IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

India's Cyberattack Surge (2023–2025): Trends, Frequency, And Sector-Wise Impact

Piyush Solanki*, Jahnvi Gulati**, Harshita Gupta***, Yogita Thareja****

*Research Scholar, Vivekananda Institute of Professional Studies, Delhi,
** Research Scholar, Vivekananda Institute of Professional Studies, Delhi,
***Research Scholar, Vivekananda Institute of Professional Studies, Delhi,
****Assistant Professor, Vivekananda Institute of Professional Studies, Delhi,

Abstract

In the modern digital era, technology has become an essential part of everyday life, supporting communication, banking, healthcare, education, and government services. As India rapidly expands its digital infrastructure and internet usage, the country has also witnessed a significant rise in cyber threats. Cybercriminals are continuously developing new techniques to exploit vulnerabilities in digital systems, making cybersecurity a critical concern for organizations, institutions, and individuals.

This journal explores several major cybersecurity incidents and trends that affected India between 2023 and 2025. It examines important cases such as the AIIMS Delhi cyberattack, the ICMR data breach, the WazirX cryptocurrency exchange hack, issues related to Aadhaar-linked data exposure, cyber activities observed during Operation Sindoor, and the broader surge of more than 265 million cyberattack detections in India during 2025. These incidents demonstrate different types of cyber threats, including ransomware attacks, phishing campaigns, malware infections, data breaches, and distributed denial-of- service (DDoS) attacks.

By analysing these real-world events, the journal highlights how cyberattacks can disrupt critical sectors such as healthcare, government institutions, financial services, and digital platforms. It also explains how attackers exploit technical vulnerabilities and use social engineering techniques to gain unauthorized access to systems and sensitive information.

Overall, this journal aims to provide a clearer understanding of the growing cybersecurity challenges in India, the evolving strategies used by cyber attackers, and the importance of strengthening cybersecurity awareness, policies, and technological defenses to protect the country's digital infrastructure and data.

Keywords: Cybersecurity, Cyberattacks in India, Data Breaches, Ransomware Attacks, Phishing Attacks, Digital Infrastructure Security, Cyber Threat Landscape

Introduction

Over the past decade, the rapid growth of digital technology has changed the way people communicate, work, and access services. Governments, hospitals, financial institutions, and businesses now rely heavily on digital systems to store data and deliver services. While this digital transformation has improved efficiency and connectivity, it has also created new security challenges. Cybercriminals continuously attempt to exploit weaknesses in computer networks, making cybersecurity one of the most important concerns in today's digital world.

India is currently one of the fastest-growing digital economies, with millions of people using online banking, digital payment platforms, cloud services, and e-governance systems every day. As the number of internet users and connected devices increases, the risk of cyberattacks also grows. Cyber attackers use various techniques such as phishing emails, ransomware attacks, malware infections, data breaches, and distributed denial-of-service (DDoS) attacks to gain unauthorized access to systems or disrupt online services. These attacks can lead to financial losses, exposure of sensitive information, and disruption of critical services.

In recent years, several high-profile cyber incidents have highlighted the vulnerability of digital infrastructure in India. Attacks on healthcare institutions, cryptocurrency exchanges, and government databases have shown how cyber threats can affect multiple sectors of society. At the same time, cybersecurity organizations and government agencies have reported a steady increase in the number of cyber threats detected across the country.

Understanding cyberattack trends helps researchers, policymakers, and organizations identify emerging threats and strengthen cybersecurity defenses. The table below shows an overview of the estimated number of cyberattack detections in India from 2022 to 2026, based on cybersecurity threat reports and national security data.

