standards (Tariq RA, Hackert PB, 2024)[13]. As the healthcare industry becomes more digitalized, it becomes crucial to realize the dangers of cyber threats and to analyse current security measures (Abernethy, 2022)[14]. The surge in cybercrime in the recent times has adversely impacted the digital economy, emphasizing the necessity for effective cybersecurity framework to safeguard sensitive data and reliability of AI-driven systems[15] (Gandhi & Tandon 2021). The objective of this study is to provide a complete analysis of current cybersecurity within India's healthcare sector, evaluate the adequacy of existing legal and regulatory frameworks and provide recommendations for efficient cybersecurity. By addressing these issues, the study contributes to the broader goal of safeguarding sensitive patient data, ensuring uninterrupted healthcare services in a secured digital environment.

1.2 Objectives

The aim of this paper is:

1. To examine the existing cybersecurity measures, practices and challenges within India's healthcare sector.
2. To evaluate the impact of cyberattacks, particularly ransomware, on healthcare services and patient data.
3. To assess the efficiency of present laws and regulations related to cybersecurity in the Indian healthcare industry.
4. To propose recommendations for improving cybersecurity measures, including technological advancements, regulatory updates and training programs.

1.3 Research Methods

The researcher employed a doctrinal approach to analyze the research paper, utilizing various statutes, texts, legal journals and magazines to gather all relevant material on the topic. Through this method, the researcher aimed to identify the problems and draw final conclusions using logical reasoning. This research paper adopts a socio-legal research approach to explore the problems meted out by the Indian healthcare industry because of the rising rate of cyber attacks

1. Overview of Cybersecurity Threats in Healthcare

Cybersecurity is the practice of safeguarding the computer systems, its network and data from cyberattacks, theft and damage. Further, it requires implementing measures to prevent unauthorized access, ensure the protection of data and secure the confidential information. This includes using technologies, policies and procedures to defend against various threats such as malware, phishing and hacking. Cybersecurity aims to secure digital assets and maintain the safe and reliable operation[16]. Digital illiteracy is a major reason for increasing cybercrimes in India (Srivastava S, 2020)[17]. With the affordability and accessibility of technology, majority of people including children, now use the internet and often visit risky sites without realizing the dangers. Google found that 50% of mobile ad clicks are mistakes and 72% of those lead to harmful sites.[18] Phishing attacks have increased by 350% since the pandemic, with criminals using fake websites, emails and phone calls to steal information (Yadav A, 2021)[19]. Check Point Software Technologies Ltd. a leading provider of cybersecurity solutions globally, revealed in its latest Threat Intelligence Report that India's healthcare sector faced approximately 6,935 cyberattacks per week in six months, significantly

[13] Tariq RA, Hackert PB. Patient Confidentiality. [Updated 2023 Jan 23]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2024 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK519540/

[14] Abernethy, A., Adams, L., Barrett, M.A., Bechtel, C., Brennan, P.A., Butte, A., Faulkner, J., Fontaine, E., Friedhoff, S., Halamka, J.D., Howell, M., Johnson, K., Long, P., McGraw, D., Miller, R., Lee, P., Perlin, J.A., Rucker, D., Sandy, L., Savage, L.C., Stump, L., Tang, P., Topol, E., Tuckson, R.V., & Valdes, K. (2022). The Promise of Digital Health: Then, Now, and the Future. *NAM perspectives, 2022*.

[15] Gandhi, P., & Tandon, N. (2021). To assess the impact of CRM implementation in health industry. *Vidyabharati International Interdisciplinary Research Journal*, (Special Issue 10), 126–129. http://www.viirj.org/specialissues/SP10/Part%201.pdf

[16] Hlatshwayo, Mthokozisi. (2023). 'Cybersecurity in the Digital Space'. Available at https://www.researchgate.net/publication/375115830_CYBERSECURITY_IN_THE_DIGITAL_SPACE/citation/download.

[17] Srivastava, S. (2020, September 8). International Literacy Day: Bridging India's Digital Divide. BloombergQuint. https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-

digitalivide#:%7E:text=As%20per%20a%20report%20from,India's%20population%20is%20digitally%20illiterate.
&text=The%20coverage%20targe ts%20have%20been,in%20rural%20India%20digitally%20literate.
18 Kim, R. (n.d.). Report: 40 percent of mobile ad clicks are fraud or accidents. Retrieved from http://www.raisingthevolume.com/wp-content/uploads/2012/01/Mobile.pdf
19 Yadav, A. (2021). Phishing in India – Analytical study. International Advanced Research Journal in Science, Engineering and Technology, 8(8), 674-679. https://doi.org/10.17148/IARJSET.2021.88110

higher than the world average of 1,821 attacks per organization (India Technology News, 2024) [20]. This surge is attributed to the increased adoption of electronic health records (EHRs), telemedicine and IoT devices. These incidents highlight the growing vulnerability of healthcare facilities to cyber threats and need for stringent cybersecurity framework within the sector.

1.1 Incidents of Cyber Attacks in India

The healthcare sector is increasingly targeted by cybercriminals, with 60% of organizations globally experiencing attacks in 2022. Notable Indian institutions like AIIMS and ICMR have been affected, with a rise in data encryption during ransomware attacks.

- In November 2022, the All India Institute of Medical Sciences (AIIMS) in New Delhi experienced a significant cyberattack, disrupting its digital services and compromising patient data. The ransomware attack targeted the hospital's servers, affecting various departments and critical operations. Despite efforts to restore systems and secure data, the breach highlighted vulnerabilities in the cybersecurity infrastructure of one of India's premier healthcare institutions. Authorities have since been investigating the attack, emphasizing the need for efficient cybersecurity in the healthcare industry (IndiaTimes, 2nd December 2022)[21].
- On 13th May 2023, KD Hospital in Ahmedabad experienced a ransomware, which had encrypted its online systems, including CCTV footage and patient data. The attackers demanded $70,000 in bitcoins for decryption. Despite the attack, the hospital managed to maintain its services manually and restored its systems using a backup server (Express News Service. 17th May 2023)[22].
- In October 2023, the personal details of over 81.5 crore Indian citizens, including Aadhaar and passport information, were found being auctioned in the dark web[23] following a data breach at the Indian Council of Medical Research (ICMR) (Economic Times., 2023)[24]. The breach, discovered by the US-based firm Resecurity, was attributed to a hacker named 'pwn0001' who claimed the data was collected during Covid-19 testing. The source of the leak remains unknown, but the dataset was offered for sale at $80,000 (TechCircle, 31st October 2023). [25].
- In April 2024, The Regional Cancer Centre (RCC) in Thiruvananthapuram faced a ransomware attack, disrupting operations for five days and crippling several departments, including radiation. The hospital received a ransom demand of $100 million, but patient data remained secure due to robust data backup (The Hindu, 8th July 2024). Similarly, a hospital in Mumbai was struck by ransomware, resulting in the loss of access to critical patient history and billing data, which disrupted its operations[26].

