GKU Journal of Multidisciplinary Research (GKUJMR)
ISSN: 3049 – 298X, Volume – II, Issue – I, April – 2026

Analysis of Digital Governance Implementation in Indian Organizations: Challenges and Strategic Solutions

Dr. Manpreet Singh Gill

Assistant Professor, Dept. of Computer Science, Akal Degree College, Mastuana Sahib, Punjab, India

Email ID: gillkotra@gmail.com

Accepted: 10.04.2026 Published: 30.04.2026 Page No. 27 – 38 DOI: 10.5281/zenodo.19909028

Abstract

India Organizations in India are shaken by the aspect of digital governance due to such immense initiatives as Digital India, as well as the National e-Governance Plan. This study plunges into the reality of challenges that the Indian organizations (publicly or privately owned) encounter in their lives. Having flipped through heaps of documentation and managed to monitors developments in policy changes, the study sets down the most significant challenges: poor infrastructure, lack of digital expertise, security risks, disorganized regulations, and lack of resources. The study does not only identify issues, but also provide evidence-based solutions, such as ramps in infrastructure with BharatNet, capacity-building with investments, the introduction of the Digital Personal Data Protection Act 2023, the simplification of regulations, and even a leap of new technologies such as AI and big data. The results do not merely remain theoretical. The study provides organizations with viable frameworks in which the things can become more transparent and accountable in addition to integrating global digital governance concepts into the Indian specific social and economic realities.

Keywords: Digital Governance, E-Governance, Digital India, Cybersecurity, Digital Literacy, BharatNet, DPDP Act 2023, AI Governance, Smart Cities Mission

1. Introduction

The fast growth rate of information and communication technologies (ICT) has essentially changed the paradigm of governance in the world, forcing. companies to redefine their business models, service products, and their relationship strategies with stakeholders [1]. The visionary national programs such as the National e-Governance Plan in 2006 and the overall Digital India Mission in 2015 have pioneered this digital transformation in India as both seek to use technology to promote transparency, efficiency, and accessibility in governance [2][3]. These programs symbolize the effort of India to make a shift towards the traditional.

bureaucratic systems into digitally-enabled systems of governance which are capable of dynamically responding to the needs of over 1.4 billion citizens.

Digital governance in the Indian context, is much more than digitizing the paper-based processes. It is a comprehensive strategy that combines policy frameworks, technological infrastructure, human capability, and regulations in the accomplishment of organizational goals and ensuring the principles of transparency, accountability, participatory decision-making, and legal compliance [4]. Digital governance is increasingly being perceived by modern Indian government departments, public sector undertakings, corporate entities in the country as well as non-governmental entities as a necessity not only in terms of operational efficiency but also in terms of organizational competitiveness in a globally intertwined economy [5].

The State of India Digital Economy Report 2024 states that India currently occupies the third place in terms of digitalization, as the digital economy has become 11.74% of national income in 2022-23 and is expected to increase almost to 20 percent of GDP by 2030 [6][7]. Such an impressive growth pattern has been supported by sensational increases in digital infrastructures. The number of internet users increased three times to over 970 million in 2024 as compared to 250 million in 2014, and the cost of data dropped to ₹9.34 per GB as compared to 308 per GB, making digital access more democratic [8].

Nevertheless, the way to full implementation of digital governance is still full of significant difficulties. These challenges are not limited to technical factors, which includes cultural resistance, capacity issues, regulatory ambiguity and socio-economic differences that exist in the diverse Indian terrain [9]. The urban-rural digital divide is a continuing illustration of such complexity as major urban centres have high connectivity and digital literacy, large rural areas are still grappling with poor infrastructure and lack of information [10]. By March 2025, BharatNet had service-enabled 2.18 lakh Gram Panchayats, but has not been able to ensure comprehensive last-mile connectivity [11].

Threat to cybersecurity is another critical issue to digital governance in India. In 2025, more than 265 million cyberattack attempts were witnessed in the country and an estimated financial loss in the country was above ₹20,000 crores [12]. Large-scale data breaches of organizations like BoAt (7.5 million users), BSNL (278 GB of data), and Hathway ISP (41.5 million customers) in 2024 demonstrate the uncertainty and high security risk of digital systems and the importance of effective security infrastructure [13]. In India, the cost of data breach on average increased 13 percent to 220 million rupees in 2025, highlighting the cost factor associated with poor cybersecurity efforts [14].