Year	Estimated Cyberattack Detections in India	Source
2022	134 million cyber threats detected	CERT-In Annual Report
2023	192 million cyber threats detected	CERT-In & Cybersecurity Research Reports
2024	221 million cyber threats detected	Data Security Council of India (DSCI)
2025	265 million cyber threats detected	Seqrite India Cyber Threat Report 2026
2026	290 million cyber threats projected	Quick Heal / Seqrite Cybersecurity Forecast

Table 1. Cyberattack Detection in 2022-2026

The rising trend shown in the table clearly indicates that cyber threats are increasing each year. As India continues to expand its digital infrastructure, strengthening cybersecurity policies, improving threat detection technologies, and increasing public awareness will be essential to protect sensitive data and national digital infrastructure.

1. AIIMS New Delhi Ransomware Attack

In late November 2022 the All India Institute of Medical Sciences (AIIMS), New Delhi — India's premier public hospital and a national health landmark — suffered a severe ransomware incident that immediately exposed how fragile hospital IT systems can be when under attack. The first signs were classic: hospital applications and e-services including online registration, laboratory reporting, billing and appointment systems abruptly stopped working on the morning the incident was detected, forcing staff to

switch to manual paper processes to keep care going.

The operational pain was real and visible: long queues at OPD counters, delayed test reports, and clinicians forced to rely on memory or hand-written notes instead of electronic records. Officials and journalists later reported that the attackers encrypted a very large volume of hospital data — more than 1 TB of files, according to government responses reported in the media — and that recovery was neither immediate nor trivial.

Scale mattered. Early media coverage and subsequent government questions suggested that the breach potentially touched patient information at a very large scale — reports even quoted fears that data of millions of patients (figures like 3–4 crore were mentioned in some news pieces) may have been affected, which helped the incident quickly become a national conversation about health- data security. Whether every one of those records was exfiltrated or merely rendered temporarily inaccessible remains a technical question, but the perceived scale alone changed how policymakers and hospital leaders viewed digital-health risk.

As often happens in high-profile hacks, there were also claims and counterclaims in the open press: some outlets reported ransom demands (news reports mentioned a demand figure widely circulated on social media and some sources, e.g., Rs. 200 crore), while official spokespeople and police statements were more cautious about confirming specific ransom amounts. The mixture of leaked claims, investigative reporting and official briefings made it important to separate verified facts (systems down, manual processes adopted, forensic investigations launched) from early, unverified figures.

Technically, several structural weaknesses in typical public hospital IT setups were revealed: centralized servers without robust segmentation, inconsistent patching and legacy software, and backups that were not isolated in a way that would make quick recovery straightforward. These are the recurring themes cyber experts pointed to when analysing why healthcare institutions are attractive ransomware targets and why recovery can be so slow and expensive. The partial resumption of some server functions weeks later showed progress in containment and restoration, but it also underscored the need for better preparedness (offline backups, table-top incident drills, endpoint protections and staff phishing awareness).

Beyond hospital corridors, the incident raised national-level concerns: AIIMS treats high-profile patients and handles research and critical public-health functions, so an outage or data compromise had implications for national security, public confidence, and the overall momentum of India's digital health programs. In short, the AIIMS episode became a wake-up call — not just about one hospital's IT, but about sectoral readiness and the urgency of treating healthcare cyber resilience as a public-safety priority.

2. ICMR Data Breach (2023)

In October 2023, India faced what many cybersecurity experts described as one of its largest data breaches in history, involving the personal information of approximately 81.5 crore (815 million) Indian citizens. The breach became public when a hacker using the alias *pwn0001* posted an offer on a notorious dark web forum to sell an enormous dataset including *Aadhaar numbers, passport details, phone numbers, names, and addresses* of Indian residents — supposedly sourced from the database of the Indian Council of Medical Research (ICMR), the nation's apex body for biomedical research and public health data. Cybersecurity intelligence firm Resecurity first identified the leaked data, and partial samples containing valid Aadhaar information were verified via the official *Verify Aadhaar* portal, indicating that the data could be genuine and not just fabricated entries.

