JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Hygiene and Capacity Building in Indian Bureaucracy: Lessons from Aadhaar and CoWIN

Archana MS ; Fathima Nitha PT ; Smera BR ; Meenakshi VV ; Devanandha. S

Post Graduate Students in Integrated MA Politics and International Relations,Govt.Arts &Science College,Tavanur,University of Calicut

Abstract

By integrating biometric identification and pandemic-related platforms into routine administration, India's increasing reliance on digital infrastructures has revolutionized governance. Although efficiency is promised by these innovations, they have also revealed serious flaws in bureaucratic readiness, especially with regard to institutional resilience and cyber hygiene. Through the experiences of Aadhaar data leaks and cyber incidents related to the CoWIN vaccination platform, this study investigates these problems.Drawing on legal developments, policy frameworks, and documented lapses, the paper demonstrates how security is compromised by fragmented practices, inadequate accountability, and inadequate training. Reforms like the Digital Personal Data Protection Act (2023) and CERT-In's guidelines are a step in the right direction, but they won't be enough unless cyber hygiene is integrated into administrative procedures.The report makes the case for a capacity-building agenda that emphasizes ongoing training, open reporting of security breaches, and fostering citizen trust. By placing these issues in a democratic framework, it comes to the conclusion that maintaining cyber hygiene is a constitutional obligation to protect the legitimacy of digital governance, not just a technical solution.

Keywords: cyber hygiene, Indian bureaucracy, Aadhaar, CoWIN, digital state, data security, capacity building

Introduction

India has become one of the most aggressive adopters of digital governance in the past 20 years. The goal of flagship initiatives like Digital India is to use technology to increase inclusivity, guarantee transparency, and expedite the delivery of public services. Milestones in this journey include platforms like CoWIN, which became essential during the COVID-19 vaccination drive, and Aadhaar, the largest biometric identity system in the world.However, there are risks associated with relying on digital infrastructures. Weak cyber protocols, system abuse, and data breaches put millions of citizens at risk. In this situation, the idea of cyber hygiene—the routine digital behaviors that guard against compromise—becomes essential. Cyber hygiene, in contrast to more general cybersecurity frameworks, emphasizes practices like software updates, access security, and reporting irregularities. Errors in these procedures erode public trust in the government as well as the systems in bureaucracies that handle private citizen data.

Two significant cases—repeated Aadhaar data leaks and cyber incidents involving CoWIN—are used in this paper to examine these problems. Both demonstrate how India's digital governance is impacted by deficiencies in bureaucratic training, readiness, and disclosure. Conceptual clarifications are the first step in the analysis, which is then followed by case studies, regulatory reactions, and recommendations for enhancing bureaucratic capability.

Conceptual Foundations

Cyber Hygiene

Cyber hygiene refers to consistent and disciplined practices that lower the risks of digital compromise, much like personal health routines (Bada & Sasse, 2015). Multi-factor authentication, stringent user access guidelines, phishing awareness, patch updates, and required incident reporting are all examples of this in state institutions. Raising awareness is just as crucial as creating secure infrastructure because breaches are frequently the result of human error.

Bureaucratic Capacity

The ability of an institution to adjust and react appropriately is referred to as capacity building. This suggests that bureaucracies in digital governance need to advance not only their technical expertise but also their understanding of policies, their ability to adjust to new threats, and their adherence to regulations. However, in India, officials are ill-equipped to handle complex cyber challenges because bureaucratic training has historically placed a higher priority on legal procedure than digital literacy.

Cybersecurity and Legitimacy

In the digital age, data protection is essential to state legitimacy. With the expectation of security, citizens exchange personal information for welfare benefits. Trust is damaged by breaches, and the repercussions can be disastrous for vulnerable groups that rely on Aadhaar and similar systems for subsidies (Rao, 2019). Cyber hygiene thus becomes a democratic duty as well as a technical defense.

Cyber Hygiene in Indian Bureaucracy

Even though India established a number of nodal agencies, including MeitY, CERT-In, UIDAI, and MoHFW, there are still gaps in the country's bureaucratic practices. Three persistent flaws are evident:

1. Training Deficit: Capacity is frequently outsourced, and few officials receive formal cybersecurity training.

2. Compliance Over Awareness: Rather than being regarded as developed habits, protocols are viewed as checklist exercises.

3.Opaque Reporting: Institutional learning is limited because breaches are rarely revealed in full.

Examining these shortcomings through the experiences of Aadhaar and CoWIN makes them more apparent.

Case Study I: Aadhaar

With over a billion registrations since its launch in 2009, Aadhaar is essential for financial access and welfare delivery. But it has experienced breaches on numerous occasions.The Tribune reported in 2018 that middlemen were charging ₹500 for Aadhaar access. Due to inadequate redaction procedures, state-level agencies had previously unintentionally posted citizen data on public portals. Virtual IDs and other fixes introduced by UIDAI were reactive measures. The underlying issue of officials' and contractors' inadequate security awareness has not been addressed.Any biometric identifier leak carries lifelong risks, such as identity theft and social security system exclusion, because biometric identifiers are permanent. Therefore, Aadhaar serves as an example of how poor bureaucratic hygiene can jeopardize systemic credibility as well as individual rights.