Digital regulations governing digital governance in India are dynamic but have not been unified yet. Another novel move is the Digital Personal Data Protection Act 2023, adopted by Parliament on August 11, 2023 that marks a significant success in providing extensive data protection frameworks [15]. Nonetheless, its application needs concerted effort on the part of various ministries and regulatory agencies, complicating the tasks of organizations trying to meet requirements on compliance [16]. Likewise, the India AI Governance Guidelines publishes in November 2025 by NITI Aayog set guidelines on responsible AI usage, but institutional processes to regulate its use continue to be operationalised [17].

The differences in infrastructure among regions have a major effect on the implementation of digital governance. Although the rural population is served by more than 400,000 Common Service Centres that bridge the digital divide [8], selective quality and poor broadband coverage, whereby only 37% of villages are linked up with reliable connections limits the delivery of the services [10].

The ambitious 1.5 crore high-speed Fiber-to-the-Home connections that BharatNet is set to implement in rural India have seen 11.74 lakh connections is positive and, however, achievements but also reflects the bespoke work left to do [18].

Another key challenge is human resource preparedness. Even after the huge digitalisation efforts, disparities in digital literacy levels among demographic groups are staggering, with rural populations, women and disparities in socio-economic groups exhibiting relatively high differences [19]. The fear of obsolescence or a lack of understanding of digital systems often is the root cause of employee resistance to technological change, which may hamper change efforts in both

the government and the marketplace [9]. The Smart Cities Mission, which was initiated in 2015 to design technology- based solutions to governance in 100 cities, is a good example of the opportunities and possibilities of digital governance in India [20]. They are the lighthouse cities that have been leading in the ways of integrated command and control centres, intelligent traffic management systems, and online grievance redressal mechanisms, but implementing such models in smaller cities and rural nations needs a major adjustment and investment [21]. It is in this context of both transformational opportunities and threats that this study uses a systematic approach to examine the nature of digital governance deployment in Indian organizations, the presence of major barriers, and the development of strategic remedies to fit within the Indian context. The paper will help to fill the gap between theoretical knowledge and practical implications of the problem by synthesizing recent academic sources, policy documents, and empirical data of current initiatives, which will in turn be applicable to the policy makers, organizational leaders, and other researchers working on enhancing the digital governance agenda in India.

2. Methodology

The study design is a qualitative literature review, which will be used to undertake an in-depth and systematic analysis of how Indian organizations have implemented digital governance. The study uses the combined sources of information provided by a variety of secondary sources like peer-reviewed academic journals, government policy documents, social reports by ministries and agencies, research publications, and contemporary analysis of digital governance projects since 2020 to 2026 [22].

This data gathering was specifically on Indian contexts and it used materials such as that of the ministry of Electronics and Information Technology (MeIT), NITI Aayog, the Unique Identification Authority of India (UIDAI), and the National e-Governance Division amongst others. The search keywords were based on the following: academic databases, digital governance India, challenges related to e-governance, Digital India implementation, cybersecurity in India organizations, smart cities governance frameworks.

They used thematic coding as the analytical method to remove common patterns, problems, and solutions to the same problem throughout the literature. Indian experiences were also compared with global best practices to place findings in digital governance wider context within the wider understanding of the digital governance scholarship. Special consideration was given to latest trends such as the Digital Personal Data Protection Act 2023, India AI Governance Guidelines 2025, and new data on BharatNet expansion, Aadhaar authentication and hacking [23]. This approach allowed an overall synthesis of the theoretical frameworks and application implementation experience, as well as a strong base of comprehending the dynamics of digital governance issues and solutions to the current Indian organizational environment. It is not denied that the use of secondary sources limits the sources, but the scope and the up-to-date nature of materials research makes this a limitation, as it guarantees the relevance and credibility of results.

3. Challenges in Implementing Digital

Indian Organization Governance.

