SHODH SAGAR®
Universal Research Reports
ISSN: 2348-5612 | Vol. 11 | Issue 2 | Apr-Jun 2024 | Peer Reviewed & Refereed

Decentralized Cloud Architectures for E-Governance: Leveraging Edge Computing and Blockchain to Improve Accessibility and Trust in Public Services

Priyanka*
Subject computer science
Research scholar
Kalinga university, Raipur

DOI: http://doi.org/10.36676/urr.v11.i2.1593
Check for updates
Accepted: 11/05/2024 Published: 25/05/2024

* Corresponding author

Abstract

Strong, scalable, and citizen-centric service delivery mechanisms are in high demand as digital transformation programs pick up steam across government sectors. However, the many demands of e-governance are often not adequately met by conventional cloud computing models, which depend on centralised data centres and processing hubs, particularly in geographically scattered, distant, or infrastructure-deficient locations. These centralised systems are inherently limited in terms of responsiveness, where high latency impedes real-time citizen interaction and service efficiency; scalability, as growing demand puts strain on centralised servers; and trust, because of worries about single points of failure and data manipulation.

To address these issues, this study suggests and examines a decentralised cloud computing paradigm that combines blockchain technology with edge computing, two innovative technologies. By placing tiny data centers such as community centres, local administrative offices, or even mobile units at the edge of the network, edge computing brings data processing closer to the user. By drastically lowering latency, this makes it possible to conduct vital services like emergency response, subsidy distribution, and identity verification in real time. Blockchain technology, on the other hand, keeps an unchangeable, decentralised record of every transaction and service interaction, guaranteeing data integrity and reliability. Every citizen interaction—from benefit disbursements to licence applications—is securely verified and clearly documented, which promotes increased accountability in government processes.

The suggested hybrid framework improves accessibility by operating in low-connectivity environments and tamper-resistance by making data changes nearly impossible without system-wide consensus, in addition to strengthening the resilience of e-governance platforms ensuring continuity during internet outages or cyberattacks.

The research compares three different national e-governance models Kenya's eCitizen site, India's DigiLocker and Aadhaar ecosystem, and Estonia's X-Road platform in order to assess the feasibility of this strategy. Each provides insightful information on the advantages and disadvantages of the e-governance systems in use today. Kenya exemplifies the difficulties of growing digital services in environments with limited resources; India exhibits extensive digital identity integration but encounters obstacles to accessibility in rural areas; Estonia exhibits sophisticated interoperability but still relies on centralised servers. Together, these

examples demonstrate the viability, flexibility, and scalability of the decentralised approach, which can be tailored to regional governance contexts while upholding international norms for efficiency, privacy, and openness.

1. Introduction

With the emergence of digital governance, the public sector is undergoing a radical change in the way governments engage with their constituents, corporations, and other stakeholders. Initiatives for e-governance, which include digital identification systems, online citizen portals, and automated public service delivery, are becoming more and more important for promoting openness, boosting administrative effectiveness, and facilitating inclusive citizen engagement. Achieving the Sustainable Development Goals (SDGs), particularly those related to lowering inequality and establishing strong institutions, depends on these systems.

Scaling these activities has been made possible by the introduction of cloud computing, which provides affordable, adaptable, and on-demand infrastructure solutions. Governments have been able to centralise and digitise their services using cloud-based e-governance systems, which has improved operational control and accessibility. Nevertheless, the majority of these systems depend on centralised cloud infrastructures, which inevitably bring with them some drawbacks. The timeliness and dependability of public digital services have been seriously threatened by problems including single points of failure, system outages, and network latency. Furthermore, worries about data breaches, illegal spying, and the lack of auditability in centralised data repositories often erode public confidence in digital government.

Furthermore, the digital divide is still a major issue, especially in impoverished, rural, or distant areas where fair access to e-governance services is hampered by inadequate computer equipment and poor internet connection. Important public interactions like healthcare registration, subsidy payout, or identity verification might be seriously delayed or disrupted in such situations due to latency and reliance on remote data centres.

