



CLOUD COMPUTING ADOPTION FOR E-GOVERNANCE IN INDIA: A THEORETICAL FRAMEWORK FOR INSTITUTIONAL READINESS AND PUBLIC VALUE

Gurbani Kaur

Scholar

Department of Computer Science and engineering

NIILM University, Kaithal, Haryana

Dr. Pawan Kumar

Professor

Department of Computer Science and engineering

NIILM University, Kaithal, Haryana

Abstract

Cloud computing has moved from being an optional information-technology arrangement to becoming a strategic infrastructure for digital government. Its elasticity, measured service, rapid provisioning and shared-resource model can help public institutions expand service delivery without repeatedly creating isolated hardware environments. However, government adoption cannot be explained by technological advantage alone because public agencies operate under legal mandates, budget rules, legacy systems, accountability obligations and citizen expectations. This theoretical paper develops an integrated framework for explaining cloud-computing adoption in Indian e-governance. It synthesises the Technology-Organisation-Environment framework, Diffusion of Innovation theory and the public-value perspective, and situates them within India's MeghRaj/GI Cloud policy environment. The paper argues that adoption readiness is produced by six interacting domains: technological suitability, organisational capability, policy and regulatory support, institutional trust, ecosystem interoperability and public-value orientation. A stage-based model is proposed in which assessment, controlled migration, service integration, institutionalisation and continuous optimisation are linked to measurable governance outcomes. The framework extends cost-centred cloud adoption models by treating citizen accessibility, transparency, resilience, inclusion and accountability as core adoption outcomes. It offers propositions for future empirical testing in ministries, state departments, municipalities and municipal corporations, and provides a structured basis for cloud-selection, capability-building and policy evaluation.

Keywords: Cloud computing; e-governance; MeghRaj; institutional readiness; public value; Technology-Organisation-Environment framework

1. Introduction

E-governance depends on the ability of public institutions to collect, process, exchange and protect information while delivering services at a scale that changes across locations and time. Traditional departmental information systems were commonly developed as separate projects, with dedicated servers, application-specific databases and limited integration. Such arrangements can produce duplicated expenditure, underused capacity, slow procurement, inconsistent security practices and difficulty in scaling services during periods of high demand. Cloud computing offers an alternative by enabling on-demand access to shared computing resources that can be provisioned and released with limited administrative effort. The NIST model identifies on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service as its central characteristics (Mell & Grance, 2011). These characteristics are directly relevant to public services that must remain available to large and diverse populations.

The supplied synopsis identifies cloud computing as a means of reducing capital expenditure, improving utilisation, supporting anywhere access and enabling e-governance applications. It also recognises that adoption involves benefits and risks, policy choices and the need for a suitable architecture for municipalities and municipal corporations. The present paper develops these ideas into a theoretical research article. Rather than treating migration as a purely technical exercise, it examines cloud adoption as an institutional decision shaped by technological fit, organisational readiness, environmental conditions and the public value expected from digital services.

India provides an important context for this analysis. MeghRaj, the Government of India Cloud initiative, was established to support secure, scalable and elastic delivery of e-governance services. Official reporting indicates that the platform expanded from 342 government departments in 2015–16 to 2,323 departments by June 2026, supporting platforms such as DigiLocker, MyGov and the National Scholarship Portal (Press Information Bureau, 2026). This growth demonstrates policy commitment, but scale alone does not guarantee effective use. Agencies may migrate unsuitable legacy applications, replicate existing silos in a new hosting environment, underestimate organisational change or adopt services without clear accountability for performance, data, security and vendor relationships.

Accordingly, this paper asks a theoretical question: what combination of conditions explains sustainable cloud adoption for e-governance in India? The answer requires more than a list of benefits

and barriers. It requires a framework connecting adoption determinants with implementation stages and governance outcomes.

2. Objectives of the Paper

The paper has four objectives: to synthesise major theoretical explanations of organisational cloud adoption; to identify determinants relevant to Indian e-governance; to propose an integrated institutional-readiness and public-value framework; and to develop propositions that can guide future empirical studies in central, state and local government organisations.

