IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

Doc-Vault: Document Locker For Institutes

Rushikesh Girase[1], Yash Vasaikar[2], Ayush Patil[3], Saurabh Girase[4], Prof. S. R. Palkar[5]
Department of Computer Engineering
Kalyani Charitable Trust's Late Gambhirrao Natuba Sapkal College of Engineering, Nashik, India

Abstract: *The Institutional Document Management Platform is a web-based system designed to simplify the collection, verification, review, and management of student documents in an educational institution. Traditional document submission processes are often manual, time-consuming, and difficult to monitor, especially when multiple students, staff members, and administrators are involved. This project provides a centralized digital platform where students can register, verify their email, upload required academic and identity documents, view document status, and receive notifications. Staff members can review uploaded documents, approve or reject submissions with remarks, request additional documents, and track student records. Administrators can manage staff accounts, monitor uploaded documents, view audit logs, and supervise the complete document workflow. The system uses Angular for the frontend, Spring Boot for the backend, MySQL for database management, JWT-based authentication for security, and email verification for user validation. By integrating role-based access control, document versioning, notifications, and audit logging, the platform improves transparency, reduces paperwork, and makes institutional document handling more efficient and reliable.*

Keywords: Institutional Document Management, Student Document Verification, Angular, Spring Boot, MySQL, JWT Authentication,

I. INTRODUCTION

Educational institutions handle a large number of student documents such as Aadhaar cards, domicile certificates, income certificates, mark sheets, admission receipts, caste certificates, and other academic or government-related documents. Managing these documents manually can lead to delays, misplaced files, lack of transparency, and difficulty in tracking approval status. Students may not know which documents are pending, staff may find it difficult to review submissions systematically, and administrators may lack a clear overview of the entire process.The proposed Institutional Document Management Platform addresses these problems by offering a centralized digital solution. The system allows students to create accounts, verify their email addresses, upload documents, preview or download submitted files, and receive status updates. Staff members can view students from their assigned college, review submitted documents, approve or reject them, and send requests for additional documents. Administrators can register staff members, block or delete staff accounts, monitor document activity, and view audit logs for system transparency.The project follows a full-stack architecture. The frontend is developed using Angular, which provides separate dashboards for students, staff, and administrators. The backend is implemented using Spring Boot with REST APIs. MySQL is used for persistent storage of users, documents, reviews, notifications, and audit logs. Security is handled through Spring Security and JWT tokens, ensuring that only authorized users can access specific features according to their roles.The main objective of this project is to reduce manual effort, improve document tracking, and provide a secure and organized workflow for institutional document verification.

II. LITERATURE SURVEY

Several researchers have studied digital document management, secure storage, access control, and smart campus systems. These studies provide a strong foundation for the proposed Institutional Document Management Platform.Chernyshenko and Chernyshenko proposed a university digital document management approach using graph theory and optimization techniques. Their work focuses on improving university information systems by reducing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

unnecessary document flow and optimizing the placement of education data warehouses. The study shows that digital document systems can improve storage, access speed, and business process efficiency in universities. This research is useful for the proposed project because it highlights the importance of structured document flow and centralized data handling in educational institutions.Baban and Mokhtar presented an Online Document Management System for Academic Institutes. Their study explains that academic institutes generate large numbers of electronic documents, and users often face difficulty in storing, retrieving, and sharing them efficiently. The paper emphasizes document classification, hierarchy-based organization, quick retrieval, access control, and knowledge sharing among students. This work directly relates to the proposed project, as the Institutional Document Management Platform also aims to replace manual document handling with a centralized online system for students, staff, and administrators.Li et al. discussed secure sharing of personal health records in cloud computing using Attribute-Based Encryption. Although their work focuses on healthcare records, it is highly relevant because it addresses privacy, fine-grained access control, user revocation, and secure data sharing in a multi-user environment. The paper shows that sensitive records should be protected using strong access policies. This idea supports the need for role-based access control in the proposed system, where students, staff, and administrators must have different permissions.Babitha and Remesh Babu proposed secure cloud storage using AES encryption. Their work explains the importance of authentication, authorization, confidentiality, and encryption before storing sensitive data in cloud environments. The study concludes that AES is faster and more secure compared with some traditional encryption techniques. This research is relevant to the proposed platform because student documents such as Aadhaar cards, certificates, and mark sheets are sensitive and must be protected from unauthorized access.Zhou, Varadharajan, and Hitchens proposed a secure Role-Based Access Control model on encrypted cloud data. Their research combines role-based access control with encryption so that users can access data only according to their assigned roles. The study is important for systems where different users require different levels of access. This directly supports the role structure of the proposed project, where students can upload and view their own documents, staff can review documents, and administrators can manage the overall system.