This study suggests a decentralised cloud architecture that uses edge computing and blockchain technologies to rethink public service delivery in order to solve these systemic issues. Edge computing greatly reduces reaction times and relieves bandwidth demand on central systems by enabling data processing to take place closer to the site of data production, whether at local devices, community servers, or micro-data centres. In addition to increasing service stability, this makes it possible for consumers with limited or sporadic internet connectivity to access essential services with the least amount of delay.

At the same time, public sector operations gain an extra degree of security, trust, and transparency with the incorporation of blockchain-based audits. Blockchain guarantees that every contact, whether it be the issuing of a government certificate, a tax submission, or a social welfare program, is tamper-proof and verifiable by logging transactions on an immutable distributed ledger. Such a framework facilitates strong supervision and accountability while also fostering public confidence in e-governance.

By guaranteeing that services are not only accessible but also robust, safe, and transparent, the suggested decentralised approach ultimately seeks to democratise access to digital public infrastructure, irrespective of a citizen's socioeconomic or geographic origin. With the use of comparative analysis from international case studies, this study examines the conceptual framework, realistic implementation techniques, and policy implications of this next-generation e-governance architecture.

2. Review of Literature

Designing digital governance systems that are reliable, scalable, and responsive has become easier because to the confluence of cutting-edge technologies like blockchain and edge computing. The ability of edge computing, which positions processing power closer to the data source, to lower latency, improve real-time responsiveness, and minimise bandwidth congestion is becoming more widely acknowledged. This is especially important in situations involving remote service delivery and extensive public data interactions. Shi et al. (2016) claim that edge computing makes distributed data processing possible, which not only speeds up reaction times but also guarantees service continuity even in areas with poor connection. This is especially important in developing countries where digital infrastructure is still dispersed unevenly.

However, blockchain technology has become a potent instrument for improving data management's immutability, security, and transparency. Tamper-proof record keeping is made possible by the decentralised ledger system, which is crucial in e-governance scenarios where accountability and trust are crucial. Blockchain may decentralise the storage and verification of public records, including identification certificates, property titles, and social welfare transactions, according to Zyskind et al. (2015). This ensures that once a record is entered to the system, it cannot be changed without consensus. This is particularly advantageous when it comes to fighting corruption and boosting public trust in digital services.

Both technologies have bright futures, but there is still a lack of integration with the general public digital infrastructure. Few have accomplished full-scale, secure, and interoperable deployments at the national level; the majority of current implementations are dispersed or limited to pilot projects. This is caused by a number of issues, such as the difficulty of modernising outdated IT systems, worries about data sovereignty, legislative voids, and the substantial upfront costs associated with infrastructure construction and capacity growth.

References from governments that have advanced digital public infrastructure are helpful. For example, the X-Road platform in Estonia is considered a standard for e-governance because of its secure data interchange layer that links several government systems. The system is still largely dependent on centralised servers and data centres, however, which leaves it open to national cyber attacks and single points of failure. In a similar vein, nearly a billion Indians have successfully digitised identity verification and document storage thanks to the Aadhaar ecosystem and DigiLocker services. Despite these systems' strength and scalability, concerns about data privacy, surveillance, and resilience are brought up by their central cloud design, particularly in light of the growing risks to cybersecurity.

This study expands on previous regional and international efforts by putting forward a genuinely decentralised, citizen-centered e-governance approach. The idea uses blockchain to give transparent and unchangeable records of all government transactions and combines edge computing to bring computation and services closer to the citizen, decreasing reliance on national data centres. By doing this, it creates the groundwork for more robust and democratic digital public systems in addition to improving scalability and service accessibility.

3. Techniques

The design and feasibility of a decentralised cloud infrastructure for e-governance are investigated in this study using a mixed-method approach. To provide a thorough assessment from technical, administrative, and policy-oriented viewpoints, the methodology combines qualitative and quantitative methodologies. The approach is organised around four main elements:

3.1 Design of the System

The creation of a conceptual architectural model that incorporates three technology pillars is at the heart of this research:

In order to lower latency and facilitate real-time, local processing, Edge Computing Nodes are positioned strategically across various geographic sites, including community centres, municipal offices, and rural kiosks.