3. Research Methodology

This is a conceptual and theoretical paper based on structured narrative synthesis. It draws on the synopsis supplied by the researcher, foundational cloud-computing literature, organisational technology-adoption studies, peer-reviewed work on government cloud adoption and current Indian policy documents. The analysis uses concept integration rather than statistical testing. Constructs from the Technology-Organisation-Environment (TOE) framework, Diffusion of Innovation (DOI) theory and public-value scholarship are compared, grouped and adapted to the administrative conditions of Indian e-governance. The proposed relationships are expressed as theoretical propositions for later verification through surveys, interviews, case studies or mixed-method research. No human participants or personal data were involved.

4. Theoretical Foundations

The TOE framework explains organisational adoption through three contexts: the characteristics of the technology, the internal condition of the organisation and the external environment in which the organisation operates (Tornatzky & Fleischer, 1990). In cloud studies, technological factors commonly include relative advantage, compatibility, complexity, security, reliability and scalability. Organisational factors include top-management support, financial capacity, technical competence, governance structure and readiness for change. Environmental factors include regulation, provider capability, procurement rules, inter-organisational pressure and supporting infrastructure. A systematic review by Al Hadwer et al. (2021) confirms that cloud adoption is not driven by one factor; it reflects interacting organisational conditions interpreted within the TOE domains.

DOI theory adds an innovation-perception perspective. Organisations are more likely to adopt an innovation when decision-makers perceive a clear relative advantage, compatibility with existing values and processes, manageable complexity, opportunities for trial and visible results (Rogers, 2003). These attributes are important in government because the consequences of failure are public, budgets are scrutinised and decision-makers may be risk-averse. Qatawneh (2024) found that technological,

organisational and environmental factors significantly influenced cloud adoption in government systems and that decision-makers' IT knowledge moderated these relationships. Therefore, readiness is partly cognitive: administrators must understand what the cloud can and cannot solve.

A public-value perspective is required because government adoption differs from commercial adoption. A private firm may emphasise cost, speed and competitiveness, while a public institution must also consider fairness, accessibility, legality, transparency, trust and continuity of essential services. Cloud adoption should therefore be evaluated by whether it improves the value experienced by citizens and the legitimacy of administrative processes. Public value acts as both a design principle and an outcome domain. It discourages technology-centred migration that reduces cost but worsens exclusion, accountability or service reliability.

5. Indian E-Governance and the Cloud Policy Context

The Indian cloud environment combines national infrastructure, empanelled providers, government data centres and multiple deployment options. Earlier studies highlighted the potential of MeghRaj to reduce duplication, promote shared infrastructure and support projects such as digital document services and online registration (Srivastava, 2018; Vijai & Joyce, 2020). Kushagra and Dhingra (2022) observed that Indian government adoption was shaped by policy gaps, legacy migration, service-model choices and sectoral differences. Their analysis reinforces the need to connect policy design with actual organisational capability.

The 2026 Guidelines for Cloud Selection Framework introduce a more explicit decision logic. Ministries and departments are required to classify applications and data by sensitivity and criticality before selecting a deployment option. The framework distinguishes categories of official applications and specifies safeguards, disaster-recovery expectations and procurement routes (Ministry of Electronics and Information Technology [MeitY], 2026). This policy direction is significant because it moves cloud adoption away from a uniform "cloud-first" assumption and toward risk-based selection. Yet classification is only one part of readiness. Agencies still require application inventories, process ownership, contract-management capacity, interoperability standards, skilled personnel, financial planning and outcome measurement.

Local governments face additional challenges. Municipalities often manage high-volume citizen services such as property tax, certificates, licences, grievance redressal, water billing and urban records, but their technical capacity varies widely. Shared cloud platforms can reduce infrastructure duplication, although poorly standardised migration may reproduce fragmented workflows. A theoretical model for

Indian e-governance must therefore be scalable across agencies while remaining sensitive to differences in administrative capacity.

6. Proposed Institutional Readiness and Public Value Framework

The proposed framework contains six mutually reinforcing domains. The first is technological suitability. An application should migrate only when its workload pattern, integration needs, data sensitivity, latency, availability requirements and technical architecture are compatible with an appropriate cloud service and deployment model. Relative advantage must be demonstrated through a business and service case rather than assumed. A technically unsuitable migration can increase cost, create performance problems or produce dependence on proprietary services.

The second domain is organisational capability. Sustainable adoption requires executive sponsorship, accountable service owners, cloud architecture skills, cybersecurity competence, financial management, change leadership and user support. Top-management support is not limited to approving expenditure; it includes resolving interdepartmental conflict, assigning responsibility and maintaining the programme beyond the initial migration. Organisational readiness also requires mapping legacy applications, cleaning data, redesigning processes and training administrative users. Cloud adoption without process reform may merely relocate inefficient systems.