3.1 Digital Divide and Infrastructure Inadequacies.

The most basic challenge to equal digital governance in India is the digital divide. Nevertheless, even at the current blistering pace, there is a growing connection between internet penetration of between 285 percent between 2014 and 2024 yet huge gaps still exist between urban and rural communities, socio-economically disadvantaged groups, and various geographic

locations [8]. Connection to the rural areas remains exceptionally poor, with only about 63 villages having productive broadband as of 2025 [10]. Its flagship rural connectivity programme, BharatNet has come a long way in bridging 2.18 lakh Gram Panchayats with the high-speed internet by March 2025 [11]. But the implementation of the programme has not been even across states and the quality of services differs significantly. The amended programme to offer 1.5 crore Fiber-to-the-Home connections needs an investment of 1.39 lakh crore, which shows the huge financial burden needed to undertake the enormous infrastructure generation [18]. Infrastructure issues are further exacerbated by network reliability and bandwidth limits. The connectivity in many rural and semi-urban places is intermittent and this means that organisations may not easily implement cloud-based digital governance systems that demand constant internet connectivity. Such inconsistency in technology acts against the confidence of the user, which curtails the viability of e- governance [9].

3.2 Cybersecurity Vulnerabilities and Data Protection Concerns.

Increased digitalization of India has rendered it one of the countries that have been targeted by cyberattacks worldwide. In 2025, a total of more than 265 million attempts to attack computers have been reported, and financial damages have been more than 20,000 crores [12]. The threat environment includes hospitals and educational institutions efforts against ransomware attacks, UPI and digital payment frauds resulting in monthly losses to the tune of thousands of crores of funds, and high-level phishing campaigns based on AI use [13].

In 2024, the security of even large institutions was revealed due to huge data breaches. The BoAT data breach resulted in the leak of personal data of 7.5 million users, and BSNL breach involved the leakage of sensitive data amounting to 278 GB of data including IMSI numbers, SIM card details, and so on [13]. In the case of 41.5 million customers hit in a breach by hackers against Hathway ISP, the hackers abused risks in the content management system owned by the company, which is based on Laravel [13]. In India, in 2025, the average cost of data breaches rose by 13 per cent to 220 million rupees, not only of direct financials, but also of reputation and loss of confidence of the population [14]. Large numbers of institutions or mostly small and medium enterprises and government departments with fewer budgets find it hard to establish full security lines such as encryption, multi- factor authentication, frequent security audits and incident response guidelines.

The Digital Personal Data Protection Act 2023 creates high standards of data fiduciaries which includes immediate breach informing the Data Protection Board and making users aware within 72 hours [15]. Nevertheless, most organizations do not have the technical abilities and procedures required in compliance, especially when it comes to consent management systems and data localization requirements. Maximum of 250 crore fines on security failures raises compliance pressure [24].

3.3 Poor Digital Literacy and Human Resource Capabilities.

Digital illiteracy has been a major obstacle to digital governance in India. Even though the governments have been trying to empower the general population with digital literacy skills including the Digital Saksharta Abhiyan (Digital Literacy Mission), large sections of the population, especially rural populace, older generations of the population, as well as socio-economically disadvantaged sections, are archaic in digital literacy [19]. This limits the demand side (citizens who do not have access into the digital services) as well as

the supply side (employees who cannot work with the digital systems efficiently).

Resistance to change in organizations is often a major issue that occurs in organizations. Digital systems can be perceived as a threat to the employment of employees who are used to working with traditional paper also due to their inability to work with digital gadgets and tools. This resistance reduces the adoption rates and require all-encompassing change management strategies that most organisations particularly in the public sector and that are difficult to enact effectively [9]. Literacy is also another problem that is enhanced by the gender digital gap. The rural rural women are experiencing the doubled disadvantage of reduced access to digital devices, cultural limitation to the use of technology, and reduced education level that poses a major challenge of inclusive digital governance [19]. Equally, linguistic diversity is a challenging issue- although most digital platforms are the ones that are becoming more accommodating of multilingual interfaces to accommodate the 22 scheduled languages of India, there is still little available in terms of content and user service in regional languages. The training programmes are usually lacking in scope, duration, and pedagogical practice. Several organisations have one-off training, which does not develop a lasting competency or in line with the never-ending transformation of digital systems. There is also a dearth of qualified trainers especially in rural areas which further limits capacity building e orts [10].

3.4. regulatory fragmentation and policy uncertainty.