The scale of this breach was unprecedented. Reporters and security analysts estimated that the exposed information covered *almost two-thirds* of India's population, leading to widespread concern among citizens, policymakers, and privacy advocates. The hacker reportedly offered the full dataset for sale for about $80,000 (≈ Rs 66 lakh) — a stark reminder of how stolen personal data has become a valuable commodity on the dark web. While *ICMR* did not immediately confirm how or whether its internal systems were directly compromised, the association with COVID-19 test records raised significant questions about how emergency-era health data was stored and secured.

The implications of this breach extend far beyond one organisation. Personal identifiable information (PII) of such magnitude raises serious privacy and security risks, including identity theft, financial fraud, and social engineering attacks. National investigative bodies, including the Central Bureau of Investigation (CBI) and the Indian Computer Emergency Response Team (CERT-In), were expected to examine the incident and offer mitigation guidance, though formal public reports remained limited at the time. Cybersecurity experts emphasised that the incident highlights the urgent need for strong data governance frameworks, strict access controls, and encryption standards
— particularly for government databases that store sensitive citizen information. The ICMR breach has therefore become a pivotal case in India's ongoing dialogue about cybersecurity, data privacy, and digital trust.

3. Wazir X Cryptocurrency Exchange Hack (2024)

The WazirX cryptocurrency exchange hack of July 2024 became one of the most significant cyber incidents in India's digital financial sector. WazirX, founded in 2018, is among India's largest cryptocurrency trading platforms and allows users to buy, sell, and store digital assets such as Bitcoin, Ethereum, and other crypto tokens. On 18 July 2024, the exchange announced that attackers had compromised one of its multisignature cryptocurrency wallets, leading to the theft of approximately
$230–235 million (around ₹2,000 crore) worth of digital assets. The stolen funds included Ethereum and several ERC-20 tokens, which were rapidly transferred to external blockchain addresses controlled by the attackers.

Initial investigations revealed that the attack targeted a multisignature Ethereum wallet connected to a third-party custody provider, Liminal Custody. Multisignature wallets normally require approvals from multiple private keys before transactions can be executed, making them more secure than single-key wallets. However, the attackers were able to manipulate the transaction approval process, enabling unauthorized transfers of funds.

Blockchain security researchers later indicated that the attack pattern resembled operations carried out by the Lazarus Group, a highly sophisticated hacking organization believed to be linked to North Korea that has previously targeted global cryptocurrency exchanges and blockchain platforms.
The consequences of the breach were immediate and severe. WazirX suspended withdrawals and paused trading operations to prevent additional losses and to begin a forensic investigation. Because cryptocurrency transactions are recorded permanently on the blockchain and cannot be reversed, recovering stolen assets becomes extremely challenging once they are transferred to attacker-controlled wallets. Reports suggested that the stolen amount represented a large portion of the exchange's reserves, which created panic among users and raised serious questions about the security of centralized cryptocurrency platforms. Law-enforcement authorities and cybersecurity firms began tracing the movement of stolen assets through blockchain analytics tools.

Beyond the direct financial loss, the WazirX incident exposed broader cybersecurity risks in the rapidly growing cryptocurrency ecosystem. It demonstrated that even advanced security mechanisms such as multisignature wallets can be vulnerable if operational processes, integration systems, or third-party infrastructure are compromised. The hack intensified debates about the need for stronger cybersecurity

frameworks, regulatory oversight, and secure custody solutions for cryptocurrency exchanges operating in India. As digital finance continues to expand, the WazirX hack remains an important case study highlighting how cyberattacks can threaten emerging financial technologies and investor trust.

4. Aadhaar and Bank-Linked Data Exposure (2024)

In 2024, cybersecurity researchers and media investigations raised concerns about the exposure of Aadhaar-linked personal information connected to Indian citizens' identity and banking records.
Aadhaar, issued by the Unique Identification Authority of India (UIDAI), is the world's largest biometric identification system and currently covers more than 1.3 billion residents of India. Because Aadhaar numbers are commonly linked to bank accounts, mobile SIM verification, government welfare programs, and digital payment systems, any leak of Aadhaar-related information can potentially expose citizens to large-scale identity and financial fraud.

