International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1(2), 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

Design and Implementation of a Multi-Authority E-Governance Framework for Secure Digital Certificate Management

S. Laxmi Lalitha[1], Siddhartha Nelakanti[2], Thippani Varsha[2], Regalla Raj Kumar[2], Velpula Charan[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (Data Science)

[1,2]Vaagdevi College of Engineering (UGC-Autonomous), Bollikunta, Warangal, 506005, Telangana

Abstract

In the contemporary digital era, transitioning government services toward automated solutions is essential for enhancing efficiency, transparency, and public accessibility. Traditional certificate issuance systems remain predominantly manual and paper-based, leading to administrative bottlenecks, security vulnerabilities, and prolonged processing times. This paper proposes a robust multi-authority e-governance framework designed to digitize and streamline the certification lifecycle. The system employs a centralized, role-based web architecture that facilitates seamless interaction between citizens, medical authorities, revenue officials, and system administrators. By integrating a Django-based backend with a MySQL relational database, the framework automates application submission, domain-specific verification, and secure document issuance. Security is bolstered through OTP-based multi-factor authentication and SMTP-enabled communication channels to ensure data integrity and accountability. Comparative analysis suggests that this digital framework significantly reduces procedural delays and manual workloads while enhancing scalability and public trust. The proposed system establishes a sustainable foundation for future decentralized digital governance initiatives.

Keywords: E-governance, digital certificate management system, automated certificate issuance, role-based access control, OTP authentication.

Received: 06-02-2026 Accepted: 13-03-2026 Published: 20-03-2026

1. Introduction

In recent years, digital technologies have changed the way governments communicate and provide services to citizens. E-government initiatives aim to improve the accessibility, efficiency, and transparency of public services. A key part of this development is the increasing use of artificial intelligence (AI) in the public sector.

Fig. 1: E-governance framework: A digital transformation.

Today, governments are increasingly deploying AI tools such as virtual assistants and chatbots to guide citizens through online procedures, including document processing systems for handling applications and licenses, fraud detection in tax and welfare services, predictive models for public health and city planning, and recommender systems that suggest services based on user needs by assisting us in navigating complex administrative procedures by directing them to relevant forms, services, or regulations. Collectively, these applications are transforming citizen–government interactions by enabling more responsive, data-driven, and cost-effective service delivery. However, the success of these technologies depends not only on their technical capability but also on whether citizens are willing to use them. Research in the field of e-government has shown that digital services are more likely to succeed when citizens trust them and find them useful and easy to use.

More recently, studies confirm that citizen trust in AI-enabled government systems is influenced by ethical robustness and context-based trust transfer mechanisms. The Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) both highlight the importance of these factors. Other studies also stress that the clarity of information and the transparency of how systems work are important for building trust and encouraging citizens to adopt these services. In the case of AI-based tools, this is even more important. Users frequently express apprehensions regarding fairness, data privacy, and the use of complex “black-box” algorithms. For this reason, citizen attitudes shaped by trust, perceived usefulness, risk, digital skills, and beliefs about fairness have become a key topic in discussions about responsible and inclusive use of AI in government.

2. Literature Survey

Goloshchapova et al. [1] proposed the role of e-government in relation to economic development within the post-COVID era. Nowadays, e-government represents the service which utilizes digital technology to create electronic pathways to improve the efficiency of public services, increase economic prosperity, and improve the standard of living. In this paper, we argue that e-government presents the only proper and viable model for public administration in the 21st century by embedding internet-based technologies to ensure smooth interactions between the government and its citizens, solving the most socially important problems, enabling internal communication between public servants, and delivering public services to the entire population regardless of age or gender. In [2], the first key is to use digital tools to make information within the organization more accessible, which more than doubles the likelihood of a successful transformation. The second is the introduction of digital self-service technology for use by employees, business partners, or both. When organizations do this, the likelihood of a successful transformation double. Tjahja et al. [3] examined how individual participants identify themselves within the framework of the Internet Governance Forum and how they

understand the internet governance ecosystem, based on the list of participants in the Public Internet Governance Forum, opening up a new path for further research on the legitimacy of multiple stakeholders.

