International Journal of Engineering in Computer Science

E-ISSN: 2663-3590
P-ISSN: 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2024; 6(1): 145-149
Received: 18-02-2025
Accepted: 26-03-2025

Saurabh Kumar
Research Scholar, Department of Computer Science, Shri Khushal Das University, Hanumangarh, Rajasthan, India

Dr. Garima Bansal
Assistant Professor and Supervisor, Department of Computer Science
Shri Khushal Das University, Hanumangarh, Rajasthan, India

Corresponding Author:
Saurabh Kumar
Research Scholar, Department of Computer Science, Shri Khushal Das University, Hanumangarh, Rajasthan, India

Enhancing cybersecurity for the digital India program: A strategic approach

Saurabh Kumar and Garima Bansal

DOI: https://doi.org/10.33545/26633582.2025.v7.i1b.171

Abstract

The Digital India is the flagship IT programme of the Government of India and has the objective of catering to all the governance and non-governance related needs of a digitally empowered society for making it a knowledge economy. As a much-needed and speedily advancing sphere, digitalization also brought about efficiency, governance, and inclusiveness at the same time as it weakens the protection for several key critical infrastructures and personal data of citizens. New areas of human activity, such as in the fields of finance, healthcare, education, alongside civil administration, have strengthened the propensity to cyber-crimes and identity theft. This paper focuses on the current cybersecurity threats within the Digital India Programme to elucidate the existing challenges and underscores the latent vulnerabilities of the nation as it transits to the digital age contemporary and emerging threats and risks associated with the Digital India Programme are identified to include Untold digital infrastructures, low public cybersecurity consciousness, improper synchronised policy execution, and inadequate number of swift-response measures. It presents the current National Cyber Security Policy enacted in 2013 and initiatives made by the Computer Emergency Response Team in India (CERT-In) to address cyber threats as the primary technological approach commonly used in the region. Therefore, to tame the rising threats, the following measures are recommended: Implementation of Artificial Intelligence, Blockchain, and real-time threat intelligence systems; Establishment of a strong Legal regime; Developing the cybersecurity infrastructure across the country; Enhancing the PPP in the field of cybersecurity. Cybersecurity is an important aspect universally and has significant relevance in the context of India as it has to safeguard not only its security interests but also build up people's confidence and achieve the vision of Digital India or the sustainable growth targets of the nation. Integrating cybersecurity with the larger vision of digital transformation is needed to ensure that India becomes safe for the vulnerable population while promoting innovation and development.

Keywords: Cybersecurity, digital India, information security, cyber threats, data protection, national security, digital infrastructure

Introduction

The Digital India campaign was adopted by the Government of India in 2015 for creating a digitally empowered India along with a knowledge economy (Ministry of Electronics and Information Technology [MeitY], 2015) [21]. While seeking to improve the delivery of police services as well as other relevant services to citizens, it seeks to boost the utilisation of electronic media in the delivery of services to help narrow down the rural to urban disparity, among others. With services and people's interactions moving online, cybersecurity has become one of the most important issues.During Digital India, there has been an incredible improvement in internet-based governmental administration, e-payment, remote health, and educational facilities, making them more comfortable and convenient (Press Information Bureau, 2021) [24]. But this digitalisation has also opened doors for various threats in India's vital information assets like ransomware attacks, phishing incidents, data thefts, and state-affiliated cyber-spying (CERT-In, 2022) [4]. The analysis of current incidents suggests that cybersecurity attacks on both the government and private organisations are on the rise, thus requiring the implementation of proper measures (Indian Computer Emergency Response Team [CERT-In], 2022) [4]. While there is the existence of the current cybersecurity frameworks, such as the National Cyber Security Policy (2013) [20], these call for an upgrade to address modern threats (Ministry of Communications and Information Technology, 2013) [20]. Lack of coordination, insufficient human resources for cybersecurity affairs, and poor sensitization remain limiting factors to India's anti-cybercrime campaign.