Permissioned blockchains, such as Hyperledger Fabric, are used in Blockchain Ledger Infrastructure to provide tamper-proof recording of citizen transactions, authentication logs, and public service interactions.

Centralised fallback systems serve as backup control centres and cloud-based repositories that facilitate synchronisation, guarantee system consistency, and provide disaster recovery capabilities.

Iterative consultation with cloud reference architectures, e-governance frameworks, and industry white papers released by organisations like NIST and MeitY (India) was used to create this architectural model.

3.2 Evaluation via Comparison

Three actual e-governance ecosystems were examined using a comparative case study methodology in order to contextualise the model:

Globally renowned for its modular, API-driven, and very secure data sharing platform is Estonia's X-Road.

As a component of the India Stack architecture, DigiLocker allows citizens of India to save and retrieve digital documents associated with their national identification.

The eCitizen portal in Kenya is a centralised public service site that faces different connection issues in remote areas.

Official documentation, technical reports, and user feedback surveys were the sources of key performance indicators (KPIs) such service response time, system downtime, scalability, and trust measures. Finding the weaknesses in each system and evaluating the usefulness and advantages of adding decentralised components were the objectives of this investigation.

3.3 Interviews with Experts

Twelve experts participated in semi-structured interviews to verify the conceptual model and provide useful insights. These experts included:

Planning for the nation's digital infrastructure involves government IT personnel.
Public-private cooperation cloud computing architects (NIC, AWS Public Sector India, etc.)
Consultants in cybersecurity with expertise implementing blockchain

Infrastructure preparedness, regulatory barriers, technological scalability, financial restraints, and cyber-risk management were the main topics of the interview questions. To improve the system model and its viability assumptions, the replies were synthesised after being thematically coded using NVivo software.

3.4 Testing via Simulation
Technical validation utilising edge computing simulation tools (such as iFogSim and EdgeCloudSim) was the last stage. The objective was to model e-governance tasks like:

Instantaneous identity confirmation
Access to land record databases locally
Processing licence and benefit applications

Among the key metrics assessed were:

Milliseconds are used to measure the latency between data input and service response.
System Availability: The percentage of simulated uptime under different load scenarios
Blocks per second under concurrent user demand is the blockchain transaction throughput.
Time required to reconcile data between edge and central nodes is known as the "data synchronisation lag."

To evaluate the system's resilience, testing scenarios included high-load events (such as during subsidy implementation), urban vs rural network settings, and disaster recovery exercises.

4. The Decentralised E-Gov Cloud Model is the suggested architecture.
The main drawbacks of conventional e-governance platforms—latency, trust, accessibility, and data control—are addressed by the suggested decentralised design, which blends edge computing, blockchain technology, and centralised cloud systems. It is composed of four interconnected levels, each of which is essential to providing safe, open, and effective public services.

4.1 The Layer of Edge Computing
This layer involves the deliberate placement of local edge nodes, which are small computer devices with processing and storage capacities, in easily accessible public infrastructure including community centres, banks, post offices, schools, and panchayat offices. The purpose of these nodes is to:

Locally cache and store citizen data to facilitate quick retrieval and less reliance on central servers.
In regions with erratic internet availability, assist offline-first processes like filing grievances, retrieving documents, and submitting forms.
For time-sensitive applications like public grievance monitoring, emergency healthcare access, and birth registrations, process requests in real-time to minimise latency.
When connection is restored, periodically sync with central servers to guarantee data backup and consistency.

These nodes run e-governance apps that are suited to local language preferences and service requirements using containerised microservices. Because they have low-energy CPUs and solar power units, they are also designed to survive severe local conditions and power outages.