3. Kinds of Cyber Attacks in Health Care Industry in India

3.1 Ransomware Attacks

Ransomware is a type of malware that takes control of a victim's sensitive data or device, threatening to keep it locked or even cause damage unless the victim pays a ransom to the attacker (The Hindu, 2024)[27]. This type of attack can

[20] Pariti, G. (2024, June 28). India's healthcare sector battling 6,953 weekly cyberattacks: Report. India Technology News. https://indiatechnologynews.in/indian-healthcare-sector-faces-6953-cyberattacks-weekly-outpacing-global-rates-check-point-threat-intelligence-report/

[21] Sharma, B. (2022, December 2). Explained: What's happening at AIIMS after sensitive ransomware attack? IndiaTimes. https://www.indiatimes.com/explainers/technology/explainer-aiims-ransomware-attack-586542.html

[22] Express News Service. (2023, May 17). Hospital falls prey to ransomware attack, hackers demand $70,000. The Indian Express. https://indianexpress.com/article/cities/ahmedabad/hospital-falls-prey-to-ransomware-attack-hackers-demand-70000-8613410/

[23] Kaur, Shubhdeep & Randhawa, Sukhchandan. (2020). Dark Web: A Web of Crimes. Wireless Personal Communications. 112. 10.1007/s11277-020-07143-2.

[24] Lohchab, H. (2023, November 3). Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: Report. Economic Times. Retrieved from https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr

[25] Bagchi, S. (2023, October 31). '*ICMR data leak reveals personal information of 81.5 cr Indians*' Report. TechCircle.

severely disrupt healthcare services by making critical data inaccessible, leading to compromised patient information and halted operations (Maji and Asibi, 2019)[28].

3.1.1 Types of Ransomwares

Scareware: Displays fake malware warnings and demands payment to remove the threat (Luo, X., & Liao, Q, 2017)[29].

Screen Lockers: Blocks access to the screen with fake alerts, preventing computer use (Narain, P, 2018)[30].

Encrypting Ransomware: Scrambles files and demands payment for decryption (kalaimannan et al 2017)[31].

Mobile Ransomware: Targets phones with harmful apps or downloads, requiring payment to unlock(Song et al , 2016) [32].

Fileless Ransomware: Operates without installing files, making detection more challenging (Pathak, P. B, 2016)[33].

Double Extortion: Encrypts files and threatens to leak stolen data if the ransom is not paid.

Doxware: Threatens to release personal or sensitive information if the ransom is not paid.

Ransomware-as-a-Service (RaaS): Ransomware tools sold or rented to other criminals, enabling them to launch attacks (Tom Meurs et al 2024)[34].

3.2 Phishing

Phishing attacks involve deceiving healthcare employees into providing sensitive information or clicking on malicious links, leading to malware infections. These infections can steal data, disrupt operations and compromise patient confidentiality (Priestman et al 2019)[35]. In 2020, several Indian hospitals experienced phishing attacks where attackers posed as government officials to deceive employees into disclosing confidential information. (Nadeem, 2023) [36]. This highlights the ongoing vulnerability of healthcare staff to such deceptive tactics.

3.3 Insider Threats

Insider threats arise when people having access to confidential data misuse their access, either intentionally or unintentionally, resulting in data breaches. For instance, in 2020, an insider at a major Indian hospital was found to have accessed and sold patient records to unauthorized parties (Saxena et al, 2020)[37]. This incident highlights the dangers associated with individuals who have authorized access to sensitive information and emphasizes the necessity for strict internal regulations.

---

[28] maji, Asibi. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods.

[29] Luo, X., & Liao, Q. (2017). Awareness Education as the Key to Ransomware Prevention. Information Systems Security, 16(4), 195-202. doi:10.1080/10658980701576412

[30] Narain, P. (2018). Ransomware - Rising Menace to an Unsuspecting Cyber Audience. The University of Houston, http://hdl.handle.net/10657/3145

[31] kalaimannan, E., John, S. K., DuBose, T., & Pinto, A. (2017). Influences on ransomware's evolution and predictions for future challenges. Journal of Cyber Security Technology, 1(1), 23-31. doi:10.1080/23742917.2016.1252191

[32] Song, S., Kim, B., & Lee, S. (2016). '*The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform',* Mobile Information Systems, 1-9. doi:10.1155/2016/2946735

[33] Pathak, P. B. (2016). Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. *International Journal of Advanced Research in Computer Science*, 7(2), 1-4

[34] Tom Meurs, Edward Cartwright, Anna Cartwright, Marianne Junger, Abhishta Abhishta, Deception in double extortion ransomware attacks: An analysis of profitability and credibility, Computers & Security, Volume 138, 2024, 103670, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103670.

[35]Priestman, Ward & Anstis, Tony & Sebire, Isabel & Sridharan, Shankar & Sebire, Neil. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ health & care informatics. 26. 10.1136/bmjhci-2019-100031.

[36]Nadeem, Muhammad & Zahra, Syeda & Abbasi, Muhammad & Arshad, Ali & Riaz, Saman & Ahmed, Waqas. (2023). Phishing Attack, Its Detections and Prevention Techniques. *International Journal of Wireless Information Networks*. 12. 13-25. 10.37591/IJWSN.

[37]Saxena, Neetesh & Hayes, Emma & Bertino, Elisa & Ojo, Patrick & Choo, Kim-Kwang Raymond & Burnap, Pete. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics. 9. 1460. 10.3390/electronics9091460.

3.4 Breach of Data

Data breaches take place when unlawfully people gain access to healthcare systems, leading to the theft of patient records, financial information and other confidential data[38]. A significant data breach in 2015 at Anthem Inc. exposed confidential information of 78.8 million individuals, illustrating that severe impact can be caused on patient privacy and trust [39]. In India, the ICMR breach in October 2023, which exposed the personal details of over 81.5 crore citizens, is a recent example of the profound impact of such data breaches.