Digital governance regulatory framework in India is poorly organized with different ministries, departments, and agencies generating problems relating to coordination and inconsistency in policies [25]. There is a lack of clear jurisdiction in digital governance, with overlapping roles by the Ministry of Electronics and Information Technology, Ministry of Communications, NITI Aayog, and state governments on various aspects of digital governance, creating a complex bureaucracy. Policy uncertainty has an implication on the strategic planning and investment. Although the Digital Personal Data Protection Act 2023 offers a comprehensive framework, specific rules were only announced in November 2025, which caused a lengthy ambiguity period when it comes to actual compliance requirements [26]. Equally, the India AI Governance Guidelines outdated in November 2025 assert principles, but they need institutional structures, including the suggested inter-ministerial AI Governance Group to be in full effect [17].

States have taken different governance forms of digital governance building inconsistencies in the implementation standards and interoperability issues. The e-governance platforms that are designed by individual states are usually not compatible with national systems and therefore they require entry of the data more than once and this generates inefficiency [9].

To harmonise these various systems, technical standardisation, and political consensus may be hard to realise in the federal Indian system.

The procurement policies and tendering of digital technologies are in most cases biased towards lowest bidding instead of quality or long-time value. This may lead to deployment of non-optimal systems that may need regular replacement, or extensive customisation, leading to the overall higher cost of ownership and providing poor user experiences [21].

3.5 Financial Constrains and resource allocation.

The process of rolling out end-to-end digital governance systems is time and money consuming in terms of infrastructure, software licensing, cybersecurity, and training initiative, as

well as long-term maintenance. Small organisations and many government departments have budgetary limitations which restrict their potential to invest in digital transformation sufficiently [9].

Initial cost of digital infrastructure such as servers, networking, security, and specialized software can be restrictive, especially when used by a state and local government organization with constrained fiscal independence. These operations costs such as maintenance of the system, software upgrades, subscriptions to cloud services and cybersecurity are the continued predetermined financial obligations that must be maintained over time [10].

Digital governance initiatives can also be a hard perspective on calculating a return on investment, especially where the outcome is a qualitative benefit like a better transparency rating, citizen satisfaction, or better accountability. This complicates the allocation of budget to the competition with other urgent needs like healthcare, education, or infrastructure development [4].

There are also specific funding constraints of rural and tier-2/tier-3 city organizations, as they are not able to access the same revenue bases or defer to the same central government funding as metropolitan areas. This contributes to the urban-rural digital divide and increases the differences of service quality in various regions [19].

3.6 System Integration and Interoperability Problems.

Lots of organizations in India use legacy systems that have been developed at various times and with different types of technology making integration difficult. Siloed applications and databases thwart smooth flow of data, which involves entering the data manually in numerous systems and this generates an inefficiency and rate of errors [9].

Interoperability between departments, levels of administration of a given government is hampered by lack of standardisation in data formats, API protocols and technical architectures. Integration failures make visible to citizens-facing services that involve coordinating services of multiple agencies, like business registration, which involves municipal corporations, state commercial tax agencies and central government registrars, needlessly complicated [4].

Lack of long-term strategies to integrate technology into an organization means that most organizations are adopting technology ad hoc without strategic enterprise architecture provisions. This technical debt has a temporal build-up, resulting in more and more challenging and costly e orts in subsequent integration [21].

Another challenge of integration is Vendor lock-in. E orts to work in proprietary systems with certain vendors of technology can impose dependencies that restrict exibility, raise costs and make it more difficult to work towards open standards or migrate to other platform choices [9].

3.7 Organizational Culture and Change Management.

The main obstacle to the implementation of digital governance is the traditional hierarchical ways of organization that many Indian public sector entities have adopted. The appearance of digital systems can often add transparency and standardization of processes that interfere with traditional power relationships and informal relationships, provoking opposition on the part of stakeholders beneficiency of status quo arrangements [9].

Organizational cultures, which are risk-averse, do not encourage experimentation and innovation, both of which must occur with successful digital transformation. The fear of failures, responsibility issues and red tape

bureaucracy can freeze the decision-making process and digital initiatives may languish in lengthy procedures of approval [10].

Poor change management culture exacerbates cultural problems. Organisations often center their attentions on the technologies implementation and they overlook human aspects viz. communication, stakeholder engagement, incentive alignment and psychological support that are critical towards success in adoption [22].