Investigations revealed that large datasets containing personal information such as Aadhaar numbers, names, addresses, phone numbers, and demographic details were circulating on online forums and dark- web marketplaces. In one widely discussed investigation connected to national health data systems, cybersecurity analysts reported that data associated with approximately 81.5 crore individuals may have been exposed. Samples of the leaked datasets reportedly contained real identity details, suggesting that attackers had gained access to poorly secured databases storing Aadhaar-linked information.

Government authorities clarified that the core Aadhaar database managed by UIDAI had not been directly breached. Instead, experts explained that most Aadhaar-related leaks occur through third-party platforms, private companies, or government portals that store Aadhaar-linked records without adequate cybersecurity protections. When these external systems are compromised, attackers may obtain sensitive identity data even though the central Aadhaar infrastructure remains protected. UIDAI has repeatedly stated that the Aadhaar system uses multi-layer encryption, biometric authentication, and strict security audits to safeguard the main identity database.

Despite these assurances, the exposure of Aadhaar-linked information still creates significant cybersecurity risks. Stolen identity data can be used by cybercriminals for identity theft, fraudulent banking transactions, SIM-swap attacks, phishing campaigns, and financial scams. The incident therefore intensified national discussions about data privacy, cybersecurity standards, and the responsibility of organizations handling Aadhaar-linked information. It also reinforced the importance of implementing India's Digital Personal Data Protection framework and strengthening cybersecurity practices among institutions that manage sensitive personal data.

Overall, the 2024 Aadhaar-related data exposure highlights the growing challenge of protecting large- scale digital identity systems in a rapidly expanding digital economy. As more services rely on Aadhaar authentication, ensuring the security of identity and banking data has become a critical priority for both government agencies and private organizations.

5. Cyber Events During Operation Sindoor (2025)

The cyber activities linked to Operation Sindoor in May 2025 show how modern conflicts increasingly involve both physical and digital dimensions. Operation Sindoor was launched by India on 7 May 2025 following the Pahalgam terrorist attack on 22 April 2025, which resulted in the deaths of 26 civilians in Jammu and Kashmir. While public attention focused mainly on the military response, cybersecurity analysts observed a parallel increase in cyberattacks targeting Indian digital infrastructure, including government websites, defence networks, and communication systems.

Security reports indicated that more than 1.5 million cyberattack attempts were directed at Indian digital systems in the days following the operation. Most of these attacks were unsuccessful due to existing

cybersecurity protections, with only about 150 incidents resulting in minor disruptions or website defacements. Many of these cyber operations were attributed to APT36 (Advanced Persistent Threat 36), also known as Transparent Tribe, a hacking group known for conducting cyber-espionage campaigns against Indian government and defence institutions.

One of the primary techniques used in the campaign was spear-phishing, where attackers sent targeted emails to individuals working in government departments and defence organizations. These emails were carefully designed to appear legitimate and often contained attachments disguised as security briefings, PDF reports, or PowerPoint presentations related to the Pahalgam attack or Operation Sindoor. When the attachment was opened, hidden malicious code executed in the background and installed malware on the victim's computer.

The malware used in many of these attacks was identified as Crimson RAT (Remote Access Trojan), a tool previously linked to APT36 cyber-espionage activities. Once installed, Crimson RAT allowed attackers to gain remote access to compromised systems. The malware could collect system information, capture screenshots, record keystrokes, and transfer files to external servers controlled by the attackers. Investigators also observed that infected machines attempted to connect to remote command-and-control (C2) servers through unusual network ports, which helped cybersecurity teams detect suspicious activity during investigations.

In addition to espionage campaigns, several hacktivist groups attempted cyberattacks on Indian websites during the same period. Groups such as Pakistan Cyber Force, Team Insane PK, and Islamic Hacker Army reportedly launched distributed denial-of-service (DDoS) attacks and website defacement attempts against government portals and public sector websites. At the peak of the cyber campaign between 7–10 May 2025, monitoring systems recorded multiple DDoS attempts per hour, with nearly 75% of attacks targeting government-related infrastructure.

