iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75095

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

DIGISEWA: A Blockchain Based Digital License and Registration System

Ashish Trivedi[1], Sejal Bhagat[2], Sejal Wagdre[3], Shruti Chedge[4], Sumit Chaple[5], Tejas Harne[6]
[1]*Assistant Professor,* [2, 3, 4, 5, 6]*VII Semester, Department of Computer Science and Engineering GH Raisoni University, Amravati Nagpur, MH, India*

Abstract: ***Traditional licensing systems involve multiple departments and rely on manual paperwork, leading to delays, lackoftransparency[1],[7],andrisksoffraud.This project proposes a Blockchain-Based Digital License and Registration System using Ethereum smart contracts and Inter Planetary File System (IPFS) [4], [5], [14] to provide a secure, decentralized, and tamper-proof solution. The system ensures authenticity through blockchain-verified documents, role-based access for departments, and immutable audittrails[6],[7]forallactions. Key components include a user portal for applications, departmentaldashboardsforapprovals,andanadmindashboard for oversight.***

Smart contracts automate workflows, while encrypted document storageonIPFSguaranteesdataintegrityandavailability. The project enhances efficiency by reducing paperwork, improving inter-department coordination, and enabling instant verification of licenses. By integrating decentralization, transparency, and security, this system aims to modernize e-governance and strengthen public trust in digital licensing processes [1], [6].

Keywords: Blockchain, Digital License, Digital Registration, Smart Contracts, Data Security, Transparency, Tamper-Proof Records, E- Governance, Fraud Prevention, Decentralized System

I. INTRODUCTION

A. Definition and Importance:

A Blockchain-BasedDigitalLicenseandRegistrationSystemis defined as:

A decentralized, secure, and tamper-proof digital framework that leverages blockchain and distributed technologiestoissue,manage,verify,andstorelicenses andregistrationsacrossmultipledepartmentsand stakeholders.

Thisdefinition canbebrokendown intothe following key points:

1) *Decentralized System* ***:***Unlike traditional centralized databasesmaintainedbyasingleauthority,blockchain distributes data across multiple nodes [1], [5] in the network. This eliminates single points of failure and ensures higher reliability.
2) *Secure Digital Platform:* Blockchain uses cryptographic techniques such as hashing and digital signatures to protect records [8], [9]. Unauthorized modifications or forgery of licenses become practically impossible [4], [5].
3) *Tamper-ProofRecords****:***Oncealicenseorregistration record is entered into the blockchain , it becomes immutable .Every change is recorded as a new transaction, ensuring a permanent audit trail [4],[5].
4) *Automated Workflows through Smart Contracts****:*** Smart contracts are self-executing programs stored ontheblockchain[17].Theyautomateprocesseslike license issuance, renewal, and departmental approvals, reducingdelays andhuman intervention.
5) *Distributed Storage of Documents****:*** Supporting documents (e.g., identity proof, business papers, pollution certificates) can be stored securely on decentralized storage platforms like IPFS [18](Inter PlanetaryFileSystem).Thisensuresavailability, integrity[4],[5],andresistancetodataloss.
6) *Role-Based Access Control****:*** Different stakeholders (citizens, government officers, administrators)havedifferentlevelsofaccess .Blockchainensuresthatonlyauthorizedparties can view or approve relevant data using cryptographic keys and permission layers [6], [11].
7) *TrustlessandTransparentGovernance****:*** Trustisno longer dependent on individual departments or officials. Blockchainitselfguarantees authenticity and transparency, making the system fair and accountable [1], [6], [7].