Leadership commitment is a major success factor in digital governance and most firms are devoid of champions at the top leadership positions who are knowledgeable in the digital technologies and can lead agendas to achieve transformation. In the absence of visible leadership, digital efforts find it difficult to mobilize the needed resources and have a way through bureaucratic hurdles [4].

4. Strategic Solutions for Strengthening Digital Governance

4.1 Expansion of infrastructure and improvement of network reliability.

The implementation of BharatNet needs to be a national agenda, and efforts to meet the aim of reaching 100 percent Gram Panchayats and delivering 1.5 crore FTTH connections in rural regions [18] should be given priority. This entails high efficiency in project execution, improved coordination among both BSNL and the state governments and performance check systems to guarantee quality. Connectivity in geographically remote or challenging terrain locations where can be tackled by leveraging satellite internet technologies. fiber installation cannot be economically viable. Recent developments in the low- earth orbit satellite, satellite constellations can provide options other than in bridging the last-mile connectivity gaps [10].

Public-private partnerships could mobilise the expertise and capital of the private sector to develop infrastructure and make sure that mandates of covering the whole population are fulfilled. Provisions like the revenue sharing scheme or state subsidies of the rural deployments can render commercially marginal areas a lure to the private telecommunications producers [11].

The use of quality-of-service standards and monitoring mechanisms will make sure that connectivity where offered, has bandwidth and reliability below the minimum required to support digital governance in good practice. Penalty provisions on non-compliance and regular audits drive the service providers to uphold the quality of infrastructure [9].

4.2 Full enforcement of the Cybersecurity Framework.

Companies should implement global security audits including ISO 27001 on information security management systems that sets out methodology on how to locate, evaluate, and reduce information security risks [9]. Periodic third-party security audits can help independently validate security postures and identify potential vulnerabilities before exploitation.

The comprehensive adoption of the requirements of the Digital Personal Data Protection Act 2023 will help to secure information about citizens and instill trust in citizens in digital governance systems [15]. This involves ensuring that there is a clear consent process, data minimization processes, purpose limitation process and a strong breach notification process [26].

The development and maintenance of internal cybersecurity capacities by establishing Chief Information Security Officer positions, security operations centres and specialized security teams are necessary to make sure that organisations can quickly react to any new threats [12]. All employee cybersecurity training covers the human factor, which is the weakest aspect of most security breaches [13].

This implies that implementing a zero-trust security architecture, multi-factor authentication, data-at-rest/data-in-transit encryption, and active or passive monitoring systems delivers defence-in-depth against advanced attack vectors [24]. Business continuity plans and incident response plans ensure organisations are operating in critical functions even when security breaches take place.

4.3. Capacity Building and Digital Literacy Programmes.

To scale the Digital Saksharta Abhiyan and such other programs to realize universal digital literacy, specialized programmes with target demographics such as women, the elderly citizens, rural and underprivileged communities are needed [19]. Support learning materials and content: Multilingual training materials and content that support the 22 scheduled languages in India make it inclusive.

In organisations, it is the aim of creating structured training curricula progressing between the ease of digital literacy to technical skills that will allow employees to build up capabilities with time. Practice with real systems, digitally-paired mentoring programmes capable individuals with students and acquisition of secure spaces to experiment help learning to fasten [10].

Collaborating with schools, non-governmental and training organizations as well as individual training providers taps the knowledge and channels of delivery. We can offer scaled access through online learning platforms and workshops that cover the hands-on skills development requirements, in person [22].

Organic knowledge transfer can be achieved through creating digital champions networks in organizations, such as employees who are skillful and demonstrate their interest in digital tools and can support each other in order to create internal capacity in a sustainable manner [9].

Rewarding the development of digital skills by providing opportunities to advance the career or financial incentives or even public recognition is an incentive to engage in such activities and is a sign that an organisation is willing to transform into a digital entity [4].

4.4 Policy Clarity and Regulatory harmonisation.

To mitigate regulatory fragmentation, establishment of inter-ministerial coordination mechanisms like the proposed AI Governance Group [17] will help to provide uniform policy implementation across agencies. Evidence based policymaking is informed by regular stakeholder consultations with industry, civil society, and academic experts [25].