The third domain is policy and regulatory support. Government agencies require clear rules for data classification, procurement, audit, service-level agreements, incident reporting, exit management and record retention. Policy must reduce uncertainty without eliminating responsible experimentation. The regulatory environment should also define how agencies remain accountable when infrastructure or software is operated by a cloud service provider. The government remains responsible for lawful and reliable public service even when technical operations are outsourced.

The fourth domain is institutional trust and assurance. Trust is produced through verifiable controls rather than provider reputation alone. Agencies need independent audits, transparent performance reporting, tested backup and disaster recovery, identity and access controls, vulnerability management and defined escalation mechanisms. Trust also has a citizen dimension. People are more likely to use digital public services when they believe that government systems are reliable, understandable and respectful of their information.

The fifth domain is ecosystem interoperability. E-governance services cross departmental boundaries; therefore, cloud platforms must support standard data formats, documented application programming interfaces, identity federation, portability and integration with common government platforms. Interoperability reduces duplication and enables a citizen to receive a coordinated service rather than

navigate multiple disconnected departmental systems. Portability and exit planning also limit vendor lock-in and preserve administrative autonomy.

The sixth domain is public-value orientation. Adoption decisions should specify the public outcomes expected from the investment. These may include shorter service-delivery time, broader geographic access, lower citizen transaction cost, improved transparency, resilience during emergencies, multilingual access, accessibility for persons with disabilities and better grievance resolution. Public-value indicators create a line of sight from technical architecture to citizen experience.

These domains operate through five implementation stages. Stage one is readiness assessment, including application inventory, data classification, stakeholder analysis, risk assessment and baseline performance measurement. Stage two is controlled migration, beginning with prioritised workloads, pilots and explicit acceptance criteria. Stage three is service integration, where migrated systems are connected to identity, payment, notification, records and analytics services. Stage four is institutionalisation, which embeds cloud governance, budgeting, skills, audit and accountability in routine administration. Stage five is continuous optimisation, where performance, cost, security, inclusion and citizen outcomes are monitored and improved. Feedback from later stages should alter architecture and policy decisions, making adoption an iterative governance process rather than a one-time project.

7. Theoretical Propositions

P1: Perceived relative advantage will positively influence government cloud adoption only when the proposed service is compatible with application criticality, data classification and existing administrative processes.

P2: Organisational capability will mediate the relationship between favourable cloud policy and successful implementation; policy support without skills, ownership and change capacity will produce symbolic or incomplete adoption.

P3: Decision-makers' cloud and risk knowledge will strengthen the positive effect of technological and organisational readiness on adoption quality.

P4: Verifiable assurance mechanisms will reduce perceived risk and increase institutional and citizen trust in cloud-based e-governance services.

P5: Interoperability and portability will positively affect service integration and negatively affect vendor lock-in.

P6: Public-value measurement will improve the sustainability of cloud programmes by aligning technical performance with accessibility, transparency, resilience and citizen outcomes.

8. Discussion and Policy Implications

The framework explains why a technically capable cloud platform may still deliver weak governance outcomes. Adoption can fail when agencies lack process ownership, migrate without redesign, select services without data classification, or measure success only by servers decommissioned and expenditure shifted from capital to operating budgets. The proposed model treats cloud adoption as coordinated institutional change. It also distinguishes readiness from adoption: an agency may purchase cloud services while remaining institutionally unready to govern them.

For policymakers, the framework supports a common readiness-assessment instrument for ministries, states and urban local bodies. Such an instrument should score application suitability, leadership, skills, procurement capacity, security assurance, interoperability and public-value indicators. For municipalities, shared reference architectures and reusable service components can reduce duplication, but local process mapping and accountability must remain explicit. Capacity-building programmes should target administrators, finance officers, procurement teams, auditors and service owners, not only technical personnel.

For researchers, the six domains and five stages can be operationalised in surveys and comparative case studies. Studies may test whether institutional capability mediates policy effects, whether public-value measurement improves post-adoption performance, and whether cloud knowledge moderates risk perceptions. Longitudinal research is especially important because adoption benefits and dependencies become visible over time.