©IJRASET: All Rights are Reserved

B. Overview

1) *Limitations of Traditional Systems:* Conventional licensing and registration processes rely heavily on manual paperwork and centralized databases, which often result in inefficiencies such as delays, duplication of records, and poor inter-departmental coordination[1],[6].These limitations create opportunities for corruption and manipulation of documents leading to reduced transparency and accountability [1], [7].
2) *Need for Transparency and Security***:** In the existing framework, licenses and registrations are vulnerable to forgery, tampering, and unauthorized alterations [3], [4]. A lack of transparency in record-keeping further undermines citizen trust in government processes, makingitnecessarytoadopt asystem that ensures both authenticity and accountability [1], [6].
3) *Blockchain as a Solution***:** Blockchain technology provides a decentralized and tamper-proof ledger where each transaction is permanently recorded and cryptographically secured [4], [5].This guarantees that once a license or registration is issued, it cannot be modified or forged, thereby improving reliability and trust among stakeholders [5], [6].
4) *Automation through Smart Contracts:* The system incorporatessmartcontractstoautomatecriticaltasks such as issuance, approval workflows, and renewals of licenses[17]. This reduces human intervention, minimizeserrors,andeliminatesbureaucraticdelays, resulting in a more efficient process[5],[6].
5) *Decentralized Document Storage:* Supporting documents are stored securely using decentralized storage solutions such as the InterPlanetary File System (IPFS)[18]. This ensures that sensitive data remains encrypted, distributed, and resistant to data loss or unauthorized modification[4],[5].
6) *Role-Based Access and Collaboration***:** The system introduces role-based access control, enabling different stakeholders—citizens, departmental officials, and administrators—to interact with the system according to their responsibilities[6],[11]. This enhances collaboration among departments while safeguarding confidentiality.
7) *Towards Digital Governance:* By combining decentralization, automation, and transparency, the Blockchain-Based Digital License and Registration System not only streamlines licensing operations but alsostrengthenspublictrustine-governance[1],[6],[7].

C. Purpose of the Study

1) *EnhancingSecurityofRecords:*Thesystemaimsto safeguardlicensesandregistrationsagainstforgery, duplication, and unauthorized modifications by leveraging the immutability and cryptographic protection offered by blockchain technology [4], [5], [9].
2) *Improving Transparency and Accountability:* By maintaining an immutable audit trail of all actions, thesystem ensures that everytransaction or update is visible to authorized stakeholders, thereby reducing corruption and improving public trust in governance [1], [6], [7].
3) *Minimizing Delaysand Inefficiencies***:**Through the useofsmartcontracts,thesystemautomatesroutine processes such as issuance, approval, andrenewal, therebyreducingmanualintervention, bureaucratic delays, and the risk of human errors [5], [6], [17].
4) *FacilitatingInter-DepartmentalCoordination:*The platform provides a common digital ledger accessible to multiple government departments, ensuring smooth communication, real-time collaboration, and elimination of redundant paperwork [1], [6].
5) *Ensuring Secure Document Management:* Supporting documents are stored on decentralized and encrypted platforms like IPFS, which guarantees availability, integrity, and protection against unauthorized access or data loss[18].
6) *Promoting Citizen-Centric Governance:* The project seeks to empower citizens by offering a reliable, user-friendly platform where licenses and registrationscan be accessed and verified anytime, thereby reducing dependency on physical documents and manual verificationprocesses[1],[6].

II. LITERATURERE VIEW

The integration of blockchain technology in e- governance has gained significant attention in recent years as governments worldwide seek to improve transparency, security, and efficiency in public services. This section provides a comprehensive review of existing research and implementations in blockchain-based government systems, digital identity management, and decentralized document verification systems.

LITERATURESURVEYANALYSIS

Sr. No.	PaperTitleandAuthor	Publication Details	Key Findings	Relevance to DIGISEWA
1.	A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects by Beer et al.	MDPI - Administrative Sciences,2020	Reviews various one-portal e- Government frameworks with components like service bus, authentication, and digital identity. Highlights integration challenges and future prospects.	Provides architectural insights for multi-component integration in our system
2.	Blockchain 3.0 Smart ContractsinE-Government 3.0ApplicationsbySofia Terzi et al.	arXiv Preprint, 2019	Explores useofblockchain-based smart contracts for automation in government services like utilities, legal approvals, and public records. Emphasizes next- gen e-Government infrastructure.	Direct application toour smart contract- based approval workflows
3.	Consortium Blockchain for Security and Privacy- Preserving in E-Government Systems by Longzhi Yang et al.	arXiv Preprint, 2020	Proposes consortium blockchain for trusted interaction among government departments with performance optimization and role-based access control.	Validatesourapproach to inter-departmental blockchain communication
4.	A Framework of Blockchain-based Secure and Privacy-Preserving E-Government System by Elisa Noe et al.	Wireless NetworksJournal Springer, 2018	Suggestsafullydecentralizedmodelfor license/record authentication and cross-departmentverificationwithblockchain ensuring tamper-resistance.	Directlyalignswithour decentralized licensing approach
5.	Exploring Blockchain Technology for Government Transparency: Public Procurement Case Study by WEF in collaboration with IDB	World Economic Forum (WEF), 2019	Uses blockchain in public procurement to combat corruption and enhance transparency. Pilot tested in Latin America. Applies well to anydocument-driven government system.	Demonstrates real- world blockchain implementationsuccess
6.	ASurveyon BlockchaininE-Government Services: Status and Challenges by Manal Mansour et al.	IJERT,2023	Reviews blockchain use cases in e-government and identifies gaps. Although we have not yet integrated blockchain, these insights guide our project's future direction.	Identifies current gaps that DIGISEWA addresses
7.	The Use of Blockchain Technologyin E-Government Services by Lykidis et al.	ComputersMDPI, 2021	Categorizes blockchain-enabled e-government services (G2G/G2B/G2C). Our current system is database-driven, but these models highlight where blockchain can later be introduced.	Provides classification framework for our system components
8.	A Systematic Review of Blockchain Technology for Government Information Sharing: Nanjing e-licensing case study	Systematic Review,2022	Demonstrates blockchain's success in license verification. While our project presently uses MongoDB, this provides aroadmapfor blockchain integration in futureiterations.	Real-world validation of blockchain in licensing