III. PROPOSED METHODOLOGY

A. System Architecture

The proposed system, Institutional Document Management Platform, follows a three-tier architecture consisting of the presentation layer, application layer, and database layer. This architecture provides clear separation between user interface, business logic, and data storage.The presentation layer is developed using Angular. It provides separate dashboards for three types of users: Student, Staff, and Admin. Students can register, verify email, upload documents, view document status, download or preview documents, and receive notifications. Staff members can view assigned students, check uploaded documents, approve or reject documents with remarks, and request additional documents. Administrators can manage staff, monitor all documents, view students, and access audit logs.The application layer is implemented using Spring Boot. It handles authentication, authorization, document processing, notification generation, audit logging, and communication between frontend and database. REST APIs are used to connect the Angular frontend with the Spring Boot backend. Spring Security and JWT are used to provide secure login and role-based access control.

The database layer uses MySQL for storing user details, document metadata, review records, notifications, and audit logs. Uploaded files are stored in the server file storage, while their details such as file name, title, status, version, upload date, and student ID are stored in the database.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

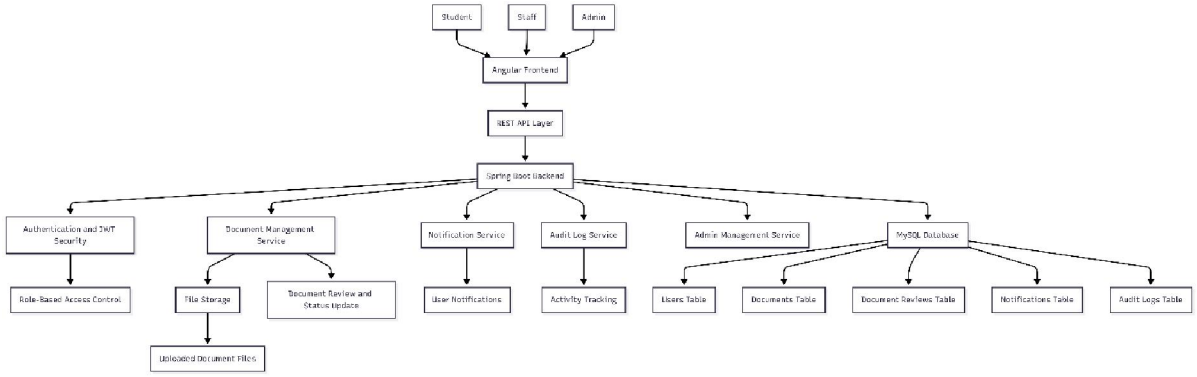

Figure 1 System Architecture

B. State Space Design

The state space design of the proposed Institutional Document Management Platform represents the different states through which users, documents, and system processes pass during execution. The system mainly includes three user roles: Student, Staff, and Admin. Each role has different permissions and moves through different operational states.For a **student**, the process begins with registration. After registration, the student account remains in an unverified state until email verification is completed. Once verified, the student can log in, update profile details, upload required documents, view document status, preview or download uploaded files, and receive notifications. A student document may remain in pending, approved, or rejected state depending on staff review.For a **staff member**, the process begins with admin-created account access. After login, staff can view students, check uploaded documents, filter pending documents, review submissions, approve or reject documents, and send remarks. Staff can also request additional documents from students and receive notifications when students upload or update documents.For an **administrator**, the state space includes login, staff registration, staff update, staff blocking or deletion, student monitoring, document monitoring, notification viewing, and audit log checking. Admin has the highest level of control and can supervise the overall document verification process.