4.2 The Layer of Blockchain

Distributed ledger technology (DLT) is introduced at this layer to guarantee traceability, transparency, and trust in all public interactions. Every transaction in the e-governance system, including the issuance of birth certificates, land records, tax returns, and welfare payments, is documented on a permissioned blockchain (such as Quorum or Hyperledger Fabric), which comprises:

Use smart contracts to enforce regulations and automate processes (such as confirming a person's eligibility for subsidies).
Unchangeable audit trails allow for real-time monitoring by authorities and people.
Decentralised identity management (DID) systems may improve privacy and lessen need on central authentication.
techniques for inter-node consensus to minimise transaction latency and guarantee uniformity across government agencies.

Government-approved validators run the blockchain network, guaranteeing decentralisation and adherence to regulations.

4.3 Backup in the Central Cloud

The centralised cloud layer serves as the fundamental infrastructure for the following, while the edge and blockchain layers decentralise operations:

long-term archival preservation of transaction logs and citizen data.
acting as the central point for coordinating the distribution of application patches, policy modifications, and software upgrades to edge nodes.
providing disaster recovery features, which allow for quick service restoration in the case of a cyberattack or regional node failure.
By safely combining anonymised citizen data for policymaking, resource allocation, and service optimisation, inter-agency data analytics are made possible.

This layer is protected by multi-layered encryption, intrusion detection systems, and adherence to international cloud security standards like ISO/IEC 27018. It makes use of national data centres (such those under NIC or MeitY in India).

4.4 Controls for Data Sovereignty

This model's compliance with data sovereignty and privacy laws, which require that private information must be kept inside the nation's legal borders, is one of its key characteristics. Important elements consist of:

Data geofencing: Making sure that, particularly for federal systems, citizen data is handled and retained within the boundaries of designated states or administrative areas.

Using the TLS 1.3 and AES-256 protocols to encrypt all data from beginning to finish, both in transit and at rest.

Government workers are subject to role-based access control (RBAC), which restricts their access to private data.

Features for data anonymisation are included into the blockchain and central layers for analytics while protecting the privacy of citizens.

adherence to national and regional standards, including the OECD Guidelines on Data Governance, the EU GDPR, and India's Digital Personal Data Protection Act, 2023.

The design minimises the dangers of cross-border data transfers, which is crucial for international collaborations and the engagement of foreign cloud vendors, while supporting local autonomy and public confidence by decentralising data storage while maintaining regulatory supervision.

Thus, this multi-tiered design creates an environment for e-governance that is robust, safe, and egalitarian and that can expand to both developed and underdeveloped areas. Emerging technologies coming together under a single framework puts governments in a position to provide digital public services that are more intelligent, inclusive, and responsible.

5. Principal Benefits

Decreased Latency

The considerable decrease in service latency in this decentralised paradigm is among its most important enhancements. All user queries are often routed via centralised cloud servers by traditional e-governance solutions, which may cause delays, particularly during periods of high demand or in distant areas. Data processing and validation may take place in real time by placing edge computing nodes closer to the data source (such as public kiosks, health facilities, or local government offices). For instance, edge nodes may locally validate user identification, perform the request, and synchronise with the central cloud asynchronously in applications like ration card verification, public grievance reporting, and birth registration. The citizen experience is improved by this almost immediate response, which also lessens the need for consistent internet access for essential services.

Transparency and Trust

This concept makes use of blockchain technology to guarantee that every digital transaction is captured irrevocably, which means that once information is entered, it cannot be changed or removed. This creates a public ledger that cannot be altered on things like service requests, permit approvals, welfare payments, and property exchanges. A visible, verifiable transaction history makes it possible for regulatory agencies to conduct real-time audits and boosts public confidence in digital government services. This is especially helpful in fields where corruption is common and record tampering has a history of undermining justice and legitimacy.