Creating detailed national guidelines on emerging technologies such as artificial intelligence, block chain, Internet of Things in such a way that it gives the organizations a clear direction on responsible usage and encourages innovation [30]. The India AI Governance Guidelines are a significant step, though need specific sectoral implementation road maps [17]. Adopting open standards and interoperability protocols by government regulation enables integration of systems between organizations and aversion of vendor lock-in [9]. India Enterprise architecture framework is a platform, which needs to be more extensively adopted and enforced [4].

Making procurement processes more streamlined with the focus on the total cost of ownership, quality, security, and long-term value over the focus on upfront costs only promotes the investment in durable digital governance solutions [21]. Procurement can be fastened by framework contracts and em Paneling of qualified vendors.

4.5 In innovative financing Models and Resource Optimisation.on

Creating special digital transformation funds at federal and state level will be long-term funds that support long-term plans that are not tied to annual cycle of budgets [10]. Such funds may be used in infrastructure investments as well as the recurrent expenses like training and maintenance.

The use of government e-Marketplace (GeM) platform in the procurement of digital technology can save on expense by buying in bulk, competing on price and specifications that are consistent [8]. Analytical tools of GeM assist organisations in price benchmarking and finding cost effective solutions.

The use of cloud- first policies allows organisations to transition to operations spending models rather than capital intensive models of infrastructure ownership with less upfront cost, and with scalability [9]. MeghRaj is a shared government cloud providing secure yet inexpensive hosting of e-governance applications [4].

Parntership activities and corporate social responsibilities can complement the government funding especially in projects that target the rural and underprivileged regions [11]. Digital inclusion is becoming an established goal by technology companies in the following aspects of social responsibility as well as market development:

4.6 Advanced Technology Integration

Digital governance can be improved with the help of artificial intelligence and machine learning applications, such as automated service delivery, predictive analytics, chatbots that provide answers to citizen concerns, and anomaly recognition in order to prevent fraud [17]. The India AI Mission offers guidelines and tools towards responsible AI uptake [30].

By being able to identify patterns in large datasets that are sourced by various topics such as social media, transaction records, sensor networks allow the provision of information on the needs of citizens and programme success [9]. Nonetheless, analytics should be accompanied by fierce privacy rights as required by the DPDP Act 2023 [15].

The promise of blockchain technology includes tamper resistant record management, transparent supply chains and security when authenticating credentials. The implementation of blockchain in government issues based on pilot projects in the land records management area as well as education credential verification show that blockchain can be effectively applied to the problems of governance [22].

Smart cities made through the implementation of Internet of Things allow real-time tracking of infrastructure such as traffic flow, air quality, water supply, waste management, which helps to promptly respond and allocate resources more optimally [20]. Nonetheless, IoT security vulnerabilities need special consideration to avoid making devices an attack point [12].

4.7 Improving Organisational Culture and Change Management.

To ensure observable executive support using executive champions with a clear view of transformation and understanding digital technologies, offers the needed propulsion of change in the organization [4]. Leadership communication on a regular basis that focuses on digital priorities is a positive indication of organizational commitment.

Installing systematic change management systems such as stakeholder analysis, communication plans, training programmemes, resistance management strategies and feedback systems that are responsive to the human aspects of digital transformation [22]. Staged deployment gives the opportunity to adjust and shows rapid wins which generate trust [9].

Promoting organizational cultures of experimentation and innovation via special innovation laboratories, hackathons and funding

pilot projects can lead to creative problem solving and to decreased fear of failure [10]. Publically celebrating success and using failures as a learning experience creates psychological safety to innovation.

By redesigning performance management systems to pay to go digital, collaborate and deliver services in a way that is citizen-oriented, the individual incentivals is congruent with the organizational goals of digital governance [4]. This can be in terms of digital service adoption rate, score of citizen satisfaction, or increase in process efficiency.

5. Conclusion

The deployment of digital governance in Indian organizations is a multifaceted tapestry of issues, which have existed on technological, human, regulatory, and financial levels. Infrastructure includes urban and rural areas, and risks to cybersecurity place millions of users at risk of data breaches, issues in digital literacy hold back citizens and employees, regulatory fragmentation among multiple agencies, and available resources limits holistic investments all contribute to the burden of the implementation of the Indian digital governance vision.