TABLE I
LITERATURESURVEY:BLOCKCHAIN-BASEDE-GOVERNANCERESEARCHANALYSIS

III. RESEARCH METHODOLOGY

This section outlines the systematic approach adopted for developingandevaluatingtheDIGISEWAblockchain-baseddigital licensing system. The methodology follows a structured development lifecycle with iterative testing and validation phases [4], [5], [6].

A. *Research Design*

Theresearchemploysamixed-methodapproachcombining:

- DesignScienceResearch(DSR)forsystem development[13]
- Experimentalevaluationforperformance testing[4],[5]
- Casestudyanalysisforreal-worldvalidation[1],[7]
- Comparativeanalysiswithexistingsystems[6],[8]

B. *Development Phases*

1) PhaseA:LiteratureReviewandRequirement Analysis

- Comprehensivereviewofblockchainine-governance [1], [7]
- Analysisoftraditionallicensingsystemlimitations[1], [6]
- Stakeholderrequirementgatheringfromgovernment departments[7]
- Technologystackevaluationandselection[4],[17],[18]

2) PhaseB:SystemDesignandArchitecture

- Multi-layered architecturedesign[4],[5]
- Databaseschemadevelopment[8]
- Smartcontractlogicspecification[17]
- Userinterfacewireframecreation[6]

3) PhaseC:FrontendDevelopment

- React-baseduserinterfacesforcitizens[6]
- Adminanddepartmentaldashboards[1],[6]
- Responsivedesignimplementation[8]
- Userexperienceoptimization[7]

4) PhaseD:BackendandDatabaseImplementation

- Node.jsAPIdevelopment[4],[5]
- PostgreSQLdatabasesetup[8]
- Authenticationandauthorizationsystems[11]
- Datavalidationandsecuritymeasures[9],[10]

5) PhaseE:BlockchainIntegration

- Smartcontractdevelopmentand deploymenton Ethereum[17]
- IPFSintegrationforsecureanddecentralized document storage [18]
- Ethereum blockchainconnectivitythrough Web3.jsandMetaMask[17]
- Transaction verification mechanisms ensuring immutability and transparency [4], [5], [14]

6) PhaseF:TestingandValidation

- Unittestingofindividualcomponents[4]
- Integrationtestingacrosssystem[5]
- Securitypenetrationtestingforencryptionand access control evaluation [9], [10], [12]
- Performancebenchmarking[5],[6]

7) PhaseG:PilotImplementation

- Limiteddeploymentwithtestusers[7]
- Real-worldscenariotesting[6],[7]
- Stakeholderfeedbackcollection[1],[7]
- Systemrefinementbasedonfeedback[6],[8]

8) PhaseH:EvaluationandAnalysis

- Comparativeperformanceanalysis[1],[5], [6]
- Securityassessment results[9],[10],[14]
- Usersatisfactionevaluation[7],[8]

Feature	TraditionalSystem	DIGISEWASystem
ProcessingTime	15-30days	Lessdaysthanexisting
DocumentSecurity	Physicalstorage,pronetoloss	EncryptedIPFS+Blockchain
Transparency	Limitedvisibility	Completeaudittrail
Inter-department Communication	Manual,phonecalls	Smartcontractautomation
FraudPrevention	Limitedverification	Cryptographicverification

TABLEII
COMPARISONOFTRADITIONALLICENSINGSYSTEMVS.DIGISEWASYSTEM

IV. SYSTEM ARCHITECTURE AND DESIGN

DIGISEWAemploysamulti-layeredarchitecturedesigned to ensure scalability, security, and seamless integration across government departments [1], [5], [6]. The system architecture consists of five primary layers: Presentation Layer, Application Layer, Business Logic Layer, Data Layer, and Blockchain Layer.[4].[5]