Case Study II: CoWIN

With billions of health records handled, the CoWIN platform proved indispensable during India's vaccination campaign. There were rumors in 2023 that a Telegram bot could access personal information related to vaccinations. The government acknowledged that some state-level APIs might have been abused, despite rejecting allegations of a "major breach" (PIB, 2023).

Two main problems were identified in the CoWIN episode:

- Coordination between state-level cyber practices and central safeguards is lacking.
- unwillingness to openly reveal violations, which damaged confidence.

CoWIN revealed communication and cultural flaws, especially denial and secrecy in official responses, in contrast to Aadhaar, which had structural vulnerabilities.

Legal and Regulatory Landscape

The Information Technology Act (2000) is the first piece of regulation in India. While the Supreme Court acknowledged privacy as a fundamental right in its historic decision in Justice K.S. Puttaswamy v. Union of India (2017), the Aadhaar Act (2016) added protections for biometric data.More recently, government agencies and other data fiduciaries have been subject to more stringent requirements under the Digital Personal Data Protection Act (2023). It requires data minimization, explicit consent, and purpose limitation.

However, its potential is diminished by the extensive exemptions given to state agencies.Although CERT-In's 2022 guidelines requiring six-hour breach reporting and log retention are noteworthy, institutional capacity issues make compliance difficult.Therefore, even though India has a legal system, its efficacy is dependent on everyday procedures and bureaucratic abilities.

Capacity Building for Resilience

For digital governance to continue to be reliable, bureaucratic reform needs to concentrate on:

- Integration of Training: Cyber hygiene courses ought to be required in all administrative schools.
- Digital Competency in HR: Digital literacy must be considered a fundamental skill in hiring and advancement.
- Cross-Sectoral Collaboration: Collaborations with private specialists and civil society can improve oversight.
- Transparency: Normalizing breach disclosure promotes institutional learning and increases public trust.

Trust, Transparency, and Governance

In digital systems, citizen trust is brittle. Aadhaar and CoWIN demonstrate that trust is reliant on both robust platforms and sincere reactions to failures. Credibility is harmed more by denials and secrecy than by actual breaches.

Globally, public accountability and prompt disclosure are emphasized in best practices. Instead, India's propensity to put reputational management first threatens democracy. Crucially, vulnerable groups bear a disproportionate amount of the consequences, which renders promises of inclusion vacuous.

Conclusion

India's digital transformation has increased risks while simultaneously creating opportunities for effective governance. Developing cyber hygiene as a bureaucratic culture is the main obstacle, not just laws or technology.The Aadhaar and CoWIN incidents demonstrate that regular vigilance and transparency cannot be replaced by regulatory reforms such as the DPDP Act or CERT-In guidelines. Important first steps include developing open communication, integrating digital literacy, and bolstering bureaucratic capacity.In the end, preserving digital governance involves defending democratic legitimacy in addition to averting cyberattacks. Therefore, in a digital democracy, cyber hygiene must be acknowledged as a constitutional obligation of the state.

References

Grindle, M. S. (1997). Getting good government: Capacity building in the public sector of developing countries. Harvard University Press.

Chand, V. (2017). Public administration in the information age: Governance and technology in India. Oxford University Press.

Singh, J. P. (2019). Digital governance: Technology and public sector reform in developing countries. Routledge.

West, D. M. (2005). Digital government: Technology and public sector performance. Princeton University Press.

Bada, A., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? International Journal of Human-Computer Studies, 88(1), 51–66. https://doi.org/10.1016/j.ijhcs.2015.02.009

Rao, U. (2019). Biometric citizenship: Aadhaar, exclusion, and the politics of recognition. South Asia: Journal of South Asian Studies, 42(3), 482–497. https://doi.org/10.1080/00856401.2019.1651507

Ramanathan, U. (2019). A flawed design: Aadhaar as a case study of surveillance and exclusion. Indian Journal of Human Rights Law Review, 10(2), 45–67.

Ramanathan, U. (2023). Data protection and state exemptions: The challenges of India's DPDP Act. Economic and Political Weekly, 58(37),

Khaira, R. (2018, January 4). Rs 500, 10 minutes, and you have access to billion Aadhaar details. The Tribune. https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361

Times of India. (2021, June 11). Government denies reports of CoWIN data breach. The Times of India. https://timesofindia.indiatimes.com

The Hindu. (2017, March 26). Aadhaar data breach raises concerns over privacy. The Hindu. https://www.thehindu.com

Press Information Bureau (PIB). (2023, June 12). Clarification on media reports regarding alleged breach of CoWIN data. Government of India. https://pib.gov.in/PressReleasePage.aspx?PRID=1931373

Unique Identification Authority of India (UIDAI). (2024). Aadhaar security and privacy framework. https://uidai.gov.in