Scalability

The rigidity of centralised systems when scaling is one of the most urgent issues in digital governance. Reconfigurations, downtime, or infrastructure modifications are often necessary when adding new modules or services. The decentralised approach, on the other hand, makes use of containerised deployments and microservices, which can be deployed to edge nodes without interfering with already-running services. For example, a municipality may expand its public service offerings in a modular and flexible manner by securely pushing updates to edge nodes across regions separately if it wishes to implement a new e-health application or disaster warning system. This adaptability guarantees that the platform will continue to respond to changing community demands and policies.

Accessibility

Increased accessibility is perhaps the greatest revolutionary benefit, especially for underprivileged, rural, or distant people. Many residents in these places have inadequate or erratic internet connectivity, which significantly limits their ability to use online portals. Governments may provide essential services offline or sporadically online by deploying edge devices in panchayats, local offices, schools, or mobile vans. This ensures uninterrupted availability even in the event of network outages or natural catastrophes. Additionally, when connection is restored, these edge nodes may retain and synchronise data with central systems, allowing for resilient service delivery in emergency scenarios when conventional digital systems often malfunction, including floods, earthquakes, or power outages.

6. Case Study Insights

Three national e-governance ecosystems—Estonia, India, and Kenya—are compared to show the unique potential and problems of using decentralised cloud infrastructures. Although the operational circumstances, infrastructure constraints, and regulatory frameworks of each scenario are different, they are all in need of increased scalability, robustness, and trust. The following observations show how service delivery in various governance contexts might be enhanced by the suggested edge-blockchain-enabled architecture.

6.1 X-Road (Centralised + API Integration) in Estonia

Since its X-Road infrastructure allows more than 1,000 public and commercial organisations to securely share data, Estonia is known across the world as a leader in digital governance. High-level interoperability and real-time service integration are ensured by the system's use of centralised middleware and an API-based design.

However, a single point of vulnerability is introduced by this dependence on centralised infrastructure. The dangers of over-centralization, particularly in vital public infrastructure, were exposed by countrywide cyberattacks in 2007, despite Estonia's robust cybersecurity posture.

By sharing workloads and allowing for localised service continuity in the case of central system failures, integrating edge computing nodes into public service centres or local municipalities may increase system resilience. In the meanwhile, blockchain integration may provide an unchangeable audit layer to monitor data access and guarantee open communication, especially for delicate processes like real estate registration or medical treatment. When combined, these technologies might add layers of redundancy, traceability, and fault tolerance to Estonia's previously developed digital architecture.

6.2 DigiLocker in India (Authentication and Storage of Documents)

As a component of the Digital India Mission, India's DigiLocker effort provides cloud-based storage for official papers such as driver's licenses, academic credentials, and information related to Aadhaar. With more than 150 million users, the system is widely used, but it has significant scalability and performance issues, particularly in rural regions with limited connectivity or during periods of high demand.

Because of its extreme centralisation, the existing infrastructure is less responsive in areas with sporadic internet access. When placed in community centres, panchayats, or local government offices, edge computing nodes may serve as mini-clouds or data caches, providing offline or low-latency access to vital documents and services.

Blockchain-based verification will also lessen the need for constant server connection for authentication. Digitally signed credentials that are maintained locally and verified via distributed ledgers might be used by citizens, increasing system efficiency and confidence. This is especially important in situations when delays in verification might have socioeconomic repercussions, such as public exams, rural banking, and subsidy distribution.

6.3 Kenya's Digital Service Aggregator, or eCitizen Portal

Business registration, passport applications, and property records are just a few of the more than 100 government services that may be accessed via Kenya's eCitizen platform. The platform has significantly improved public service delivery efficiency and decreased corruption.

However, the platform's full potential is limited by the unequal internet coverage that persists, particularly in rural and peri-urban regions. Unreliable connection often results in lengthy wait times, service interruptions, and manual backup mechanisms for citizens.

Accessibility may be significantly improved by deploying edge-enabled kiosks or mobile government vans that are outfitted with blockchain-backed transaction records and localised processing units. When connection is restored, these configurations may serve as independent service points that communicate with central systems. The implementation of blockchain in this context guarantees that, even in semi-connected contexts, all service interactions—like access to property records or applications for business licenses—are impenetrable.