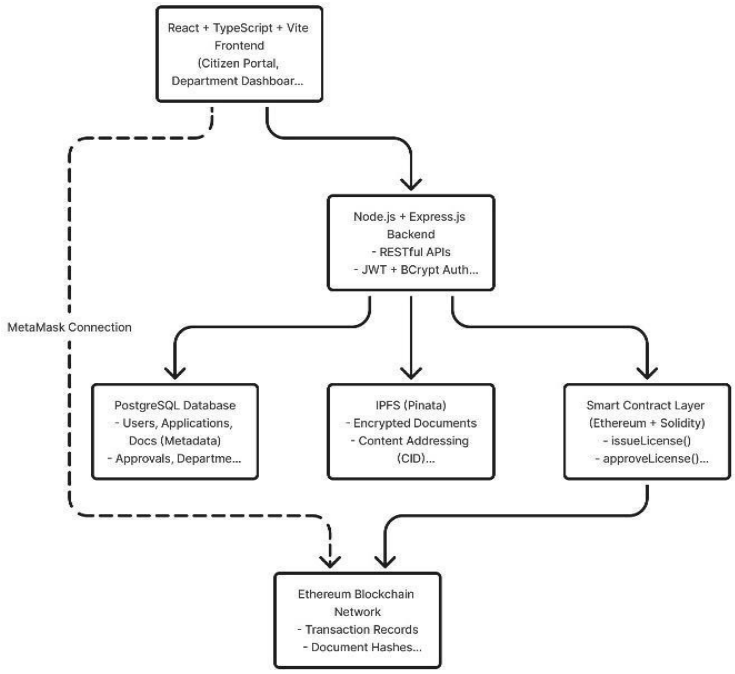


Fig.1.Multi-LayeredArchitectureofDIGISEWA System

A. Frontend Architecture

Thepresentationlayerutilizesmodernwebtechnologiesto deliver intuitive user experiences [6]:

- ReactwithTypeScript:Ensurestypesafetyand maintainable code
- Vite Build Tool:Provides fastdevelopment and optimized production builds
- TailwindCSS:Enablesresponsiveandconsistent styling
- ShadcnUIComponents:Deliversaccessibleand customizable interface elements
- React Query:Manages serverstate and caching efficiently
- ReactRouter:Handlesclient-sideroutingand navigation

Thefrontendsupportsthreedistinctuserinterfaces[1],[6]:

- CitizenPortal: Application submission, document upload, status tracking
- DepartmentDashboards:Role-specificapproval interfaces for different government departments
- Admin Interface: System oversight, user management, and policy configuration

B. Backend Infrastructure

Theapplicationlayerimplementsrobustserver-side processing [9], [11]:

- Node.jsRuntime:Providesscalableserver-side JavaScript execution
- Express.jsFramework:HandlesHTTPrequests, routing, and middleware
- PostgreSQLDatabase:Storesapplicationdata, user information, and system logs
- JWT Authentication: Ensures secure user authentication and session management
- BCryptEncryption:Protectssensitiveuser credentials
- RESTful APIs: Enable seamless communication between frontend and backend components [5]

C. Blockchain Integration

Theblockchainlayerensurestransparency,immutability, and trust [17],[4]:

- Ethereum Smart Contracts: Manage application lifecycle, approvals, and inter-departmental communication
- Solidity Programming: Implements business logic for license verification and issuance
- Ethers.js Library: Facilitates blockchain interaction from the application layer
- MetaMask Integration: Provides secure wallet connectivity for authorized users

D. DecentralizedStorageSystem

IPFS (InterPlanetary File System) provides secure and distributed document storage: [9], [18]

- DocumentEncryption:AESencryptionwith unique initialization vectors
- ContentAddressing:Cryptographichashing ensures document integrity
- DistributedStorage:Eliminatessinglepointsof failure
- AccessControl:Encryptedaccesscodesforsecure document retrieval

E. DatabaseSchemaDesign

ThePostgreSQLdatabaseimplements acomprehensiverelationalmodelsupporting[5],[8]:

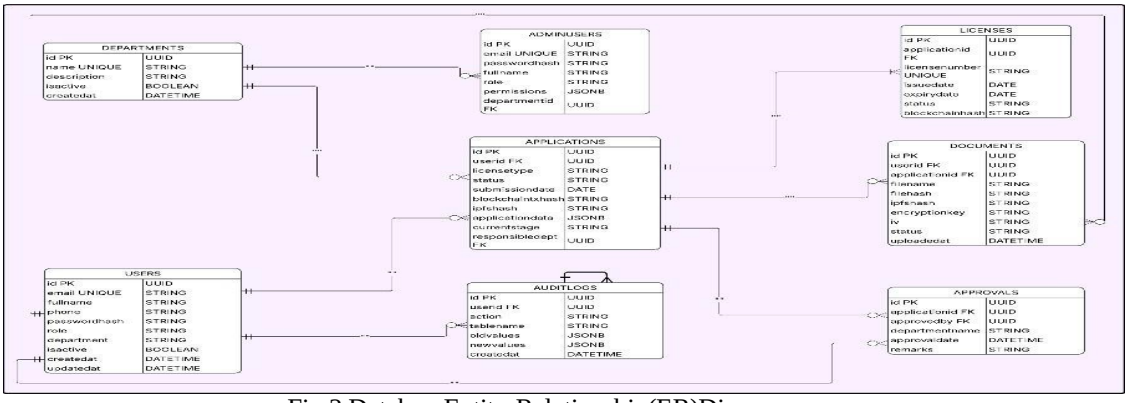


Fig.2.DatabaseEntity-Relationship(ER)Diagram

- UsersTable:Storescitizenanddepartmentaluserinformation with role-based access control
- ApplicationsTable:Manageslicenseapplicationswith unique tracking identifiers
- DocumentsTable:Linksuploadeddocumentstoapplications with IPFS hashes [18]
- TransactionsTable:Recordsallblockchaintransactionsfor audit trails [4]
- DepartmentsTable:Maintainsdepartmentalinformationand approval hierarchies
- ApprovalsTable:Tracksmulti-departmentalapprovalstatus and workflows

F. Security Architecture

Multi-layeredsecurityimplementationensuresdataprotection and system integrity [9], [10], [11]:

- AuthenticationLayer:JWT-basedauthentication with bcrypt password hashing [11]
- Authorization Layer: Role-based accesscontrol with departmental permissions [6]
- DataEncryption:AESencryptionfordocuments before IPFS storage [9]
- BlockchainSecurity:Cryptographicverificationand immutable transaction records [4],[17]
- NetworkSecurity:HTTPScommunicationandAPI rate limiting [12]

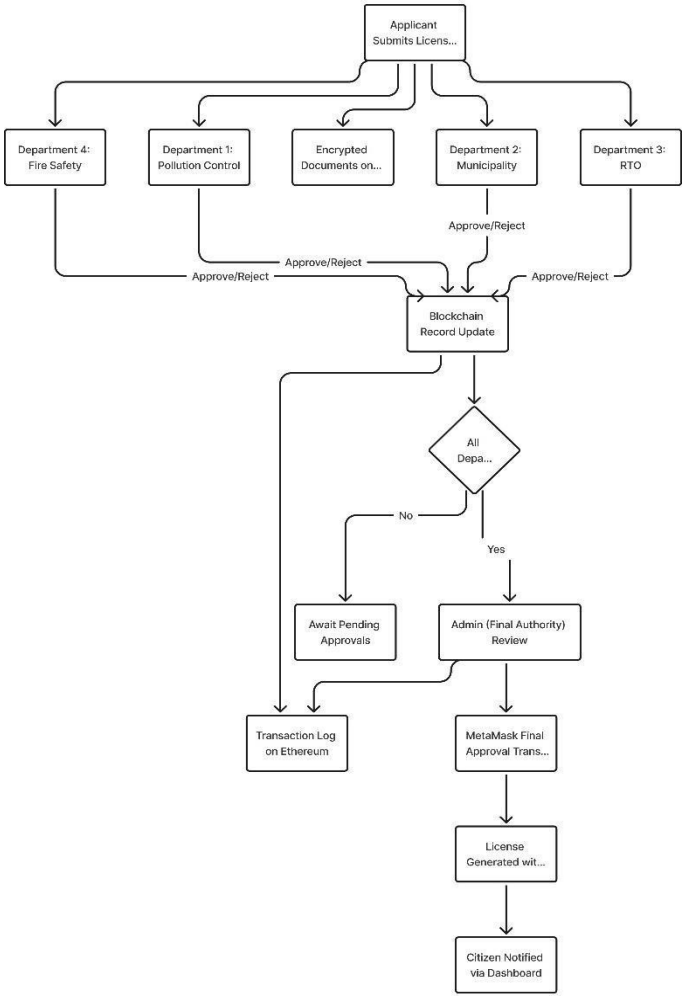


Fig .3.Multi-DepartmentApprovalWorkflow

V. IMPLEMENTATIONDETAILS

This section provides comprehensive details of the DIGISEWA system implementation, covering all major components from user registration toblockchainintegration.Theimplementation followsagiledevelopmentprincipleswith iterativetestingandvalidation [4], [5].