9. Limitations and Future Research

The framework is intentionally broad and should not be interpreted as a universal scoring formula. Government organisations differ in constitutional functions, risk exposure, financial autonomy, technical maturity and citizen populations. The relative importance of each domain may therefore vary. For example, interoperability may dominate in welfare-service integration, whereas resilience and latency may dominate in emergency or transport systems. The framework also does not prescribe a single public, private, community or hybrid cloud model. Deployment choice should follow classification, workload and accountability analysis.

Future research should translate each construct into measurable indicators and test the framework at central, state and municipal levels. A multi-stage design could first use expert interviews to validate indicators, then apply a survey to estimate relationships among readiness, adoption quality and public

value, and finally use case studies to explain differences between high- and low-performing agencies. Longitudinal studies should compare expected and realised cost, service quality and citizen outcomes before and after migration. Researchers should also examine whether common cloud platforms reduce digital inequality or concentrate capability in already well-resourced departments. Another useful direction is the development of a municipal cloud maturity index covering governance, skills, application architecture, security, interoperability and citizen-centred service design. Such research would convert the theoretical model into a practical diagnostic tool while preserving the principle that adoption quality must be assessed in relation to public purpose. Comparative work should additionally examine rural and urban service settings, because connectivity, staffing, language requirements and assisted-access arrangements may change the meaning of readiness. Evidence from unsuccessful or delayed migrations is particularly valuable, since official success reports may understate the institutional friction involved in redesigning workflows, reallocating budgets and retiring legacy systems.

10. Conclusion

Cloud computing can provide a scalable foundation for Indian e-governance, but its contribution depends on the quality of institutional decisions surrounding adoption. The paper integrates TOE, DOI and public-value perspectives to propose a framework based on technological suitability, organisational capability, policy support, trust, interoperability and public value. It further presents a stage model from readiness assessment to continuous optimisation. The central argument is that cloud adoption should not be judged by migration alone. It should be judged by whether government can govern the cloud environment, protect accountability and convert technical capability into reliable, inclusive and transparent public services. The framework is theoretical and requires empirical validation across different tiers of government, particularly municipalities and municipal corporations where capacity and service demands vary considerably. Such validation should compare institutional readiness before migration with measurable public-service outcomes after implementation.

References

1. Al Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using the Technology-Organization-Environment framework. *Internet of Things*, 15, 100407. <https://doi.org/10.1016/j.iot.2021.100407>
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. <https://doi.org/10.1145/1721654.1721672>

3. Kushagra, K., & Dhingra, S. (2022). Cloud doctrine: Impact on cloud adoption in the government organizations of India. *Journal of Science and Technology Policy Management*, 13(4), 925–951. <https://doi.org/10.1108/JSTPM-06-2019-0058>
4. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-145>
5. Ministry of Electronics and Information Technology. (2026). Guidelines for cloud selection framework (Office Memorandum F. No. 9(3)/2025-EG-II, 20 March 2026). Government of India.
6. Mohammed, F., Ibrahim, O., Nilashi, M., & Alzurqa, E. (2017). Cloud computing adoption model for e-government implementation. *Information Development*, 33(3), 303–323. <https://doi.org/10.1177/0266666916656033>
7. Mounika, K., Taduri, A., & Manda, S. (2017). A study on cloud computing in e-governance. *International Journal of Computer Sciences and Engineering*, 5(12), 254–258. <https://doi.org/10.26438/ijcse/v5i12.254258>
8. Press Information Bureau. (2026, July). Driving the future through cloud computing. Government of India.
9. Qatawneh, N. (2024). Building a framework to drive government systems' adoption of cloud computing through IT knowledge. *Discover Sustainability*, 5, 282. <https://doi.org/10.1007/s43621-024-00427-8>
10. Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
11. Srivastava, N. (2018). MeghRaj: A cloud environment for e-governance in India. *International Journal of Computer Sciences and Engineering*, 6(11), 759–763. <https://doi.org/10.26438/ijcse/v6i11.759763>
12. Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
13. Vijai, C., & Joyce, D. (2020). Cloud-based e-governance in India. *Shanlax International Journal of Management*, 8(2), 72–78. <https://doi.org/10.34293/management.v8i2.3334>
14. Yeboah-Boateng, E. O., & Essandoh, K. A. (2014). Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. *International Journal of Emerging Science and Engineering*, 2(4), 13–20.