Saravistha et al. [4] discussed the issue of optimizing consumer protection in the context of new forms of contracts, where standard digital contracts and new cross-border market mechanisms coexisted in the business world to better protect consumer privacy. Fu, X.; Zhang et al [5] propose the increasing frequency of digital economic activities on a global scale, internet governance has become a pressing issue. Traditional multilateral approaches to formulating internet governance rules have struggled to address critical challenges such as privacy leakage and low global internet defence capabilities. To tackle these issues, this study integrates SAR data processing and interpretation using AI techniques with the development of governance rules through international agreements and multi-stakeholder mechanisms. This approach aims to strengthen privacy protection and enhance the overall effectiveness of internet governance. In [6], the rural digital governance platform is closely related to rural sustainable development. By playing the role of the rural digital governance platform, it can optimize the allocation of rural resources, improve the efficiency of rural governance, promote the development of rural industries, improve the quality of life of rural residents, promote the inheritance and innovation of rural culture, and provide a strong guarantee for the sustainable development of rural areas. Bellini et al. [7] argued that the widespread adoption of technologies shows a natural bias towards growing cities, as the technologies used for promoting urban growth lack appropriate urbanization processes. If a solution to this challenge remains elusive, the technology can experience a transformation and become "censored", thereby exerting control and control over urban stakeholders.

Seunghwan Myeong et al. [8] This study examined the inherent complexity associated with institutional and technological innovation in the context of smart cities. The capability of a municipality to cultivate innovation is significantly dependent on the implementation of its technological infrastructure and institutional competence. Montree Thirasakthana et al. [9] This paper aims to propose that the sustainable government enterprise architecture framework specifically applies for the national strategic planning in the optimum exercise process and clarity guidance for the information technology organization being able to transform and improve their services for an achievable adaptation efficiency, simplification, cost management, collaboration, shareability, and standardization which accommodate the rapidly changing service usability on digitalization known as "e-Government." Zamora et al. [10] characterize "digital governance" as the extensive adoption of ICT by governments to enhance public services, increase transparency and accountability, and improve the quality of public administration. In China, research in this field can be attributed to early studies conducted by Xu Xiaolin and others. They distinguish between a broader interpretation of digital governance, referring to IT-enabled integrated resource management, and a narrower definition concerning the use of democratic tools to streamline government functions and processes**.**

3. Proposed System

The proposed Django-based multi-authority e-governance framework as shown in Fig. 2 designed to automate the application, verification, approval, and issuance of various government certificates such as Birth, Death, Income, and Community certificates. It provides a secure web portal where multiple roles such as users, hospital officials, revenue officers, and administrators interact to ensure

smooth processing and management of certificates.

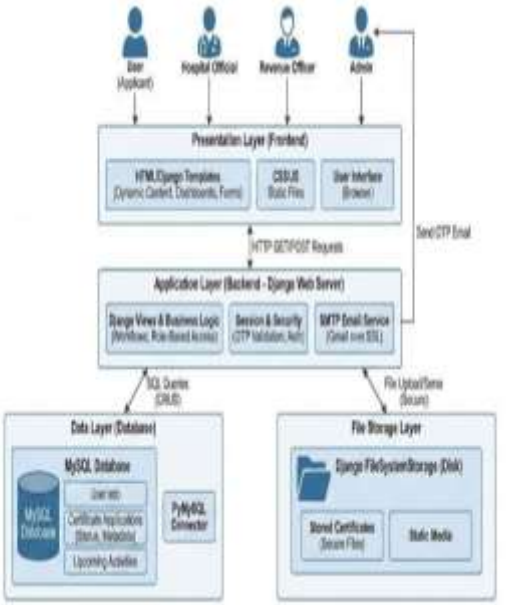

Fig. 2: Proposed system architecture of multi-authority e-governance framework.

The main features of proposed web application are as follows:

- **Multi-Role System:** The project distinguishes user roles with separate login pages and tailored dashboards. Users apply for certificates, hospital and revenue officials verify and approve applications, and administrators manage certificate uploads.
- **Certificate Workflow Automation:** Users submit certificate applications, which are checked for duplicates and tracked for status updates. Officials approve or reject applications based on the certificate type. Approved certificates are uploaded by admins and made available for secure download by users.
- **Security Features:** Downloads are protected by an OTP sent via email, ensuring only authorized users access their certificates. The system maintains audit trails of approval statuses and upload history.
- **Database Integration:** The system uses MySQL to store user data, applications, certificate statuses, and activity records, queried dynamically to provide real-time user and admin views.
- **User Interaction:** Users can sign up, log in, view application statuses, apply for new certificates, and securely download approved certificates. Admins can add upcoming activities/events relevant to users.
- **File Management:** Certificates are stored as files on the server with management for overwrites and deletions to handle updates efficiently.