Although most attacks were blocked or quickly mitigated, the incidents highlighted the growing role of cyberspace in modern geopolitical conflicts. Cyberattacks during Operation Sindoor were aimed not only at gathering intelligence but also at disrupting services and influencing public perception during a period of heightened tension. The events demonstrate that cybersecurity has become an essential component of national security, as digital infrastructure is now closely connected to defence, governance, and communication systems.

6. India's 265 Million Cyberattack Wave (2025)

In 2025, India experienced a significant surge in cyber threats, with security systems detecting more than 265 million cyberattack attempts across the country. These findings were reported in the India Cyber Threat Report 2026, released by cybersecurity firm Seqrite. The report analyzed data from over 8 million monitored devices, including computers, servers, and enterprise systems across Indian organizations between October 2024 and September 2025. The results highlight the growing challenges of cybersecurity as India continues to expand its digital infrastructure, online services, and connected technologies.

When these numbers are examined more closely, the scale of the threat becomes even clearer. The 265 million cyberattack detections translate to approximately 727,000 cyber threats every day, which means that Indian networks faced around 500 cyberattack attempts every minute during the monitored period. These attacks included various forms of malicious activity such as malware infections, phishing campaigns, ransomware attacks, and network intrusion attempts. Many of these attacks are automated, meaning cybercriminals use advanced tools to continuously scan thousands of systems for vulnerabilities.

Among all the threats detected, Trojan malware and file-infecting viruses were the most common attack types, accounting for nearly 70% of all cyber threats recorded in the report. Security researchers identified approximately 88 million Trojan detections and more than 71 million file-infector attacks.

Trojan malware is particularly dangerous because it disguises itself as legitimate software or files, tricking users into installing it. Once installed, it can secretly steal sensitive information, monitor user activity, or allow attackers to gain control of the infected device.

The report also revealed that certain regions in India experienced higher levels of cyber threats. Maharashtra, Gujarat, and Delhi were among the most targeted states, while major cities such as Mumbai, Kolkata, and New Delhi recorded the highest number of cyberattack detections.
These locations host large numbers of government offices, financial institutions, and technology companies, making them attractive targets for cybercriminals seeking valuable data or financial gain.

In addition, several industries were found to be more vulnerable than others. The education , healthcare, and manufacturing sectors accounted for nearly 47% of all detected cyber threats. These sectors often store large amounts of sensitive information but may not always have strong cybersecurity defenses, making them frequent targets for phishing attacks, ransomware infections, and data theft attempts.

Overall, the surge of 265 million cyberattacks in 2025 highlights the increasing importance of cybersecurity in India's rapidly growing digital ecosystem. As businesses, government institutions, and public services rely more heavily on digital technologies, protecting networks and sensitive information has become essential. Strengthening cybersecurity infrastructure, increasing awareness among users, and adopting advanced threat-detection systems will play a crucial role in defending against future cyber threats.

➢ **Government of India Cybersecurity Measures (2023–2026)**

1. New Laws and Legal Framework

- Digital Personal Data Protection Act, 2023 – Introduced by the Ministry of Electronics & Information Technology, this Act is one of the biggest cybersecurity developments in recent years. It controls how companies collect, store, and use digital personal data. The main aim of this law is to protect citizens' privacy and make companies legally responsible if they fail to protect user data.

- Implementation Rules under DPDP (2024–2025) – After passing the Act, the government started gradually implementing detailed rules to ensure that organizations follow proper data protection standards and compliance procedures.

- Strengthening of IT Act & CERT-In Directions – The government also reinforced cybersecurity rules under the IT framework to make incident reporting compulsory and improve digital security governance.

2. Mandatory Incident Reporting & Monitoring

- CERT-In Mandatory Reporting Rule – The Indian Computer Emergency Response Team made it mandatory for organizations to report specific cyber incidents within strict timelines (commonly six hours). This helps the government respond quickly and control cyberattacks before they spread further.