Also, new technologies that are in the market today, like Artificial Intelligence, Internet of Things, and Block chain, need new terminology in security to adapt to the new systems (NITI Aayog, 2021) [23]. That is why, to develop the concept of cybersecurity within the framework of Digital India, it is necessary to strengthen the multi-vector approach at the technological, policy, personnel, and interdisciplinary levels. The enhancement of cybersecurity is not only"(Key, 2019) important for national security and economic wellbeing, but also a necessity to restore public confidence in the use of information technology services and decision-making. Incorporating proper security is useful because without it, India's and the broader goals of Digital India are still in jeopardy on the perilous sea of threats.

Objectives

1. To identify the critical cybersecurity vulnerabilities in India's digital infrastructure under the Digital India initiative.
2. To evaluate the effectiveness of existing cybersecurity policies and measures.
3. To propose a strategic, multi-layered cybersecurity framework combining technology, policy, and awareness initiatives.
4. To recommend collaborative models involving government, industry, and civil society for strengthening cybersecurity resilience.

Research Methodology

Consequently, this research seeks to use a qualitative and descriptive research approach to capture the cybersecurity challenges that exist under the Digital India initiative and come up with proposed frameworks to improve the cybersecurity posture in the country. The major data collection will be done through the use of secondary sources, whereby relevant data will be obtained from government publications, policies, articles and journals, records of cybersecurity incidents, other sources, and international benchmarking. Some of those sources are published by the CERT-In, Meit Y, NITI Aayog, and from various peer-reviewed journals specialising in cybersecurity and digital governance. The literature review provided the analysis of the existing cybersecurity policies to understand their strengths and weaknesses, the evaluation of the current gaps in the existing frameworks, and the investigation of innovative threats. This research was done by analysing the official documents to generate evidence on the changing nature of cyber threats and how India to counter them. An analytic comparison was made when the various papers were reviewed to develop possible changes that America could apply to India's socio-technical setting. Also, for the solution, the work adopted the synthesis approach to introduce a comprehensive cybersecurity model that involves technology (such as AI and block chain), policies, and awareness streams. Also, the review of the multi-stakeholder framework and an example on the focus of practically implementing it with the contributions of government, industries, and civil society in developing the best resilience was done.

Altogether, this approach provides clearer understanding of India's cybersecurity situation, as well as helps to provide the necessary guidelines to achieve the vision of a digitally secure society.

Strengthening India's cybersecurity under the digital India initiative

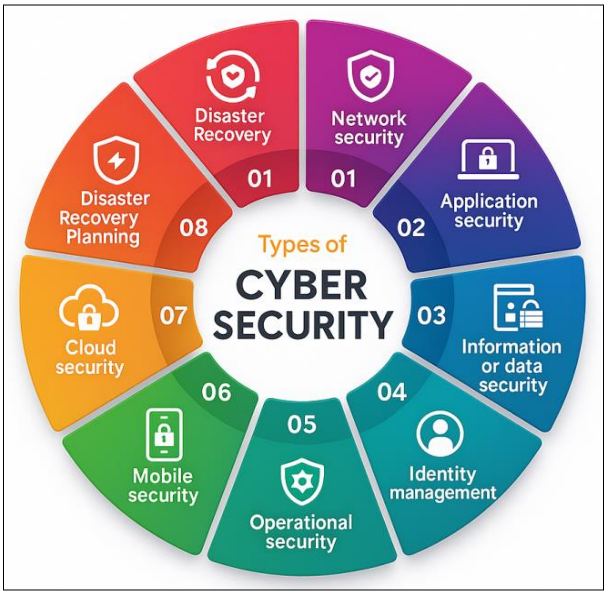
During the past few years, there has been increased connectivity through the use of the internet in India as the overall digital system begins to form, but the risks are also increasing afresh. Web applications of the government and public sector, online databases, payment gateways, and e-governance solutions are seen as increasingly accessible targets (CERT-In, 2023) [5]. Delinquent control of cybercrimes, piracy, outdated infrastructure, low observation on the provision of laws, and low sensitivity among the users are some of the challenges that hackers seize to conduct their activities such as phishing, ransomware, and data violations. Thus, the first element in this objective entails determining essential cybersecurity threats. This involves identifying risk surfaces like e-governance platforms, health care, and financial technology, which usually turn out to be the victims of cyber attacks (Gupta & Kumar, 2022) [13-14].