3.5 Distributed Denial of Service (DDoS) Attacks[40]

DDoS attacks involve overwhelming healthcare networks with excessive traffic, disrupting services and rendering systems unavailable to legitimate users. This type of attack can halt critical operations and block access to essential services[41]. For example, in 2021, the official website of the Department of AYUSH in Jharkhand was breached, exposing over 3.2 lakh patient records and causing significant operational disruption (Alhammadi and Nafea.,2021)[42].

3.6 Medical Device Hacking

Medical device hacking exploits vulnerabilities in devices such as pacemakers or insulin pumps, potentially compromising patient health(Ur Rehman et al, 2020)[43]. In 2017, researchers demonstrated how pacemakers could be hacked to deliver potentially lethal shocks, highlighting the danger of medical devices vulnerabilities (Smith and Eric., 2020)[44]. While there is no such attack reported in India, the potential for harm underscores the importance of safeguarding the healthcare devices against hacking.

3.7 Advanced Persistent Threats (APTs)

APTs involve sophisticated, long-term cyberattacks where attackers gain unauthorized access to healthcare networks to steal data over extended periods (Ali, 2024)[45]. These attacks are usually carried out by well-resourced and highly skilled adversaries[46]. APTs can be particularly damaging due to their stealthy nature and the difficulty in detecting them. An example includes the 2020 attack on India's health research data, where advanced methods were used to extract sensitive information without immediate detection[47].

3.8 Social Engineering Attacks[48](SEAs)

SEAs deceive individuals into revealing confidential information or carrying out actions that undermine security. These attacks exploit psychological manipulation and trust, often targeting healthcare employees who have access to sensitive data. For example, attackers might pose as IT support personnel to gain access to critical systems. In 2019, an Indian hospital reported a social engineering attack where an impersonator tricked staff into providing access to credentials (Balaji et al, 2023)[49].

---

[38] https://www.ibm.com/topics/data-breach

[39] Alder, S. (2017, January 8). Foreign government-backed hacker was behind 2015 Anthem breach. HIPAA Journal. Retrieved from https://www.hipaajournal.com/foreign-government-backed-hacker-behind-2015-anthem-breach-8638/

[40] https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack

[41] Muhammad Zeeshan, et al. "Ensemble Learning Techniques for DDoS Attack Detection: A Comparative Study." *Journal of Information Security and Applications*, vol. 50, 2020.

[42] Alhammadi, Nafea. (2021). A Review of the Common DDoS Attack: Types and Protection Approaches Based on Artificial Intelligence. 10.54216/FPA.070101.

[43] Ur Rehman, Muhammad & Rehman, Hafiz & Khan, Zeashan. (2020). Cyber-Attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability. IJCDS Journal. 9. 10.12785/ijcds/0906020.

[44] Smith, Eric. (2020). Hacking Humans: A Glimpse into the Future of Hacking Wireless Medical Devices. 10.13140/RG.2.2.11973.27367.

[45] Ali, Strategies & Shabir, Ghulam. (2024). Advanced Persistent Threats (APTs): Analysis, Detection, and Mitigation.

[46] Ibid.

[47] Ibid.

[48] Hassan Saad Fadhil. (2023). Social engineering attacks techniques. International Journal of Progressive Research in Engineering Management and Science (IJPREMS), 3(1), 18-20. https://www.ijprems.com

[49] Balaji, P., Raghunathan, D., Aravinth, V., Sivasamy, S., Swetha, V., & Chaly, P. E. (2023). Cyber attack - Envenom in Indian healthcare: A review. International Journal of Research Publication and Reviews, 4(6), 1262-1266. Retrieved from https://iarjset.com/wp-content/uploads/2021/09/IARJSET.2021.88110.pdf

3.9 Zero-Day Exploits

Zero-day exploits are attacks that take the advantage of flaws in healthcare systems that no one knew about before. Because these flaws are unknown, there are no fixes or protections in place when the attack happens. This makes the attacks especially dangerous, as hackers can break in or cause problems without anyone being able to stop them right away (Samuel and Danita., 2023)[50]. An instance of a zero-day exploit in India's healthcare sector remains undocumented but poses a significant risk.

3.10 Email bombing

Email bombing occurs when an attacker inundates a single email address with a massive number of emails, overwhelming the recipient's server. This flood of emails can significantly slow down the server or even cause it to crash. While it doesn't involve stealing information, it disrupts communication and can cause problems for businesses. Fixing this issue involves blocking the source of the emails, filtering out spam and getting the server back to normal, which can be challenging and time-consuming[51]. Preventive steps include limiting the number of emails from one source, using spam filters, monitoring for unusual email activity and setting up servers to handle large volumes of emails. Even though email bombing doesn't steal data, it can still cause significant disruptions, so it is important to take steps to prevent it (Singh, 2021)[52].

These threats highlight the complexity and range of cybersecurity challenges faced by the healthcare sector. Addressing these threats requires a multifaceted approach, including improved security measures, employee training and robust incident response strategies.

4. Challenges in Cyber Security

4.1 Inherent Vulnerabilities in Cyberspace

The digital nature of the internet makes some vulnerabilities inevitable. For instance, in 2022, the Indian Council of Medical Research[53] (ICMR) suffered a significant data breach where personal details of over 81.5 crore citizens were exposed and sold on the dark web. This breach occurred due to inherent weaknesses in the systems managing sensitive patient data. Despite advanced security measures, the vulnerabilities in the ICMR's digital infrastructure allowed attackers to exploit these weaknesses and access large amount of confidential information (The Hindu, 2023)[54].

4.2 Numerous Entry Points

The vast number of entry points in the internet gives multiple opportunities for cyber attackers to have access without permission. In April 2024, RCC in Thiruvananthapuram faced a ransomware attack that disrupted hospital operations for five days. The attack exploited vulnerabilities across various systems and devices within the hospital, including those used for radiation and other critical functions. Each connected device, application and network connection can be a potential target, making it challenging to secure every possible access point effectively[55].

4.3 Attribution Challenges

Identifying and attributing cyberattacks is complex because of the programming of internet technology, which can obscure the nature of attacks. For example, in May 2023, KD Hospital in Ahmedabad was hit by a ransomware attack that disrupted patient data and hospital operations. The attackers demanded $70,000 in bitcoins, but the origin of the cyberattack was

[50] Samuel, Danita. (2023). Zero-day Vulnerabilities: An In-depth analysis. 10.13140/RG.2.2.12775.01445.

[51] Bass, Tim & Freyre, Alfredo & Gruber, David & Watt, Glenn. (1998). E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity. Network, IEEE. 12. 10 - 17. 10.1109/65.681925.