C. Action Space

The action space of the proposed Institutional Document Management Platform defines all possible actions that can be performed by different users and system components. Since the system is role-based, each user role has a specific set of permitted actions according to its responsibility.For the Student, the available actions include registration, email verification, login, profile update, document upload, document preview, document download, document deletion, checking missing documents, viewing document status, reading notifications, and logout. These actions allow students to manage their own academic and personal document records digitally.For the Staff, the action space includes login, viewing student records, viewing uploaded documents, searching students, filtering documents by status, previewing or downloading documents, approving documents, rejecting documents, adding review remarks, requesting additional documents from students, marking notifications as read, and logout. Staff actions mainly focus on document verification and student document monitoring.For the Admin, the possible actions include login, registering staff members, viewing staff records, updating staff information, blocking or unblocking staff accounts, deleting staff accounts, viewing students, viewing all uploaded documents, previewing or downloading documents, requesting documents from students, viewing notifications, checking audit logs, and logout. Admin actions are designed for system supervision and institutional control.The system also performs several automatic actions in the background. These include generating JWT tokens after successful login, validating user roles before allowing access, storing uploaded files, saving document metadata, updating document status, creating notifications after upload or review, sending email verification links, and recording important activities in audit logs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

D. Reward Function

The reward function defines how the proposed system evaluates successful and unsuccessful operations during document management. In the Institutional Document Management Platform, the reward function is not used as a mathematical reinforcement learning model, but as a logical evaluation mechanism to measure whether each system action improves efficiency, security, accuracy, and user satisfaction.A positive reward is assigned when the system performs an action that supports the main objective of secure and efficient document management. For example, successful student registration, email verification, document upload, staff review, document approval, notification generation, and audit log creation are considered positive outcomes. These actions improve transparency and reduce manual work.

A negative reward is assigned when an action fails or violates system rules. Examples include invalid login, unverified email login attempt, unauthorized document access, duplicate email or roll number registration, failed file upload, invalid document review, or access by a user without the required role. Such actions reduce system reliability and must be prevented by authentication, validation, and role-based access control.

E. Training Pipeline

In the proposed Institutional Document Management Platform, the training pipeline can be considered as the step-by-step process through which the system is configured, tested, and improved to handle real institutional document workflows. Since this project is mainly a web-based document management system and not a machine learning model, the training pipeline refers to workflow preparation, data validation, role configuration, and system testing.

The first step is data preparation. In this stage, required user roles such as Student, Staff, and Admin are defined. Common document categories such as Aadhaar Card, Domicile Certificate, Income Certificate, SSC, HSC, Previous Year Mark Sheet, Admission Receipt, Ration Card, Undertaking, Caste Certificate, and Non-Creamy Layer Certificate are identified. These document categories help the system check whether students have uploaded the required documents.The second step is user role configuration. The admin account is created first. Admin can then create staff accounts and assign them to a particular college or course. Students register themselves through the registration form and verify their email before accessing the dashboard. This step prepares the system for role-based operation.The third step is workflow execution. Students upload documents through the Angular frontend. The uploaded files are sent to the Spring Boot backend through REST APIs. The backend stores the files, saves metadata in the MySQL database, assigns the document status as pending, and generates notifications for staff.

F. Evaluation Protocol

The evaluation protocol defines how the proposed Institutional Document Management Platform is tested and measured to ensure that it works correctly, securely, and efficiently. The system is evaluated based on functional correctness, security, usability, performance, and reliabilityThe first evaluation criterion is functional testing. In this stage, all major modules are tested separately. Student registration, email verification, login, profile update, document upload, document preview, document download, document deletion, staff review, admin staff management, notification generation, and audit log creation are checked. Each function is tested with valid and invalid inputs to confirm proper system behavior.