Secondly, the evaluation in the current framework gives an understanding of the preparedness of India. Particularly, applying it at the state level and, more specifically, enforcement, reaction, integration, and participant awareness (Ministry of Electronics and Information Technology, 2022). Studies on cyber audits accompanied by digital risk assessments revealed the fact that the cyber defence policies are far from having a coherent strategy, not only between the states but also between the agencies. This conceptualises a need to undertake a stock of the existing legal, regulatory, and operational frameworks. To meet these challenges, the third part of the stated objective is focused on the formulation of a strategic, multi-tiered framework for cybersecurity. The kind of framework that could contain such cyber threats should therefore be supported by the implementation of Artificial technologies like machine learning and block chain, policies, as well as public awareness campaigns at the community level. It should also be compatible with risk zones, including urban, rural, and critical infrastructure, and the layers of governance, such as local, state, and Central governance bodies (Sharma & Tiwari, 2021) [27]. Its emphasis is more or less on creating cybersecurity in the initial platforms rather than simply deploying it when there is something bad that has occurred. Finally, cybersecurity at the dawn of the digital age cannot be solely dictated by the government. Accordingly, it can be stated that the objective highly inclines toward collaborative models. It is for PPPs, cross-sector collaborations, and international collaborations to involve themselves and plug the technology aspects to make that sharing fit and relevant to enhance cyber hygiene. Civil society organisations are helpful when it comes to sensitization, particularly an illiteracy prevalent in rural areas. Therefore, for improving the protection for cyber threats in India following key models of relationship need to be set: academia-industry-government-citizen (Jain, 2023) [15-16].

The effectiveness of existing cybersecurity policies and measures.

India, being one of the world's leading digital economies, has undertaken several notable steps towards constructing a strong cybersecurity framework, especially given the widened digital implications owing to the 'Digital India' programme. Till now, the prominent institutions that deal with cyber threats are the Indian Computer Emergency Response Team (CERT-In), the National Critical Information Infrastructure Protection Centre (NCIIPC), and Cyber Swachhta Kendra. These bodies provide real-time alerts, carry threat estimation, and help in policy implementation in government as well as private networks (CERT-In, 2023) [5]. The primary legal recognition lies in the Information Technology (IT) Act 2000, which offers legal redressal against cybercrime, including hacking, theft of data, and identity theft (Chatterjee, 2020) [7]. The National Cyber Security Policy (NCSP) 2013 [20] was a significant measure towards building India's cybersecurity. It set goals, for instance, in raising awareness on cybersecurity, building defences, and collaboration between the public and private sectors in countering cyber threats. There are more specific policies on areas such as the rules issued by the Reserve Bank of India for financial institutions, banks, and cybersecurity measures of the Department of Telecommunications, data protection norms (RBI, 2022; DoT, 2021) [25, 10]. These have contributed to getting the major organisations to incorporate basic cybersecurity measures and engage in regular scans.

Types of Cyber Security: Key Areas of Protection



However, several gaps in the existing measures question their efficacy. The Social Engineering thread in the current NCSP is very limited because the NCSP 2013 [20] has not considered the new emerging threats like Cloud-based, Ransomware, AI/ML-enabled attacks, and quantum computing threats, etc (MeitY, 2022) [19]. However, at the time of writing this paper, India has not had a formally passed National Cybersecurity Strategy; the current version has been in draft form since 2020. This absence hinders the country's preparedness for immediate and coherent action, given the dynamic situation in cyberspace (Stephen & Mansfield, 2022).

Nonetheless, there is still significant concern about enforcement across sectors and at the state and local government levels. Most executive-level departments are still encountering a shortage of professional staff and Cyber audit systems, causing issues of delayed identification of threats and also weaker measures to combat the incident (Jain, 2023) [15-16]. Another challenge is the lack of awareness — a significant portion of the population is still susceptible to phishing, social engineering attacks, and mobile fraud, mainly due to the absence of information security literacy (Srivastava & Mehra, 2021) [28]. While the Indian government has put in place a basic cybersecurity policy framework, it is weak due to old policies, poor inter-agency cooperation, an inadequate number of personnel, and public ignorance of cybersecurity threats. More than the implementation of new national strategies and policies, cybersecurity capacity must be developed, as well as consciousness-raising campaigns performed, and the use of new technologies such as AI and blockchains should be brought to the scene for developing a robust cybersecurity posture. This indicates that despite the existing policy reforms, India's digital infrastructure continues to be at risk categorically.