[52] Singh, A. (2021). A study on emerging issues of cyber attacks & security: In India. International Journal of Advanced Research and Innovative Ideas in Education (IJARIIE), 7(1), 405. Retrieved from https://ijariie.com/AdminUploadPdf/A_Study_on_Emerging_Issues_of_Cyber_Attacks_____Security___n_India_ijariie13501.pdf

[53] The Indian Council of Medical Research (ICMR), New Delhi, the apex body in India for the formulation, coordination and promotion of biomedical research, is one of the oldest medical research bodies in the world.

[54] An American cybersecurity company has said that the personally identifiable information of many Indian citizens, including Aadhaar numbers and passport details, were being sold on the dark web. (2023, November 7). Retrieved from https://www.thehindu.com/sci-tech/technology/how-the-personal-data-of-815-million-indians-got-breached-explained/article67505760.ece

[55] George, V. (2024, July 8). Cyberattack disrupted functioning of RCC, but patient data uncompromised. The Hindu. Retrieved from https://www.thehindu.com/news/national/kerala/cyber-attack-disrupted-functioning-of-rcc-but-patient-data-uncompromised-veena/article68381750.ece

not immediately clear[56]. Techniques such as IP spoofing and routing attacks through multiple networks make it difficult to trace the origin of the attack and identify those responsible, complicating efforts to respond effectively.

4.4 Defense Technology Lagging Behind Attack Technology

The rapid advancement of attack technologies often outpaces the development of defensive measures[57]. In the healthcare sector, this is evident from incidents like WannaCry ransomware attack[58] in 2017, which affected various organizations globally, including some in India. The attack used a flaw in Microsoft Windows which many systems were not trained to fix it [59]. This disparity between the speed of attack development and the pace of defensive technology updates means that new and sophisticated threats can evade detection until security measures are updated.

4.5 Diverse Actors Capable of Attacks

Cyberattacks can be perpetrated by a variety of individuals or groups, including individual hackers, nation-states and organized crime groups, each with varying capabilities and motives. In healthcare industry, the diversity of actors complicates defense strategies[60]. Like, the widespread phishing attacks in 2020 targeted several Indian hospitals, where attackers impersonated government officials to steal sensitive information. This diversity in threat actors requires adaptable and comprehensive cybersecurity strategies to address various threats effectively, from state-sponsored hacking to individual cybercriminals.

5. Regulatory Framework on Cybersecurity

5.1 Computer Emergency Response Team (CERT-In)[61]

CERT-In plays an important role in safeguarding the healthcare industry by providing specialized support and expertise in responding to cybersecurity incidents. For healthcare systems, which are subjected to cyberattacks because of the sensitive nature of their data, CERT-In offers essential guidance on managing and mitigating threats. When there is breach of data or a cyberattack, CERT-In coordinates the response, helping healthcare organizations contain the incident, assess the damage and implement measures to prevent future occurrences. By enhancing the overall security posture of healthcare institutions through proactive threat intelligence and response strategies, CERT-In ensures that these organizations can maintain the confidential critical patient information with integrity. In the recent times, huge attacks by ransomware had targeted the Indian healthcare sector. A significant report by the CERT-In revealed a 51 percent rise in ransomware incidents in India during the first half of 2022[62]. CERT-In has at times advised that victims immediately disconnect infected systems from the network, disable wireless internet connectivity and isolate all system backups to mitigate damage. In this regard, automated cloud backups can indeed protect the data from being lost due to encryption[63].

[56] Express News Service. (2023, May 17). Hospital falls prey to ransomware attack, hackers demand $70,000. The Indian Express. https://indianexpress.com/article/cities/ahmedabad/hospital-falls-prey-to-ransomware-attack-hackers-demand-70000-8613410/

[57] Lalonde Levesque, Fanny & Chiasson, Sonia & Somayaji, Anil & Fernandez, Jose. (2018). Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach. ACM Transactions on Privacy and Security. 21. 1-30. 10.1145/3210311

[58] Akbanov, Maxat & Vassilakis, Vassilios. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journal of Telecommunications and Information Technology. 1. 113 -124. 10.26636/jtit.2019.130218.

[59] Ibid

[60] Nori Katagiri. (2023) Artificial Intelligence and Cross-Domain Warfare: Balance of Power and Unintended Escalation. *Global Society* 0:0, pages 1-15.

[61] The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of Electronics and Information Technology of the Government of India. It is the nodal agency to deal with cyber security incidents. It strengthens security-related defence of the Indian Internet domain. Available at https://www.cert-in.org.in/

[62] CERT-In, India Ransomware Report 2022 [Online]. Available: https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

[63] Manuj Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," paper presented at the 14th ICCCNT IEEE Conference, July 6-8, 2023, IIT Delhi, Delhi, India. Available at https://www.meity.gov.in/writereaddata/files/Ransomware_Attack_An_Evolving_Targeted_Threat.pdf

5.2 National Critical Information Infrastructure Protection Center (NCIIPC)[64]

NCIIPC is dedicated to protecting vital information infrastructure, including healthcare systems, from cyber threats. NCIIPC's role involves identifying potential vulnerabilities within healthcare IT systems, developing robust protection strategies and ensuring the resilience of these critical infrastructures[65]. It involves working in association with healthcare providers so as to secure effectively the electronic health records (EHRs), medical devices and other essential digital resources. By focusing on the resilience and security of healthcare systems, NCIIPC helps mitigate the risks posed by cyber threats, ensuring that healthcare services remain uninterrupted and secure.

5.3 The Cyber Security Association of India (NCSAI)

NCSAI significantly impacts the healthcare sector by promoting cybersecurity awareness and best practices [66]. NCSAI serves as a medium for collaboration of cybersecurity people, professionals and organizations fostering a community focused on improving security measures across various sectors, including healthcare. Through training programs, workshops and forums, NCSAI educates healthcare organizations about cybersecurity threats and mitigation strategies. By advocating for robust cybersecurity practices and facilitating knowledge sharing, NCSAI helps healthcare institutions in safeguarding against evolving cyber threats.

5.4 Indian Cyber Crime Coordination Centre (I4C)[67]

I4C is instrumental in coordinating responses to cybercrimes, including those targeting healthcare institutions [68]. I4C supports the investigation of cybercrimes, facilitates law enforcement actions and strengthens the overall cybersecurity framework. For healthcare organizations, I4C provides critical assistance in addressing and resolving cyber incidents, such as ransomware attacks or data breaches. By working with law enforcement and other stakeholders, I4C ensures a cohesive response to cyber threats, helping healthcare providers recover from attacks and improve their security measures.