Furthermore, by providing governance services to populations who were previously excluded due to infrastructure constraints, this hybrid design promotes digital inclusion.

Integration of Case Study Findings

In each of the three situations, it is clear that:

Localised decision-making, robustness, and quicker reaction times are made possible by edge computing, which is especially important for tasks that are sensitive to latency.

Transparency, trust, and non-repudiation are provided by blockchain, which is crucial for citizen confidence and public accountability.

In addition to meeting each nation's infrastructure requirements, a decentralised cloud architecture promotes the more general objectives of fairness, accessibility, and national sovereignty in data management.

All of these observations support the idea that a decentralised cloud architecture that is adaptable to the distinct technical, geographical, and regulatory contexts may greatly increase the resilience and inclusiveness of e-governance platforms around the globe.

7. Difficulties and Restrictions

Decentralised cloud architectures have the potential to revolutionise e-governance, but their implementation and sustainability depend on a number of issues and constraints that need to be properly handled. These include legal, technological, and infrastructure barriers that may affect the viability and expandability of such models.

1. Infrastructure Deployment Cost

Decentralised cloud infrastructure implementation necessitates a large initial expenditure, particularly when incorporating permissioned blockchain networks and edge computing nodes. With edge-based systems, many localised devices are deployed across urban and rural areas, in contrast to typical centralised cloud setups that depend on fewer but bigger data centres. In addition to physical gear (such edge servers and local storage units), these devices also need a steady power source, internet access, and regular maintenance.

Because blockchain deployment requires smart contract platforms, distributed ledger systems, and strong security frameworks, the cost goes up even more. Budgetary restrictions may affect the public sector, especially in developing nations, making it difficult to give such digital infrastructure top priority without outside investment or public-private partnerships.

Moreover, infrastructure is not the only expense. The Total Cost of Ownership (TCO) is increased by managing network operations, training staff, and converting existing systems to new protocols. Government organisations could be reluctant to commit to such extensive changes in the absence of explicit return-on-investment indicators or legislative incentives.

2. Conflicts with Data Synchronisation

A major technological problem in a decentralised e-governance architecture, particularly one that uses edge computing, is synchronising data in real-time across many nodes. The system must make sure that all other pertinent nodes and the central cloud are updated precisely and quickly when data is created or changed at various places (for example, when a citizen changes their information at a rural service centre).

This raises the possibility of version conflicts or inconsistent data, particularly in places with sporadic connection. For example, it becomes difficult to determine whether data is the most current or legitimate when two distinct edge nodes update the same citizen record offline. Data integrity problems, which are especially important in delicate fields like healthcare, taxes, or legal paperwork, might result from inadequate dispute resolution procedures.

Strong consensus methods, real-time monitoring, and fallback mechanisms are necessary for effective synchronisation; they may raise system complexity and resource use. These issues are made worse in areas with inadequate network infrastructure, resulting in a digital divide in the consistent provision of services.

3. Gaps in the Law and Regulation Framework

Lack of a supportive legal framework is a significant barrier to the broad use of blockchain and decentralised cloud technologies for public governance. The majority of current e-governance and data protection regulations are based on centralised systems, in which data is owned and managed by a single organisation, usually the government or a central agency.

However, decentralised systems include dispersed ownership, self-sovereign identification, and cross-border data interchange, challenging this conventional approach. Blockchain records are still not legally recognised as official or admissible evidence in many countries, which leaves their use in public record-keeping legally unclear.

Additionally, data controllers must handle data deletion, consent tracking, and auditability in accordance with privacy laws like the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023—functions that are challenging to integrate with immutable blockchain structures.

The lack of explicit cybersecurity regulations, data governance guidelines, and standard operating procedures (SOPs) for decentralised systems may impede inter-agency interoperability, discourage adoption, and result in legal liability.

8. Concluding remarks and suggestions

The incorporation of decentralised technologies, particularly blockchain and edge computing, represents a substantial advancement in the planning and provision of public digital services. These technologies provide a paradigm change from conventional centralised cloud-based e-governance systems, which, while good at standardisation and scalability, sometimes have issues with latency, accessibility in distant locations, system resilience, and public confidence.