- Centralized Incident Handling System – The government improved national-level monitoring systems, threat alert mechanisms, and coordination between different cybersecurity agencies.

- Critical Infrastructure Reporting (CII Rules) – Extra protection measures were introduced for important sectors like banking, telecom, power, and transportation, because attacks on these sectors can affect the entire country.

3. Technical Guidelines & Security Controls

- Sector-Specific Security Guidelines (2023–2026) – CERT-In released various cybersecurity frameworks for government departments, MSMEs, and even emerging sectors like space and satellite communications. These guidelines help organizations follow standard security practices.

- Mandatory Cyber Audits & Vulnerability Assessments – Organizations were required to conduct regular security audits and vulnerability testing to identify weaknesses and fix them before hackers exploit them.
- Financial Sector Cybersecurity Framework – The Reserve Bank of India strengthened cybersecurity requirements for banks and digital payment systems. Banks were instructed to use Security Operations Centers (SOC), real-time monitoring systems, and fraud detection tools to protect customers.

4. Capacity Building & Training

- Cyber Surakshit Bharat Program – This initiative focuses on training government IT officials and Chief Information Security Officers (CISOs) to improve cyber awareness and technical skills.

- National Cyber Exercises – The government conducted cyber drills and simulations to test how departments respond during cyber emergencies.

5. Citizen Protection & Awareness

- Cyber Swachhta Kendra Initiative – The Cyber Swachhta Kendra provides free malware removal tools and spreads cybersecurity awareness among citizens to reduce botnet and ransomware attacks.

- Public Cyber Awareness Campaigns – The government regularly issues advisories about phishing, OTP fraud, ransomware, and digital payment scams to educate citizens.

6. Institutional Strengthening

- Role of NCIIPC – The National Critical Information Infrastructure Protection Centre strengthened protection of national critical infrastructure like power grids, telecom networks, and financial systems.

- Inter-Agency Coordination – Better coordination was developed between MeitY, CERT-In, financial regulators, and private sector organizations to improve national cyber resilience.

CONCLUSION

The rapid growth of digital technology has transformed the way societies function, making cybersecurity a critical component of national security and economic stability. As India continues to expand its digital ecosystem through online banking, e-governance platforms, healthcare databases, cloud computing, and digital payment systems, the risk of cyber threats has increased significantly. The incidents discussed in this journal clearly demonstrate how cyberattacks can affect different sectors of society and highlight the importance of strong cybersecurity frameworks.

Major incidents such as the AIIMS Delhi cyberattack, the ICMR data breach, the Wazir X crypto currency

exchange hack, concerns surrounding Aadhaar-linked data exposure, and the cyber activities observed during Operation Sindoor reveal the diverse nature of cyber threats faced by India. These cases illustrate how attackers use techniques such as ransomware, phishing, malware infections, data breaches, and distributed denial-of-service (DDoS) attacks to gain unauthorized access to systems, steal sensitive data, or disrupt critical services.
The report of over 265 million cyberattack detections in India during 2025 further highlights the scale and seriousness of the growing cybersecurity challenge.

These events show that cyber threats are no longer isolated incidents but part of a broader and evolving threat landscape. Cybercriminal groups, hacktivists, and even state-sponsored attackers increasingly target government institutions, healthcare systems, financial organizations, and digital platforms. As technology becomes more integrated into daily life, protecting digital infrastructure becomes essential for maintaining national stability and public trust.

At the same time, the Government of India has introduced several measures to strengthen cybersecurity, including the Digital Personal Data Protection Act, CERT-In reporting guidelines, cybersecurity frameworks for critical infrastructure, and public awareness initiatives. These efforts aim to improve national cyber resilience and ensure that organizations follow proper security practices.

In conclusion, addressing cybersecurity challenges requires a collective effort from governments, organizations, and individuals. Continuous investment in advanced security technologies, regular security audits, improved cyber awareness, and stronger data protection policies are necessary to safeguard India's digital future. Building a secure and resilient cyber environment will be essential to protect sensitive information, critical infrastructure, and the overall digital economy of the country.