5.5 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[69]

These rules establish a regulatory framework for managing and securing digital information, including in the healthcare sector. These rules outline guidelines for data protection, incident reporting and compliance, that are crucial for cybersecurity in healthcare. By setting standards for how healthcare organizations should handle and protect patient data, personal health information can be safeguarded against unauthorized access and breaches. Further, following these regulations enable healthcare institutions maintain high standards of data security and privacy, thereby enhancing overall trust and reliability.

5.6 The National Cyber Security Policy 2013[70]

This policy provides a strategic framework for protecting India's cyberspace and information infrastructure, including the healthcare sector. The policy emphasizes the importance of building capabilities to prevent and respond to cyber threats through collaboration among various stakeholders. It focuses on enhancing cybersecurity education, awareness and research to bolster overall resilience. For healthcare institutions, this policy helps in protecting the cyber space by promoting best practices, developing advanced technologies for safeguarding and encouraging cybersecurity measures.

[64] National Critical Information Infrastructure Protection Centre (NCIIPC), a unit of NTRO, is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16th Jan 2014 based in New Delhi, India. It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. Available at https://www.nciipc.gov.in/index.html

[65] Ibid

[66] https://www.ncsai.in/about-csai

[67] Indian Cybercrime Coordination Centre (I4C) was established by MHA, in New Delhi to provide a framework and eco-system for Law Enforcement Agencies (LEAs) for dealing with Cybercrime in a coordinated and comprehensive manner. Available at https://i4c.mha.gov.in/

[68] Ibid.

[69] In February 2021, the Ministry of Electronics and Information Technology released the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Available at https://www.meity.gov.in/writereaddata/files/Revised-IT-Rules-2021-proposed-amended.pdf

[70] The Indian government introduced the National Cyber Security Policy on July 2, 2013. This policy, developed by the Department of Electronics and Information Technology (DeitY), aims to protect both public and private infrastructure from cyberattacks and safeguard sensitive information, including personal, financial, and sovereign data. Available at https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

By aligning with the National Cyber Security Policy, healthcare sector can protect its digital assets efficiently and effectively protect their patient information[71].

6. Legal framework on Cyber Attacks and Cyber Security

6.1 Bhartiya Nyaya Sanhitha 2023

1. **Section 318**: Cheating involves deceiving someone to induce them to deliver property, consent to retaining property, or act in a way that causes harm to their body, mind, reputation, or property. If cheating causes wrongful loss, the penalty can extend to 5 years imprisonment with fine, or both. If cheating induces someone to deliver property or alter or destroy valuable security, the punishment can extend to 7 years imprisonment with fine[72].
2. **Section 319:** Cheating by Personation takes place when one person pretends to be another person or represents another falsely. The punishment for this offense can extend upto five years imprisonment, with fine or both[73].
3. **Section 336** of the IPC defines forgery as the creation of a false document or electronic record with the intent to cause damage or injury, support a false claim, cause someone to part with property, or commit fraud. The general punishment for forgery is up to 2 years of imprisonment, a fine, or both. If forgery is intended for the purpose of cheating, the penalty can extend to 7 years of imprisonment and a fine. Additionally, if the forgery is meant to harm someone's reputation, the punishment can be up to 3 years of imprisonment and a fine[74].
4. **Section 352** deals with intentional insults intended to provoke breach of the public peace and punishes with up to 2 years of imprisonment with fine or both[75].
5. **Section 356** covers defamation, including in cyberspace. It criminalizes the act of making or publishing harmful statements or representations, whether spoken, written, or visual, with the intent to damage someone's reputation. This applies to defamatory content spread through digital platforms, with penalties of up to 2 years imprisonment, a fine, or both[76].

6.2 Information Technology Act, 2000[77]

This Act provides legal framework to address and mitigate various cyber threats, ensuring the security and confidentiality of health sector data and services.

1. Ransomware:

a. Section 66: Addresses hacking, which includes unauthorized access to computer systems and data, relevant for ransomware attacks[78].

b. Section 66F: Covers cyber terrorism, which can include ransomware attacks that threaten critical infrastructure, including health services[79].

2. Phishing:

a. Section 66D: Punishes cheating by personation using computer resources, covering phishing attacks in which attackers impersonate other genuine entities to steal information[80].

b. Section 66C: Deals with identity theft, which is often a consequence of phishing attacks[81].

3. Data Theft:

a. Section 43: Imposes penalties for unauthorized access and downloading of data, which applies to data theft[82].

b. Section 66B: Penalizes dishonestly receiving or retaining stolen computer resources or communication devices, relevant to handling stolen health data[83].

4. Unauthorized disclosure of Information:

[71] https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf
[72] THE BHARATIYA NYAYA SANHITA, 2023 NO. 45 OF 2023 Available at https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
[73] ibid
[74] id.
[75] id
[76] id
[77] THE INFORMATION TECHNOLOGY ACT, 2000. Available at https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[78] Ibid
[79] ibid
[80] id
[81] id
[82] id
[83] id

a. Section 72: Penalizes unauthorized access to information and its disclosure, ensuring the protection of sensitive health information.
b. Section 72A: Punishes the disclosure of information in breach of lawful contract, protecting the confidentiality of health data shared under contractual agreements[84].

5. Disrupting Services:

a. Section 69: It gives powers to government to receive, observe or decode information to prevent activities that threaten public order, which can include disruptions in health services[85].
b. Section 70: Declares certain computer systems as protected systems, making unauthorized access and disruption of these systems a punishable offense. This can apply to critical health infrastructure systems[86].

6.3 The Digital Personal Data Protection Act 2023[87]

a. **Section 8:** Mandates that organizations implement sufficient technology and organizational safeguards to secure personal data. This includes protections against unauthorized access, data breaches and other cyber threats[88].
b. **Section 10:** Requires organizations to notify the Board constituted under the Act and affected individuals about the data breach. This is crucial for timely responses to cyberattacks involving personal data, including health data[89].
c. **Section 14:** Specifies the obligation to report data breaches to the Data Protection Board within a stipulated timeframe, detailing the nature of the breach, data involved and remedial measures taken[90].
d. **Section 7:** Mandates conducting DPIAs to identify and mitigate risks related to data processing activities, including those that could be exploited by cyber attackers[91].
e. **Section 21:** Outlines penalties for non-compliance with data protection regulations, including failures in implementing adequate cybersecurity measures or reporting breaches[92].
f. **Section 27:** Requires organizations to demonstrate compliance with data protection requirements, including cybersecurity measures, to prevent and mitigate cyber threats[93].
g. **Section 30:** Establishes the Data Protection Board, which oversees compliance and adjudicates on matters related to data protection and cybersecurity breaches[94].