By bringing computer resources closer to the end user, edge computing solves the crucial problem of network and geographic constraints. Local processing lowers latency, improves real-time service performance, and guarantees continuity even in offline or low-bandwidth scenarios. This methodology makes sure that vital services like health records, identification verification, and welfare distribution are available to underprivileged and rural populations where dependable internet connectivity may be erratic.

In the meanwhile, blockchain technology adds an immutability and transparency layer that is crucial for fostering confidence in public governance. Blockchain improves accountability, deters data manipulation, and gives individuals verifiable records of their contacts with the government by logging every citizen interaction and government transaction in a tamper-proof ledger. This is especially helpful in situations where public confidence has traditionally been damaged by bureaucratic opacity and corruption.

Decentralised approaches improve system resilience in contrast to monolithic centralised infrastructures, which constitute a single point of failure. Blockchain records may be restored from different places, and edge nodes can continue operating independently in the case of hardware failures, natural catastrophes, or cyberattacks, guaranteeing data integrity and continuous service delivery.

Important Suggestions:

1. Test Decentralised Deployments in Areas with High Needs

Pilot projects should be started by governments in underserved, rural, or disaster-prone areas where integrating edge and blockchain technology would have the most positive social effects. Use cases might include monitoring vaccinations, managing property records, or resolving local grievances.

2. Decentralisation Policy and Regulatory Frameworks

Laws must change to accommodate blockchain-based digital signatures, decentralised data storage, and identification frameworks that operate with distributed systems. Policies for interoperability and data protection should be well-defined.

3. Partnerships between the public, private, and community (PPCPs)

Government agencies, IT companies, and local communities working together may guarantee context-sensitive service models, speed up implementation, and lower infrastructure costs. Additionally, communities need to be active in blockchain validation and edge node governance.

4. Create Standards for National Edge Infrastructure

Compatibility, scalability, and resilience across countries may be guaranteed by establishing technical and operational standards for the deployment of edge nodes, with respect to power efficiency, security, storage, and connection.

5. Campaigns for Citizen Digital Literacy and Trust

It is essential to raise awareness of the advantages of decentralised platforms. Users should be able to engage with digital public services with confidence after completing training programs and learning about the security and use of personal data.

6. Ongoing Auditing and Monitoring

Use blockchain-based auditing tools and smart contracts to automatically track service delivery KPIs (key performance indicators), identify irregularities, and generate transparency reports in real time.

References

Ali, O., Shrestha, A., & Soar, J. (2018). **A framework for cloud computing adoption for e-government implementation**. *Information Systems Frontiers, 20*(3), 531–555. https://doi.org/10.1007/s10796-016-9689-6

Azbeg, K., & El Boukili, Y. (2020). **Towards a blockchain-based e-Government model: A comparative analysis of Estonia and Dubai**. *Procedia Computer Science, 177*, 516–523. https://doi.org/10.1016/j.procs.2020.10.073

Kshetri, N. (2021). **1 Blockchain and E-Government: Applications and Challenges**. *Journal of International Affairs, 74*(1), 101–120.

Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2020). **Blockchain and IoT-based data transparency architecture for e-government**. *Future Generation Computer Systems, 106*, 441–451. https://doi.org/10.1016/j.future.2019.12.040

MeitY (Ministry of Electronics and Information Technology, Government of India). (2023). *India Stack: Open Digital Ecosystem for Public Services*. https://www.meity.gov.in/

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). **Edge computing: Vision and challenges**. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

Tapscott, D., & Tapscott, A. (2016). **Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world**. Penguin.

United Nations Department of Economic and Social Affairs. (2022). *United Nations E-Government Survey 2022: The Future of Digital Government*. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022

Zyskind, G., Nathan, O., & Pentland, A. (2015). **Decentralizing privacy: Using blockchain to protect personal data**. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27