A strategic, multi-layered cybersecurity framework combining technology, policy, and awareness initiatives

The Government of India's Digital India programme has given ample social and economic benefits to the country in this digital technology age. Nonetheless, the current advancement in digital media usage has also increased the level and level of cybercrimes. Thus, the conceptual framework of a single layer of protection does not seem sufficient to counteract this threat. Thus, the proposed goal is to devise a complex, integrated approach to cybersecurity that would be based on both technical, legal-political, and awareness activities. Such a framework is imperative to promote India's cyber defence, which is stringently crafted while also being firm, scalable, and sustainable in way in responding to future predicaments. The first precondition is the advancement and incorporation of technologies. Recent advancements like AI for threat detection, blockchain for secure transactions, and encryption for data protection are required to mitigate new forms of threats. AI helps in the identification of suspicious patterns and behaviour anomalies, hence can easily and quickly respond to the incident (Aithal, 2021) [1]. Likewise, through smart contracts, the Blockchain can provide irreversible and transparent transaction histories for the best use in instances such as securing public records as well as digital identities (Bhattacharya & Raj, 2022) [3].

The second layer relates to the formulation of security policies for enhanced protection of cyberspace and the formulation of sound regulatory measures. Although India has departments like CERT-In and laws like the Information Technology (IT) Act in place, these should be revised periodically to catch up with the development and newer dangers. Currently, there is a task to implement the National Cybersecurity Strategy that has been in discussion since 2020. This strategy should identify requirements for different actors, ensure compliance with data protection measures, and also report requirements on security plan checks with all government and critical infrastructure networks (Chakraborty, 2023) [6]. The third layer concerns awareness and training. In other cases, even advanced tools and policies will not assist in the enhancement of cybersecurity, since key measures may not directly involve, but address users of technology. Some of the preventive measures include awareness creation, cyber hygiene practices, and teachings, which are commenced at the school and university levels (Desai & Mehta, 2022) [11]. These populations should be accorded special consideration to check on the digital gap to alleviate vulnerability to cyber scams and fraud.

Recommending collaborative models for strengthening cybersecurity resilience

Today, because the working environment in organisations is highly digital, threats are more diverse, numerous, and intelligent. Singly, across organisations or governments, efforts in combating cyber threats are not adequate anymore, especially given the new and complex form that threats come in. One vulnerability can lead to severity with impacts on a nation, economies, and, let alone, the critical infrastructure sectors. Thus, there has been an increased focus on the need and the emergence of conglomerate approaches of government, industries, and civil society as core approaches of enhancing cybersecurity resilience (Shackelford, 2020) [26]. These are crucial in the formulation of an all-inclusive, pro-active, and adequately ill-equipped anti-malware framework that would encourage competent estimation and action against any possible threats.

Importance of Collaborative Models

Cyber attacks are cross-border in nature and blur the lines of sectors, including financial, healthcare, energy, and even public services. A single bank can cause the upset of national economies, a lack of trust from the public, and even social order. Likewise, the hacks in healthcare firms further warrant exposure of personal data, identity theft, and fraud. In this interrelated world, none of the actors can have all the prerequisites in terms of the equipment, skills, or authorization to tackle these threats (Kuerbis & Badiei, 2017) [18]. Collaborative models are important indeed because this way different people, who could have various experiences, knowledge, or skills, can share them and act together. Governments are inclined to provide legislative assistance and security experience, while industries possess technological advancement and organisation of infrastructure, civil society helps to not lose sight of citizen rights, transparency, and ethics. Altogether, these actors can set the body of works in an associative manner, creating a modern and multi-level protective structure that might respond to various threats and challenges at the national and societal level.