Nevertheless, such daunting obstacles are overcome with an integrated, situation-specific plans. Increasing BharatNet coverage to 100% rural connectedness, thoroughly adopting the Digital Personal Data Protection Act 2023 to foster trust, and capacity building programmes to realise inclusive digital literacy, harmonisation of regulatory frameworks across ministries and states, and the development of new models of financing long-term investments are pillars to success.

The combination of innovative technologies, such as artificial intelligence regulated through the recently published India AI Governance Guidelines, big data analytics to make evidence-based decisions, blockchain to store the records transparently, and IoT to control the work of the smart city have transformative potential when supplemented with adequate security policies and ethical governance principles.

Cultural change in organizations is also important. Digital governance is not only effective with the use of technology but can be successful with the application of fundamental changes in the mindsets processes, responsibility, and relationships with the stakeholders. The key enablers include leadership commitment, systemic change management, organizational cultures that embrace transparency, experimentation, and citizen-centricity.

India the digital governance has made impressive achievements with 970 million internet users, 1.38 billion Aadhaar numbers issued containing 9.6 crore daily authentications, UPI processing over 100 billion transactions yearly and the digital economy is expected to contribute 20% of GDP by 2030 [6][7][8][28]. Such accomplishments reflect the groundbreaking capabilities of digital governance and pinpoint the magnitude of the work still to be done.

The way forward should involve a long-term commitment of government both at the state and local level, involvement of the private sector in provision of technology, involvement of the civil society groups representing the interests of citizens and the agency of the citizen as the active end users that can create a digital governance system. Not only the level of technological sophistication will be viewed as a measure of success, but will also be the degree to which digital governance fulfils its core functions, which include transparency in decisions governing its operations, accountability of elected leaders, efficiency in using available resources, and provision of services to all citizens without

geographical, language, and socio-economic boundaries.

With India still on its way to becoming one of the most digital economies and societies, digital governance will be both an enabler and a measure of success. The problems found out in this study are huge but not unfeasible. The solutions described will contain practical guidelines that can be used by organisations aiming at navigating this convoluted landscape. Future studies need to concentrate on longitudinal studies of implementation results, cross-state and cross-sector comparison, and the new challenges presented by new-generation technologies. India utilises evidence-based policymaking, sustained investments, inclusive capacity building, and adaptive governance frameworks to achieve the full potential of digital governance as a strategic national development and global competitiveness resource.

References

[1] Z. T. Rony, F. A. Alijoyo, and F. Surfaifel, "Analysis of digital governance implementation in modern organisations: Challenges and solutions," MORFAI Journal, vol. 5, no. 3, pp. 5399-5405, Sep. 2025. [Online]. Available: https://doi.org/10.54443/morfai.v5i3.4140

[2] "E-Governance in India: Bene ts & Challenges," PMF IAS, May 27, 2025. [Online]. Available: https://www.pm as.com/e-governance-in-in dia/

[3] "Challenges and Opportunities of E-Governance in India," Sanskaram University, 2025. [Online]. Available: https://sanskaramuniversity.ac.in/challenges-and-opportunities-of-e-governance-in-india

[4] R. E. Indrajit, Electronic Government: Strategi Pembangunan dan Pengembangan Sistem Pelayanan Publik Berbasis Teknologi Digital. Yogyakarta, Indonesia: Andi, 2004.

[5] E. Barrow, "The role of digital infrastructure in e ective governance: Lessons from developing countries," Journal of Public Sector Innovation, 2024.

[6] "Digital India Mission, About, Approach, Methodology," Vajira Mandravi IAS, Feb. 18, 2026. [Online]. Available: https://vajiramandravi.com/current-a airs/digital-india-mission/

[7] "Digital India Mission," Vision IAS Current A airs, Aug. 18, 2025. [Online]. Available: https://visionias.in/current-a airs/monthly-magazine/2025-08-19/economy/digital-india-mission

[8] "10 Years of Digital India Mission," Drishti IAS, Jul. 1, 2025. [Online]. Available: https://www.drishtiias.com/daily-updates/daily-ne ws-editorials/10-years-of-digital-india-mission

[9] D. Permana, "Overcoming challenges in e-Government implementation in Papua," Parlementer Journal, 2023.