The second criterion is role-based access testing. The system has three roles: Student, Staff, and Admin. Each role must access only its permitted features. A student should access only personal documents, staff should review documents of assigned students, and admin should manage staff and monitor all records. Unauthorized access attempts are tested to verify the effectiveness of JWT authentication and Spring Security.The third criterion is document workflow testing. The complete document lifecycle is evaluated from upload to review. A document should move from uploaded state to pending review, then to approved or rejected state. If rejected, the student should be able to upload a corrected document. The system should correctly store document metadata, status, version, upload date, and review remarks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed Institutional Document Management Platform was developed and tested in a local development environment. The system uses a full-stack architecture consisting of an Angular frontend, Spring Boot backend, and MySQL database. The experimental setup was prepared to verify document upload, role-based access, document review, notification generation, and audit log tracking.The frontend was implemented using Angular 17, which provides separate dashboards for Student, Staff, and Admin users. The Angular application communicates with the backend through REST APIs. The backend was developed using Spring Boot 3.2.4 with Java 17. Spring Security and JWT were used for authentication and authorization. MySQL was used as the database for storing user records, document metadata, review details, notifications, and audit logs.Uploaded documents were stored in server-side file storage, while related metadata such as document title, original file name, stored file name, content type, size, upload date, version, and status were stored in the database. Email verification was configured using SMTP service to validate student accounts before login.The system was tested using three types of users: Student, Staff, and Admin. Test cases were created for student registration, email verification, login, document upload, document preview/download, staff document review, admin staff management, notification display, and audit log monitoring.

B. Expected Behavioural Outcomes

The proposed Institutional Document Management Platform is expected to improve the overall document submission, verification, and monitoring process in an academic institution. The expected behavioural outcomes describe how the system should behave for students, staff, administrators, and backend services during normal operation.For students, the system is expected to provide a simple and secure way to register, verify email, log in, upload documents, and track document status. After uploading a document, the student should immediately see the document listed in the dashboard with a pending status. Once staff reviews the document, the status should change to approved or rejected, and the student should receive a notification with review remarks. If a document is rejected, the student should be able to upload a corrected version.For staff members, the system is expected to display student records and uploaded documents according to access permissions. Staff should be able to search students, filter documents by status, preview or download submitted files, and review each document by approving or rejecting it with remarks. After review, the system should automatically update the document status and notify the student.For administrators, the system is expected to provide complete supervision of the platform. Admin should be able to register staff members, update staff details, block or unblock staff accounts, delete staff accounts, view students, monitor uploaded documents, request additional documents, view notifications, and check audit logs. Admin actions should be reflected immediately in the system.For the security mechanism, the system is expected to allow access only after successful authentication. JWT tokens should be generated after login and used for secure API communication. Role-based access control should prevent students, staff, or admins from accessing unauthorized features. Unverified students should not be allowed to log in until email verification is completed.

For the document workflow, the system is expected to maintain a clear lifecycle: document upload, pending review, approval or rejection, notification, and re-upload if required. Uploaded files should be stored securely, while document metadata should be maintained in the database.

C. Offline Bootstrapping Convergence

In the proposed Institutional Document Management Platform, offline bootstrapping convergence refers to the initial preparation and stabilization of the system before it is used in a real institutional environment. Since the system is not a machine learning model, convergence here represents the point at which all predefined roles, workflows, database records, document categories, and access rules become stable and ready for online operation.During offline bootstrapping, the system is first configured with basic institutional data such as user roles, admin account, college names, courses, class levels, caste categories, and required document categories. The backend database is initialized

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

using MySQL, and required tables such as users, documents, document reviews, notifications, and audit logs are created. The admin user can then create staff accounts, and students can register through the frontend.The convergence process is achieved when the system correctly performs the core workflow without runtime dependency on manual setup. This includes successful user authentication, role-based dashboard redirection, document upload, file storage, metadata storage, notification creation, document review, and audit log generation.