CREDIT

1. Press Information Bureau. "Ransomware Attack on AIIMS Delhi Systems." Accessed March 9, 2026. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1887282
2. CERT-In. "Advisory on Ransomware Attacks in Healthcare Sector." Accessed March 9, 2026. https://www.cert-in.org.in/PDF/CERT-In_Advisory_Ransomware_Healthcare.pdf
3. Ministry of Health and Family Welfare. "AIIMS Cyberattack Response Measures." Accessed March 9, 2026. https://main.mohfw.gov.in
4. The Hindu. "AIIMS Delhi Server Attack: What Happened." Accessed March 9, 2026. https://www.thehindu.com/sci-tech/technology/aiims-delhi-cyberattack-explained/article66230018.ece
5. Indian Council of Medical Research (ICMR). "ICMR Data Breach Incident Overview." Accessed March 9, 2026. https://www.icmr.gov.in
6. Economic Times. "ICMR Data of 81 Crore Indians Leaked on Dark Web." Accessed March 9, 2026. https://economictimes.indiatimes.com/tech/technology/icmr-data-breach-81-crore-records-leaked/articleshow/104239013.cms
7. Indian Express. "Massive ICMR Data Leak Explained." Accessed March 9, 2026. https://indianexpress.com/article/technology/tech-news-technology/icmr-data-breach-explained-8974312
8. Resecurity. "India Data Leak of 815 Million Records Analysis." Accessed March 9, 2026. https://www.resecurity.com/blog/article/india-data-leak-815-million-records
9. WazirX. "Security Incident Update." Accessed March 9, 2026. https://wazirx.com/blog/security-incident-update
10. CloudSEK. "WazirX Hack Detailed Analysis." Accessed March 9, 2026. https://www.cloudsek.com/blog/wazirx-hack-analysis
11. Halborn. "Cryptocurrency Exchange Security Assessment." Accessed March 9, 2026. https://halborn.com
12. Chainalysis. "Crypto Crime Report – Exchange Hacks." Accessed March 9, 2026. https://www.chainalysis.com/reports/crypto-crime-report
13. UIDAI. "Aadhaar Data Security Clarification." Accessed March 9, 2026.

https://uidai.gov.in/en/media-resources/press-releases
14. CyberPeace Foundation. "Aadhaar Data Exposure Research." Accessed March 9, 2026. https://www.cyberpeace.org/resources
15. Business Standard. "Aadhaar Data Leak Reports." Accessed March 9, 2026. https://www.business-standard.com/topic/aadhaar-data-leak
16. Data Security Council of India (DSCI). "Data Protection and Aadhaar Security Reports." Accessed March 9, 2026. https://www.dsci.in/content
17. Institute for Defence Studies and Analyses (IDSA). "Cyber Warfare and India Security Reports." Accessed March 9, 2026.
https://www.idsa.in
18. Recorded Future. "Cyber Threat Intelligence Reports." Accessed March 9, 2026. https://www.recordedfuture.com/research
19. CloudSEK. "India Threat Landscape Reports." Accessed March 9, 2026. https://www.cloudsek.com/threat-intelligence
20. Times of India. "Cybersecurity Threats in India Coverage." Accessed March 9, 2026. https://timesofindia.indiatimes.com/topic/cyber-attack
21. Seqrite. "India Cyber Threat Report 2026." Accessed March 9, 2026. https://www.seqrite.com/reports/india-cyber-threat-report-2026
22. Quick Heal Technologies. "Annual Cybersecurity Report." Accessed March 9, 2026. https://www.quickheal.com/reports
23. VarIndia. "Cyberattack Trends in India." Accessed March 9, 2026. https://www.varindia.com/news/cyberattack-india
24. India Cybersecurity Landscape. "Cyberattack Statistics India 2026." Accessed March 9, 2026. https://www.indusface.com/learning/cyber-security-statistics-india