[10] "Challenges to Digital Governance in Rural India," Journal of Accounting and Finance Research, Dec. 11, 2025. [Online]. Available: https://rjwave.org/jaafr/papers/JAAFR2512198.pdf

[11] "Bridging Urban-Rural Digital Divide: BharatNet makes 2.18 lakh GPs service-ready," Economic Times Government, Apr. 21, 2025. [Online]. Available: https://government.economictimes.indiatimes.com/

[12] "Cybersecurity Threats Statistics 2025 and Government of India," Prime Infoserv, Dec. 29, 2025. [Online]. Available: https://primeinfoserv.com/cyber-security-statistics-2025-global-facts-major-breaches-and- indias-rising-cyber-risk/

[13] "Biggest Cyber Incidents of 2024 & What We Learned in 2025," ISACA Mumbai, Sep. 23, 2025. [Online]. Available: https://www.isacamumbai.org/blogs/cyber-incidents-2024-learnings-in-2025 Digital India Mission, Vision IAS, 2025.

[14] "Government noti es DPDP Rules to empower citizens," Press Information Bureau, Nov. 19, 2025. [Online]. Available: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014

[15] "India's Digital Personal Data Protection Act 2023 Brought Cybersecurity to Board-Level," Prime Infoserv, Jan. 14, 2026. [Online]. Available: https://primeinfoserv.com/indias-digital-personal-data-prot ection-act-2023-cybersecurity-board-level/

[16] "India AI Governance Guidelines 2025 - Towards Safe," Vajira Mandravi, Nov. 10, 2025. [Online]. Available: https://vajiramandravi.com/current-airs/india-ai-governance-guidelines-2025/

[17] "BharatNet Achieves 11.74 Lakh FTTH Connections in Rural India," BharatNet, Dec. 20, 2024. [Online]. Available: https://bharatnet.

in/bharatnet-achieves-11-74-lakh-ftth-connections-in-rural-india/
[18] N. Noordiyati, "Implications of digital government for public sector accountability," Advances in Accounting and Research, 2025.
[19] M. Schermann, H. Bast, and C. Feilmayr, "Digitalization as a challenge for public governance: A con gurational approach," Government Information Quarterly, 2023. [Online]. Available: https://doi.org/10.1016/j.giq.2023.101724
[20] "IT Law Framework Governing India's Smart Cities Mission," KS&K, Jan. 19, 2026. [Online]. Available: https://ksandk.com/informati on-technology/it-law-framework-indias-smart-cities-mission/
[21] A. Bolderston, "Writing an e ective literature review," Journal of Medical Imaging and Radiation Sciences, vol. 39, pp. 71-76, 2008.
[22] E. Eliyah and A. Aslan, "Stakes evaluation model: Metode penelitian," in Presiding Seminar Nasional Indonesia, vol. 32, 2025.
[23] "An Overview of India's Digital Personal Data Protection Act," UpGuard, Sep. 7, 2023. [Online]. Available: https://www.upguard.com/blog/dpdp-2023
[24] "Digital Governance in India: Challenges, Opportunities," Dhyeya IAS, Nov. 8, 2025. [Online]. Available: https://www.dhyeyaias.com/daily-current-affairs/digital-governance-india-challenges-opportunities-re commendations
[25] "India AI Governance Guidelines | 07 November, 2025," Sansad TV, Nov. 7, 2025. [Online]. Available: https://sansadtv.nic.in/episode/perspective-india-ai-governance-guidelines-07-november-2025
[26] "Decoding Digitalization of Urban Governance in India," Centre for Policy Research, Jan. 16, 2023. [Online]. Available: https://cprindia.org/briefsreports/
[27] "Annual Report 2024-25," Unique Identi cation Authority of India, 2025. [Online]. Available: https://uidai.gov.in/images/E_UIDAI_Annual_Report_24-25.pdf
[28] "Aadhaar: A Global Benchmark in Digital Identity and Governance," OpenGov Asia, Oct. 25, 2024. [Online]. Available: https://archive.opengovasia.com/2024/10/26/aadhaar-a-global-benchmark-in-digital-identity-and-governance/
[29] "India AI Governance Guidelines," Vision IAS Current A airs, Dec. 22, 2025. [Online]. Available: https://visionias.in/current-affairs/monthly-magazine/2025-12-23/polity-and-governance/india-ai-governanc-guidelines