D. Discussion

The proposed Institutional Document Management Platform provides a structured and secure solution for managing student documents in academic institutions. The system addresses the limitations of traditional manual document handling, where students submit physical copies, staff manually verify them, and administrators face difficulty in tracking the overall process. By converting this workflow into a digital platform, the system improves speed, transparency, accessibility, and accountability.The role-based structure is one of the major strengths of the system. Students, staff, and administrators are given separate dashboards and permissions according to their responsibilities. Students can upload and manage their own documents, staff can review and approve or reject documents, and administrators can supervise the complete process. This reduces confusion and prevents unauthorized access to sensitive records.The document workflow also improves institutional efficiency. Each uploaded document is stored with metadata such as title, file name, upload date, status, version, and student details. Staff can review the document and provide remarks. If a document is rejected, the student can upload a corrected version. This creates a clear feedback loop between students and staff.Security is another important aspect of the proposed system. JWT authentication, password encryption, email verification, and role-based access control help protect user accounts and documents. Since student documents may contain personal and academic information, controlled access is necessary. The system ensures that users can access only the features and records allowed by their role.The notification and audit log modules increase transparency. Notifications inform users about document uploads, reviews, and additional document requests. Audit logs record important actions such as upload, review, deletion, and staff management. This makes the system more accountable and helps administrators monitor activity.

V. CONCLUSION

The Institutional Document Management Platform provides an effective digital solution for managing student documents in academic institutions. The system reduces the limitations of manual document handling by allowing students to upload documents online, staff members to review and verify them, and administrators to monitor the complete workflow from a centralized dashboard.The proposed system uses Angular for the frontend, Spring Boot for backend services, and MySQL for database storage. Security is maintained through JWT authentication, email verification, password encryption, and role-based access control. The platform also includes document status tracking, notifications, review remarks, and audit logs, which improve transparency and accountability.The system supports three major roles: Student, Staff, and Admin. Students can register, verify email, upload documents, view status, and receive notifications. Staff can review documents, approve or reject them, and request additional documents. Admin can manage staff, monitor students, view documents, and check audit logs.From the implementation and expected outcomes, it can be concluded that the proposed platform improves document submission, verification, storage, and monitoring. It saves time, reduces paperwork, prevents unauthorized access, and provides a structured workflow for institutional document management. In future, the system can be enhanced with cloud storage, AES encryption, OCR-based document validation, digital signatures, and automated authenticity checking.

REFERENCES

1. B. I. Onyeashie, P. Leimich, S. McKeown, and G. Russell, “Secure Evidence Management Through TDAG-Based Digital Twin Architecture: A Smart Locker System for Tamper-Evident Chain of Custody,” in Proc.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

2025 IEEE International Conference on Communications Workshops (ICC Workshops), 2025, pp. 627–633, doi: 10.1109/ICCWorkshops67674.2025.11162354.

2. Y. Wu, M. Dong, H. Yang, Y. Huang, X. Huang, G. Chen, and S. Bi, "A Design of Smart Locker System Based on IoT for Campus," in Proc. 2023 IEEE 13th International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), 2023, pp. 1287–1291, doi: 10.1109/CYBER59472.2023.10256600.
3. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013, doi: 10.1109/TIFS.2013.2286456.
4. L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud," The Computer Journal, vol. 54, no. 10, pp. 1675–1687, Oct. 2011, doi: 10.1093/comjnl/bxr080.
5. M. P. Babitha and K. R. Remesh Babu, "Secure Cloud Storage Using AES Encryption," in Proc. 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, doi: 10.1109/ICACDOT.2016.7877709.
6. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, Jan. 2013, doi: 10.1109/TPDS.2012.97.
7. H. Baban and S. Mokhtar, "Online Document Management System for Academic Institutes," in Proc. 2010 3rd International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 4, 2010, pp. 315–319, doi: 10.1109/ICIII.2010.555.
8. S. Chernyshenko and V. Chernyshenko, "University Digital Document Management and Optimal Strategy of Education Data Warehouses' Placement," in Proc. 2022 2nd International Conference on Technology Enhanced Learning in Higher Education (TELE), 2022, pp. 237–243, doi: 10.1109/TELE55498.2022.9801018.