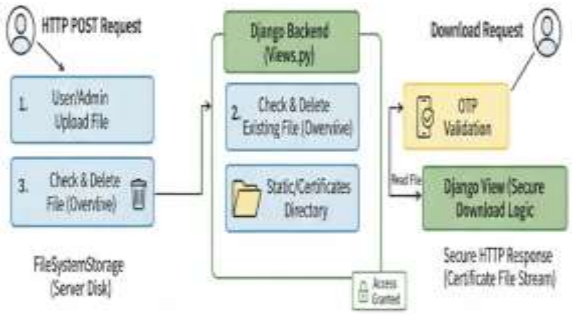

Fig. 3: Secure file handling and downloads.

Role-Based Access and Authentication

Role-based access control ensures that users, admins, hospital officials, and revenue officers have access only to the functions pertinent to their role. It strengthens security and operational boundaries by separating privileges. The internal operational flow is as follows:

- Separate login views and forms capture credentials for each user type.
- The backend verifies inputs against stored credentials (manual

verification, not Django's default auth).

- Post-login, users are redirected to role-specific dashboards.
- Each role views filtered data and performs authorized activities (e.g., hospitals verify birth certificates).
- Session or global variable (uname) tracks the logged-in user context internally for request handling.

File Management Using Django FileSystemStorage

Handling digital certificate files securely and efficiently is critical. Django's FileSystemStorage provides an abstraction to upload, save, overwrite, and serve files from a designated directory on the server. Fig. 3 demonstrates the working of secure file handling and downloads.

OTP Generation and Email Verification

To enhance download security, the system uses One-Time Passwords (OTP) for validating user identity before allowing certificate downloads. OTPs are digitally sent to users registered email addresses. Fig. 4 illustrates sequence diagram of certificate authentication download and its internal working flow is as follows:

- When a download is requested, a random 4-digit OTP is generated.
- The backend retrieves the user's email from the database.
- SMTP (Gmail SMTP over SSL) is used to send an email containing the OTP.
- Users enter the OTP on the website; the backend matches it against the stored value.
- If matched, the certificate file is served for download; otherwise, an error prompts retrying.

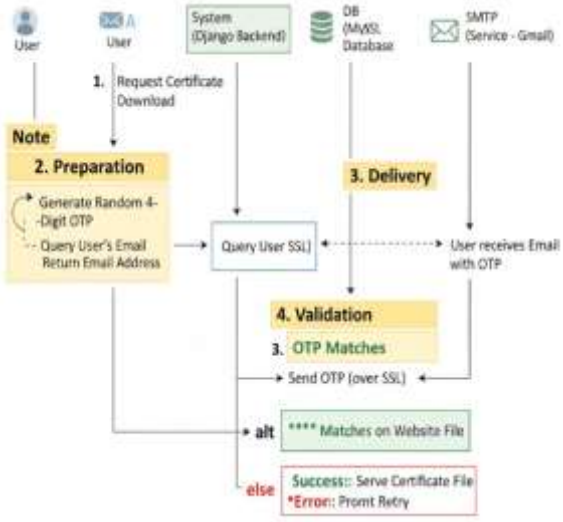

Fig. 4: Sequence diagram of certificate authentication download.

4. Results Description

In Fig. 5, users can select the certificate type and provide necessary information to submit an application. This feature is strictly user-only, with eligibility checking to prevent multiple duplicate applications. In Fig. 6, the users track the progress of their applications. Status updates are role-triggered based on approval or rejection by respective verification authorities. Fig. 7 shows the dashboard for hospital officials' post-login. Hospital role limitations ensure officials only access birth and death certificate verifications, excluding other certificate types.

In Fig. 8, hospital officials view pending requests relevant to their role. They can perform verifications and update application statuses accordingly. In Fig. 9, the hospital authority validates certificate details and approves genuine applications, enforcing role-driven workflow control. In Fig. 10, following hospital approval and admin upload, the user's status updates to "Approved," enabling download options visible only to the user role. Fig. 11 demonstrate the security checkpoint

International Journal of Engineering Research and Science & Technology

where the user must enter an OTP received via email to securely download the certificate, ensuring user identity verification and preventing unauthorized access.

Fig. 5: Apply certificate page showing the selection certificate type and description.

Fig. 6: Status page after applying for certificate.

Fig. 7: Welcome page for the hospital after a successful login.

Fig. 8: Illustration of certificate request by hospital authority.