Role of the Government

It is therefore mandatory that the government be included as an originating party of any collaborative cybersecurity plan. One of them is to set up legal and regulatory frameworks that would lay down the norms and requirements concerning cybersecurity, reporting, and penalties for violation thereof. Furthermore, governments need to encourage secure ways through which information can be exchanged between the public and private sectors to disseminate threats in real time without jeopardising the security of a country or business competitiveness (Bada & Nurse, 2019) [2]. When engaging in PPPs, there is an opportunity for the government to harness the creativity of the private sector while keeping the state's control. For example, India's National Cyber Security Policy 2013 [20] mentions that PPPs should be developed for securing critical information infrastructure; other organisations, such as the Indian Computer Emergency Response Team (CERT-In), augment inter-sectoral responses to cyber threats. Moreover, the governments can venture into contributing to the advances in cybersecurity by funding key research institutes, providing grants for technology advancement, and supporting cybersecurity entrepreneurial firms. The opportunities for small business participation can be extended even further through other appealing, specific policy carrots: tax incentives for adoption of best practices and cybersecurity certifications, for example.

Role of Industry

Almost 95% of the world's critical cyberinfrastructure is held in the private domain, encompassing banking networks, telecommunications networks, healthcare facilities, and supply chains. Therefore, industries suffer the aggression of cyber criminals, making them play a more proactive part in both national and international security of cyberspace. Private sector organizations can contribute by standardizing cybersecurity protocols across industries, participating in joint threat intelligence-sharing initiatives, and collaborating with governments to draft sector-specific cybersecurity guidelines (Chertoff & Simon, 2015) [8]. Major technology firms like Microsoft, Google, and IBM have taken significant initiatives to collaborate globally on cybersecurity efforts, often sharing threat intelligence, offering cybersecurity services to vulnerable sectors, and advocating for international cyber norms. Such actions depict some ways that companies can protect not only their interests but also serve to bolster the defence of cyberspace at large.

SMEs also contribute a lot to the economy but they cannot afford to dedicate a lot of capital to spend on security. Industry driven models can close this gap by providing an environment in which organisational members can provide services at low costs, trainers to offer regular training, and other forms of support to smaller organisations to improve the security of the digital economy.

Role of Civil Society

Civil society is made up of other institutions including non-profit organisations, academics, advocacy groups, and individuals who are vigilant to ensure that the cybersecurity policies are progressive, liberal and respect human rights. Civil society organisations also play a critical role of protecting privacy rights, ensuring that everyone has an equal access to technology, and promoting the ethical use of the technology for any purposes that do not harm any individuals or groups (DeNardis, 2014) [9]. Some of the things that civil society organisations done include; More so, educational institutions have their roles in that they create awareness of new threats, work on technologies to prevent such threats, and prepare a talent that is ready to counter threats in the information sphere. Civil society also engages the public, sensitising people on risks, the available information on risks, and engaging communities especially those who are vulnerable in the society such as children, the elderly, and those in the rural areas.In addition, civil society organisations can be involved in the formulation of the policies and laws in issues of cybersecurity since such policies should be made in the open manner and in a democratic way. It enhances people's confidence in promoting cybersecurity and makes the society more resilient to cyber threats.

Conclusion

The Digital India is a planned framework for the country's socio-economic growth designed at eradicating digital divide and expending affirmative outcomes and actionable opportunities to the country's citizens. But as a nation it also gets exposed to increased cyber threats that compromise on the security of its infrastructure, individuals and security of the country. Thus, the weaknesses definable in the Indian digitisation profile have been expected, the shortcomings of existing protection policies have been evaluated, and the general and coordinated measures that can improve the country's cyber security have been described.

It has analyse that despite having effective frameworks National Cyber Security Policy (2013) [20] and operational body Computer Emergency Response Team-India (CERT-In), the cyber threat environment is now rapidly changing and therefore require update mechanism and need to integrate more effectively. When coupled with AI, blockchain and real-time threat intelligence systems, these policies are very effective along with other non-technical measures to propagate and advocate general awareness to the global population that cybersecurity cannot be addressed independently. There is need to develop a tripartite form of cooperative effort with government, industry, academia, and civil society involved. Governments must set the policies and facilitate an environment for industries while industries need to implement and safeguard their structures; the civil society has to ensure the promotion of standards and digital rights in addition to establishing awareness within their populace. This is the only way that India can ensure it's digital future As the ministry if information technology emphasises in the project dubbed Digital India, it is not a mere call for improving cyber security. When information security is embedded fundamentally in India's digital advancement, then it will not only safeguard the citizens and their resources but also help foster trust, lead to sustainable innovations and create a lasting economic growth.