7 Suggestions to enhance Cyber Security

a. **Safety Certification:** Establish a safety certification mechanism for systems before public release, starting with sectors like healthcare and transport where safety is critical due to human life involvement[95].
b. **Raising Awareness**: Healthcare professionals and employees need to be informed about the latest cyber threats and how they can impact patient data and safety. Educating staff on recognizing and managing these risks is crucial for maintaining a secure healthcare environment. Awareness helps prevent breaches and enhances overall cybersecurity practices. [96]

[84] id
[85] id
[86] Id
[87] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023) is an Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. Available at https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[88] Ibid
[89] ibid
[90] id
[91] id
[92] id
[93] id
[94] id
[95] Fowler, Daniel & Epiphaniou, Gregory & Maple, Carsten. (2022). Cybersecurity Assurance and Certification for Systems. 10.13140/RG.2.2.11527.16805/1.
[96] NotPetya (2017) – International cyber law: interactive toolkit. (2022, November 14). International Cyber Law: Interactive Toolkit. https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)

c. **Invest in Security Innovation:** To stay ahead of evolving threats, invest in and prioritize the development of advanced cybersecurity solutions. This includes adopting cutting-edge technologies, continuous research and development fostering innovation to address emerging threats effectively[97].

d. **Promote Open Platforms and Standards:** Encourage the use of open platforms and security standards to facilitate collaboration among different stakeholders. This approach can accelerate the adoption of best practices, improve interoperability and enhance the collective defense against cyber threats[98].

e. **Ensure Trustworthiness of Providers:** Select technology and security providers who demonstrate a high level of trustworthiness and transparency in their operations. Evaluate their commitment to security practices, regular audits and compliance with industry standards to ensure the integrity of their products and services.

f. **Harden Products and Services:** Focus on designing and implementing products and services with robust security features. This includes rigorous testing for vulnerabilities, incorporating built-in security mechanisms for providing transparent and user-friendly cyber space[99].

g. **Adopt a Global Framework:** Support the global cybersecurity framework that provides a unified approach to security practices and standards. This framework should facilitate international cooperation, harmonize security measures and address cross-border cybersecurity challenges effectively[100].

8. Conclusion

The escalating threat of cyberattacks in the healthcare industry highlights the need for a stringent and effective cybersecurity framework. The recent advisory issued by the Indian Union Government in November 2023 mandates that social media intermediaries identify and remove misinformation and deepfakes within 36 hours, in accordance with the IT Rules 2021(Ministry of Electronics & IT, 2023)[101]. This directive not only highlights the government's commitment to enhancing user safety and trust but also sets a precedent for how cybersecurity should be approached across all sectors, including healthcare. With India now ranking as the third most cyberattacked country globally, trailing only behind the U.S. and China, the gravity of the situation is evident. This alarming statistic from Symantec Corp. signals an imperative for heightened vigilance and the implementation of advanced cybersecurity practices (Press Trust of India, 2024)[102].

As technological advancements in healthcare industry becomes inevitable, driven by its numerous benefits such as improved productivity, decision-makingand and operational efficiency (Kasoju N et al, 2023) [103] , it is crucial that healthcare organizations adopt strong and comprehensive cybersecurity measures. The integration of cutting-edge technology must be accompanied by a commitment to safeguarding sensitive patient data and protecting against emerging cyber threats. By strategically implementing robust security protocols and developing efficient cybersecurity practices, healthcare institutions can effectively mitigate risks and safeguard the critical information (Willie & Michael, 2023) [104]. Nonetheless, these measures will certainly enhance the resilience of the healthcare sector and also contribute to a more secure and trustworthy digital ecosystem.

[97] U.S. Department of Health & Human Services, Office for Civil Rights (OCR), "Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History," Guidance Portal, issued June 8, 2020, https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach.

[98] Spaeth, Sebastian & Niederhöfer, Sven. (2022). Compatibility promotion between platforms: The role of open technology standards and giant platforms. Electronic Markets. 32. 10.1007/s12525-022-00590-8.

[99] Michael Schmitt and Jeffrey Biller, "The NotPetya Cyber Operation as a Case Study of International Law," EJIL: Talk!, July 11, 2017, https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/.

[100] Greg Slabodkin, "Insulin Pumps Among Millions of Devices Facing Risk from Newly Disclosed Cyber Vulnerability, IBM Says," MedTech Dive, August 25, 2020, https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/.

[101] Ministry of Electronics & IT. (2023, November 7). Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes. PIB Delhi. Retrieved from https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445

[102] Press Trust of India. (2024, April 30). India recorded 79 million cyber attacks in 2023, ranks 3rd globally: Report. NDTV. Retrieved from https://www.ndtv.com/india-news/india-recorded-79-million-cyber-attacks-in-2023-ranks-3rd-globally-report-5558748

[103] Kasoju N, Remya NS, Sasi R, Sujesh S, Soman B, Kesavadas C, Muraleedharan CV, Varma PRH, Behari S. Digital health: trends, opportunities and challenges in medical devices, pharma and bio-technology. CSIT. 2023;11(1):11–30. doi: 10.1007/s40012-023-00380-3. Epub 2023 Apr 11. PMCID: PMC10089382.

[104] Willie, Michael. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture.

References:

1. Abernethy, A., Adams, L., Barrett, M. A., Bechtel, C., Brennan, P. A., Butte, A., Faulkner, J., Fontaine, E., Friedhoff, S., Halamka, J. D., Howell, M., Johnson, K., Long, P., McGraw, D., Miller, R., Lee, P., Perlin, J. A., Rucker, D., Sandy, L., Savage, L. C., Stump, L., Tang, P., Topol, E., Tuckson, R. V., & Valdes, K. (2022). The promise of digital health: Then, now, and the future. NAM Perspectives, 2022.
2. Alder, S. (2017, January 8). Foreign government-backed hacker was behind 2015 Anthem breach. HIPAA Journal. Retrieved from https://www.hipaajournal.com/foreign-government-backed-hacker-behind-2015-anthem-breach-8638/ as Accessed on October 23, 2024.
3. Ahmad, S., Dar, S., Ahmad, N., & Lone, N. (2022). Cyber crime in India. Sambodhi (UGC Care Journal), 43(4). Available from https://www.researchgate.net/publication/357839318_CYBER_CRIME_IN_INDIA. Accessed on 23/10/2025.
4. Akbanov, M., & Vassilakis, V. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention, and propagation mechanisms. Journal of Telecommunications and Information Technology, 1, 113-124. https://doi.org/10.26636/jtit.2019.130218. Retrieved from https://doi.org/10.26636/jtit.2019.130218. Accessed on 25/10/24.
5. Alhammadi, N. (2021). A review of the common DDoS attack: Types and protection approaches based on artificial intelligence. Frontiers in Physical Analytics, 7(1).. Retrieved from https://doi.org/10.54216/FPA.070101 As Accessed on October 24, 2025.
6. Apollo Hospitals. (2022, October 11). Apollo Hospitals has launched an automated AI-based real-time rapid-response patient monitoring system, Enhanced Connected Care. Apollo in the News.
7. Bagchi, S. (2023, October 31). ICMR data leak reveals personal information of 81.5 cr Indians: Report. TechCircle. Retrieved from https://www.techcircle.in/2023/10/31/icmr-data-leak-reveals-personal-information-of-81-5-cr-indians-report. Accessed on 23/10/2024.
8. Balaji, P., Raghunathan, D., Aravinth, V., Sivasamy, S., Swetha, V., & Chaly, P. E. (2023). Cyber attack - Envenom in Indian healthcare: A review. International Journal of Research Publication and Reviews, 4(6), 1262-1266. Retrieved from https://iarjset.com/wp-content/uploads/2021/09/IARJSET.2021.88110.pdf. As Accessed on October 24, 2025.
9. Bass, T., Freyre, A., Gruber, D., & Watt, G. (1998). E-mail bombs and countermeasures: Cyber attacks on availability and brand integrity. IEEE Network, 12, 10-17. Retrieved from https://doi.org/10.1109/65.681925. As Accessed on October 24, 2025.
10. Blackman, J. (2024, July 16). Four in five using AI, says TCS – as it brings gen AI and IoT support for enterprises. RCR Wireless News. Available from https://www.rcrwireless.com/20240716/ai-ml/industrial-ai/four-in-five-using-ai-says-tcs-as-it-brings-gen-ai-and-iot-support-for-enterprises. Accessed on 23/10/2025.
11. Chandwani, R., Edacherian, S., & Sud, M. (2023). National digital infrastructure and India's healthcare sector: Physician's perspectives. The Qualitative Report, 28(2), 360-386. Available from https://doi.org/10.46743/2160-3715/2023.4964. Accessed on 23/10/2025.
12. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118.
13. Express News Service. (2023, May 17). Hospital falls prey to ransomware attack; hackers demand $70,000. The Indian Express. Retrieved from https://indianexpress.com/article/cities/ahmedabad/hospital-falls-prey-to-ransomware-attack-hackers-demand-70000-8613410/. Accessed on 23/10/2024.
14. Fadhil, H. S. (2023). Social engineering attacks techniques. International Journal of Progressive Research in Engineering Management and Science (IJPREMS), 3(1), 18-20. Retrieved from https://www.ijprems.com. Accessed on October 24, 2025.
15. Gandhi, P., & Tandon, N. (2021). To assess the impact of CRM implementation in the health industry. Vidyabharati International Interdisciplinary Research Journal (Special Issue 10), 126–129. Available from http://www.viirj.org/specialissues/SP10/Part%201.pdf. Accessed on 23/10/2025.
16. George, V. (2024, July 8). Cyberattack disrupted functioning of RCC, but patient data uncompromised. The Hindu. Retrieved from https://www.thehindu.com/news/national/kerala/cyber-attack-disrupted-functioning-of-rcc-but-patient-data-uncompromised-veena/article68381750.ece. Accessed on 23/10/2024.
17. Government of India. (2023). The Bharatiya Nyaya Sanhita, 2023 No. 45 of 2023. Retrieved from https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf. As Accessed on 25/10/24.

18. Government of India. (2000). The Information Technology Act, 2000. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf. Accessed on 25/10/24.
19. Gliklich, R. E., Leavy, M. B., & Dreyer, N. A. (Eds.). (2020). Registries for evaluating patient outcomes: A user's guide (4th ed.). Agency for Healthcare Research and Quality (US). Available from https://www.ncbi.nlm.nih.gov/books/NBK562575/. Accessed on 23/10/2025.
20. Healthcare MEA. (2021, November 26). Dr. Lal PathLabs, Ibex partner to deploy AI-powered cancer diagnostics in India. Healthcare MEA. Available from https://www.healthcaremea.com/dr-lal-pathlabs-ibex-partner-to-deploy-ai-powered-cancer-diagnostics-in-india/. Accessed on 23/10/2025.
21. Hlatshwayo, M. (2023). Cybersecurity in the digital space. Available at https://www.researchgate.net/publication/375115830_CYBERSECURITY_IN_THE_DIGITAL_SPACE/citation/download. Retrieved on 23/10/2024.
22. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., Abdulkarim, M., Shuaibu, A. N., Garba, A., Sahalu, Y., Mohammed, A., Mohammed, T. Y., Abdulkadir, B. A., Abba, A. A., Kakumi, N. A. I., & Mahamad, S. (2022, October 3). Recent advancements in emerging technologies for healthcare management systems: A survey. Healthcare (Basel), 10(10), 1940. Available from https://doi.org/10.3390/healthcare10101940. Accessed on 23/10/2025.
23. Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. Wireless Personal Communications, 112, 112. https://doi.org/10.1007/s11277-020-07143-2. Retrieved on 23/10/2024.
24. Kalaimannan, E., John, S. K., DuBose, T., & Pinto, A. (2017). Influences on ransomware's evolution and predictions for future challenges. Journal of Cyber Security Technology, 1(1), 23-31. https://doi.org/10.1080/23742917.2016.1252191. Accessed on 23/10/24.
25. Kim, R. (n.d.). Report: 40 percent of mobile ad clicks are fraud or accidents. Retrieved from http://www.raisingthevolume.com/wp-content/uploads/2012/01/Mobile.pdf. Accessed on 23/10/2024.
26. Lalonde Levesque, F., Chiasson, S., Somayaji, A., & Fernandez, J. (2018). Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security, 21, 1-30. https://doi.org/10.1145/3210311. Retrieved from https://doi.org/10.1145/3210311. Accessed on 25/10/24
27. Lohchab, H. (2023, November 3). Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: Report. Economic Times. Retrieved from https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr. Accessed on 23/10/2024.
28. Luo, X., & Liao, Q. (2017). Awareness education as the key to ransomware prevention. Information Systems Security, 16(4), 195-202. https://doi.org/10.1080/10658980701576412. Accessed on 23/10/24.
29. Ministry of Electronics & IT. (2023, November 7). Union government issues advisory to social media intermediaries to identify misinformation and deepfakes. PIB Delhi. Retrieved from https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445. Accessed on 25/10/24.
30. Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. Computers & Security, 138, 103670. https://doi.org/10.1016/j.cose.2023.103670. Accessed on 23/10/24.
31. Muhammad, Z., et al. (2020). Ensemble learning techniques for DDoS attack detection: A comparative study. Journal of Information Security and Applications, 50. Retrieved from https://doi.org/10.1016/j.jisa.2020.102427. As Accessed on October 24, 2025.
32. Nadeem, M., Zahra, S., Abbasi, M., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing attack, its detections and prevention techniques. International Journal of Wireless Information Networks, 12, 13-25. https://doi.org/10.37591/IJWSN Retrieved from https://doi.org/10.37591/IJWSN as Accessed on October 23, 2024.
33. Narain, P. (2018). Ransomware - Rising menace to an unsuspecting cyber audience. The University of Houston. Retrieved from http://hdl.handle.net/10657/3145. Accessed on 23/10/24.
34. NotPetya (2017) – International cyber law: Interactive toolkit. (2022, November 14). International Cyber Law: Interactive Toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017). Accessed on 25/10/24.
35. Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the future – Big data, machine learning, and clinical medicine. New England Journal of Medicine, 375(13), 1216-1219. Available from https://doi.org/10.1056/NEJMp1606181. Accessed on 23/10/2025.