Fig. 9: Approving the details as genuine from hospital authority.

Fig. 10: Updation of user view status as approved and showing the certificate download option.

International Journal of Engineering Research and Science & Technology

Fig. 11: OTP authentication page after clicking on download the OTP received to the email.

Fig. 12 demonstrates multi-certificate application capability within user role constraints. In Fig. 13 is the revenue official dashboard, limiting access to income and community certificate requests according to their jurisdiction.

Fig. 12: Applying for another sample certificate from user 2 access.

Fig. 13: Rejecting the details as its fake by revenue department authority.

5. Conclusion

The proposed multi-authority e-governance framework is a crucial advancement in public administration, streamlining the traditionally manual and error-prone process of certificate issuance, verification, and download through automation and secure web technologies. By integrating role-based access, online application processing, real-time status tracking, and OTP-secured certificate delivery, the system enhances transparency, efficiency, and user convenience. It bridges gaps between citizens and government entities such as hospitals and revenue officials, ensuring that each certificate type follows a proper verification workflow under authorized supervision. The adoption of Python 3.7.6 and Django framework provides a stable, scalable, and modular foundation, while MySQL and SMTP services support robust data management and secure communications. This system addresses challenges in accessibility, security, and process delays by reducing manual intervention, thereby mitigating risks of data loss, fraud, and unauthorized access. It promotes digital governance with improved record keeping, resource optimization, and user engagement through well-designed dashboards and activity notifications. Overall, the solution leads to accelerated government

service delivery, fostering public trust and regulatory compliance.

REFERENCES

[1]. Goloshchapova, T.; Yamashev, V.; Skornichenko, N.; Strielkowski, W. E-Government as a Key to the Economic Prosperity and Sustainable Development in the Post-COVID Era. *Economies* **2023**, *11*, 112. https://doi.org/10.3390/economies11040112.

[2]. Hakanen, Jari J., Annina Ropponen, Wilmar B. Schaufeli, and Hans De Witte. 2019. Who is engaged at work? A large-scale study in 30 European countries. *Journal of Occupational and Environmental Medicine* 61: 373–81.

[3]. Tjahja, N.; Trisha, M.; Jamal, S. Who do you think you are? Individual stakeholder identification and mobility at the Internet Governance Forum. *Telecommun. Policy* **2022**, *46*, 102410–102411.

[4]. Saravistha, D.B.; Sukadana, I.K.; Suryana, K.D. Urgency of Contract Model Settings in the Global Digital Market Related to Tourism Business: A Study on Consumer Protection and Electronic Information and Transactions. *Bp. Int. Res. Crit. Inst.-J. BIRCI-J.* **2022**, *5*, 4549–4556.

[5]. Fu, X.; Zhang, W.; Li, Z. Internet Governance in the Context of Global Digital Contracts: Integrating SAR Data Processing and AI Techniques for Standards, Rules, and Practical Paths. *Information* **2025**, *16*, 697. https://doi.org/10.3390/info16080697

[6]. Zhang, B.; Xiong, W.; Yin, J.; Zhang, P.; Liu, B. How to Form the Rural Digital Governance Platform Under the Framework of Mixed-Scanning–Multiple Streams Based on an Empirical Investigation of the Platform of "JuHaoban" in Julu County, Hebei Province. *Sustainability* **2025**, *17*, 2517. https://doi.org/10.3390/su17062517

[7]. Bellini, P.; Nesi, P.; Pantaleo, G. IoT-enabled smart cities: A review of concepts, frameworks and key technologies. *Appl. Sci.* **2022**, *12*, 1607.

[8]. Seunghwan Myeong, S.; Bokhari, S.A.A. Building Participative E-Governance in Smart Cities: Moderating Role of Institutional and Technological Innovation. *Sustainability* **2023**, *15*, 15075. https://doi.org/10.3390/su152015075

[9]. Montree Thirasakthana, M., & Kiattisin, S. (2021). Sustainable Government Enterprise Architecture Framework. *Sustainability*, *13*(2), 879. https://doi.org/10.3390/su13020879

[10]. Zamora, D.; Barahona, J.C.; Palaco, I. Case: Digital Governance Office. *J. Bus. Res.* **2016**, *69*, 4484–4488.

[11]. Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. American Journal of AI Cyber Computing Management, 5(3), 85–93. https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93

[12]. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615

[13]. Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines. (2025). Inaternational Journal of Communication Networks and Information Security, 16(4). https://doi.org/10.48047/ijcnis.16.4.2111