References

1. Aithal PS. Role of Artificial Intelligence in National Cybersecurity Strategies. Journal of Emerging Technologies and Innovative Research. 2021;8(4):102-110.
2. Bada M, Nurse JRC. The social and psychological impact of cyberattacks. Oxford Research Encyclopedia of Criminology. 2019. https://doi.org/10.1093/acrefore/9780190264079.013.573
3. Bhattacharya A, Raj N. Leveraging Blockchain for Secure Digital Governance in India. Indian Journal of Technology and Public Policy. 2022;5(2):45-58.
4. CERT-In. Annual report: Cybersecurity incidents in India 2022. Indian Computer Emergency Response Team. 2022. Available from: https://www.cert-in.org.in
5. CERT-In. Annual Report on Cybersecurity Incidents in India. Ministry of Electronics and Information Technology. 2023. Available from: https://www.cert-in.org.in/
6. Chakraborty T. Challenges in Implementing India's National Cybersecurity Strategy. Cyber Law Review. 2023;11(1):78-94.
7. Chatterjee R. Legal challenges in India's cybersecurity framework. Indian Journal of Law and Technology. 2020;16(2):101-115.
8. Chertoff M, Simon T. The impact of the dark web on internet governance and cyber security. Global Commission on Internet Governance Paper Series. 2015.
9. DeNardis L. The global war for internet governance. Yale University Press. 2014.
10. Department of Telecommunications (DoT). Cybersecurity Directions for Telecom Service Providers. 2021. Available from: https://dot.gov.in
11. Desai M, Mehta V. Digital Literacy and Cyber Hygiene: A Study of Urban and Rural Users. International Journal of Digital Society. 2022;13(3):60-72.
12. Goyal R. Bridging the Skill Gap in India's Cybersecurity Workforce. Journal of Cybersecurity Training and Awareness. 2021;9(1):33-47.
13. Gupta A, Kumar V. Evaluating India's Cybersecurity Framework: Gaps and Recommendations. Journal of Information Security and Applications. 2022;67:103146.
14. Gupta R, Kumar A. Cybersecurity Challenges in India: A Policy Review. Journal of Digital Governance. 2022;9(3):45-58.
15. Jain M. Bridging the Cybersecurity Skill Gap in India: Need for Public-Private Collaboration. Cyber Policy Review. 2023;11(1):42-59.
16. Jain M. Building Cyber Resilience through Public-Private Partnerships in India. Indian Journal of Cyber Policy. 2023;12(1):77-89.
17. Kapoor A. A Risk-Based Approach to National Cybersecurity Planning. Journal of Information Risk and Cyber Strategy. 2023;6(1):22-39.
18. Kuerbis B, Badiei F. Mapping the cybersecurity landscape. Journal of Cyber Policy. 2017;2(1):26-44. https://doi.org/10.1080/23738871.2017.1299581
19. MeitY. Draft National Cyber Security Strategy 2021. Ministry of Electronics and Information Technology. 2022. Available from: https://www.meity.gov.in
20. Ministry of Communications and Information Technology. National Cyber Security Policy 2013. Government of India. 2013.
21. Ministry of Electronics and Information Technology (MeitY). Digital India Programme. 2015. Available from: https://www.digitalindia.gov.in
22. Nair S. Enhancing Real-time Threat Intelligence Sharing in India's Cyber Ecosystem. Cyber Defense Quarterly. 2022;4(2):50-65.
23. NITI Aayog. Harnessing Artificial Intelligence for Digital Transformation in India. Government of India. 2021.
24. Press Information Bureau. Digital India achievements report. 2021. Available from: https://pib.gov.in
25. Reserve Bank of India (RBI). Master Direction on Information Technology Framework for NBFCs. 2022. Available from: https://rbi.org.in
26. Shackelford SJ. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press. 2020.
27. Sharma D, Tiwari P. Multilayered Cybersecurity Framework for Smart Governance in India. International Journal of Information Security and Applications. 2021;63:102980.
28. Srivastava D, Mehra N. Cyber Hygiene and Public Awareness in India: A Rural-Urban Study. Asian Journal of Cyber Psychology. 2021;8(4):55-67.