36. Pathak, P. B. (2016). Malware: A growing cybercrime threat: Understanding and combating malvertising attacks. International Journal of Advanced Research in Computer Science, 7(2), 1-4. Retrieved from [URL if available]. Accessed on 23/10/24.
37. Pariti, G. (2024, June 28). India's healthcare sector battling 6,953 weekly cyberattacks: Report. India Technology News. Retrieved from https://indiatechnologynews.in/indian-healthcare-sector-faces-6953-cyberattacks-weekly-outpacing-global-rates-check-point-threat-intelligence-report/. Accessed on 23/10/2024.
38. Press Trust of India. (2024, April 30). India recorded 79 million cyber attacks in 2023, ranks 3rd globally: Report. NDTV. Retrieved from https://www.ndtv.com/india-news/india-recorded-79-million-cyber-attacks-in-2023-ranks-3rd-globally-report-5558748. Accessed on 25/10/24.
39. Priestman, W., Anstis, T., Sebire, I., Sridharan, S., & Sebire, N. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ Health & Care Informatics, 26, Article 100031. https://doi.org/10.1136/bmjhci-2019-100031 Retrieved from https://doi.org/10.1136/bmjhci-2019-100031 as Accessed on October 23, 2024.
40. Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347-1358.
41. Rao, P., & Tiwari, A. K. (2020). Laws related to cyber-crime in India. Research Journal of Engineering and Technology, 11(2), 41-44. Available from https://doi.org/10.5958/2321-581X.2020.00007.0. Accessed on 23/10/2025.
42. Saha, N. (2024, June 24). Innovative telemedicine startups of India promising connected healthcare. Digital Health News. Available from https://www.digitalhealthnews.com/innovative-telemedicine-startups-of-india-promising-connected-healthcare. Accessed on 23/10/2025.
43. Samuel, D. (2023). Zero-day vulnerabilities: An in-depth analysis. https://doi.org/10.13140/RG.2.2.12775.01445. As Accessed on October 24, 2025.
44. Schmitt, M., & Biller, J. (2017, July 11). The NotPetya cyber operation as a case study of international law. EJIL: Talk! Retrieved from https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/. Accessed on 25/10/24.
45. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9, 1460. https://doi.org/10.3390/electronics9091460 Retrieved from https://doi.org/10.3390/electronics9091460 as Accessed on October 23, 2024.
46. Sharma, B. (2022, December 2). Explained: What's happening at AIIMS after sensitive ransomware attack? IndiaTimes. Retrieved from https://www.indiatimes.com/explainers/technology/explainer-aiims-ransomware-attack-586542.html. Accessed on 23/10/2024.
47. Slabodkin, G. (2020, August 25). Insulin pumps among millions of devices facing risk from newly disclosed cyber vulnerability, IBM says. MedTech Dive. Retrieved from https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/. Accessed on 25/10/24.
48. Smith, E. (2020). Hacking humans: A glimpse into the future of hacking wireless medical devices. ResearchGate. https://doi.org/10.13140/RG.2.2.11973.27367
    Retrieved from https://doi.org/10.13140/RG.2.2.11973.27367. As Accessed on October 24, 2025.
49. Srivastava, S. (2020, September 8). International Literacy Day: Bridging India's digital divide. BloombergQuint. Retrieved from https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-digitalivide. Accessed on 23/10/2024.
50. Song, S., Kim, B., & Lee, S. (2016). The effective ransomware prevention technique using process monitoring on Android platform. Mobile Information Systems, 1-9. https://doi.org/10.1155/2016/2946735. Accessed on 23/10/24.
51. Spaeth, S., & Niederhöfer, S. (2022). Compatibility promotion between platforms: The role of open technology standards and giant platforms. Electronic Markets, 32. https://doi.org/10.1007/s12525-022-00590-8. Retrieved from [Link]. Accessed on 25/10/24.
52. Tariq, R. A., & Hackert, P. B. (2023). Patient confidentiality. In StatPearls [Internet]. StatPearls Publishing. Available from https://www.ncbi.nlm.nih.gov/books/NBK519540/. Accessed on 23/10/2025.
53. Ur Rehman, M., Rehman, H., & Khan, Z. (2020). Cyber-attacks on medical implants: A case study of cardiac pacemaker vulnerability. IJCDS Journal, 9. Available at https://doi.org/10.12785/ijcds/0906020. Retrieved from https://doi.org/10.12785/ijcds/0906020. As Accessed on October 24, 2025.

54. U.S. Department of Health & Human Services, Office for Civil Rights (OCR). (2020, June 8). Anthem pays OCR $16 million in record HIPAA settlement following largest U.S. health data breach in history. Guidance Portal. Retrieved from https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach. Accessed on 25/10/24.

55. Yadav, A. (2021). Phishing in India – Analytical study. International Advanced Research Journal in Science, Engineering and Technology, 8(8), 674-679. https://doi.org/10.17148/IARJSET.2021.88110. Retrieved on 23/10/2024.