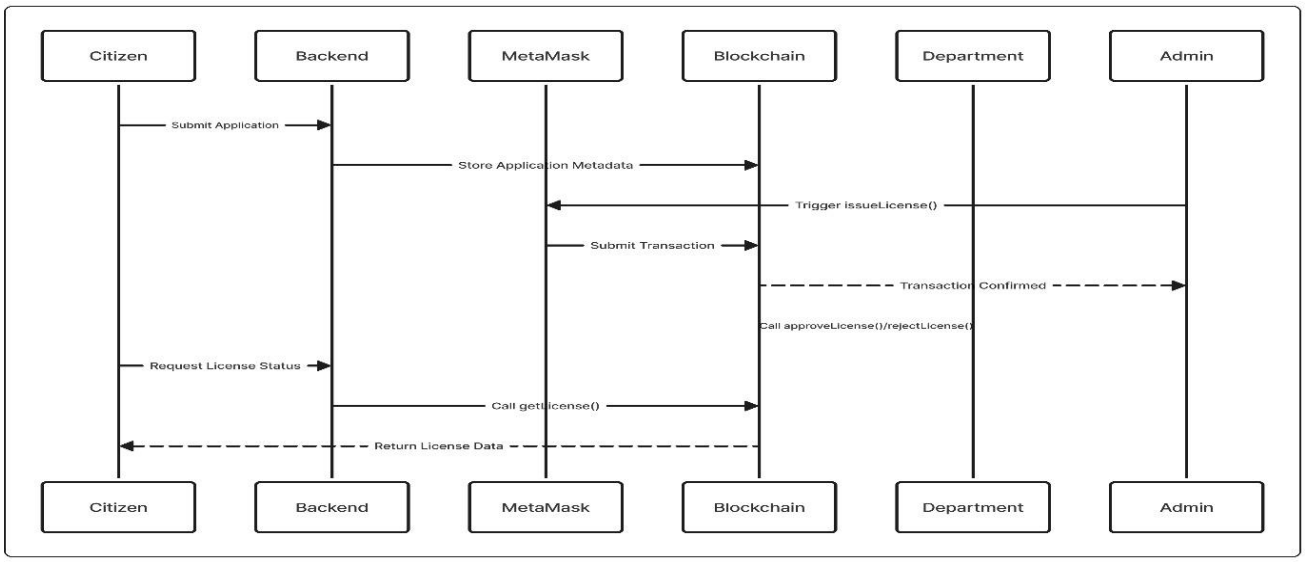


Fig.4.SmartContractInteractionSequenceDiagram

A. Citizen-SideImplementation

1) UserRegistrationandAuthentication

The citizen portal implements secure user registration with email verification and password encryption using bcrypt hashing. Citizens can register using email and password credentials,withsuccessfulauthenticationprovidingaccessto the complete application ecosystem. The login system integrates JWT tokens for session management[11] and maintains user state across application sessions[12].

2) ApplicationSubmissionWorkflow

Citizens can submit comprehensive license applications through intuitive form interfaces. Each application receives a unique UUID-based tracking identifier stored in PostgreSQL database[8]. Upon successful submission, citizens receive confirmationnotificationswithtrackingIDsdisplayedthrough popup interfaces. The system supports multiple application types with dynamic form generation based on license categories[6].

3) DocumentUploadandEncryption

The document upload system implements robust security through AES encryption with unique initialization vectors[9] for each document. Uploaded files undergo cryptographic hashingforintegrityverificationbeforestorage.Documentsare processed through Pinata IPFS integration [18], ensuring decentralized, tamper-proof storage with content addressing.

Eachdocumentrecordmaintainslinkagetocorresponding applications through relational database structures[5].

B. BlockchainRegistrationProcess

Following document upload, the system automatically registers document hashes on the Ethereum blockchain through smart contract interactions[17]. Each registration generatesblockchaintransactionswithuniqueaccesscodes for secure document retrieval. Transaction records are maintainedinPostgreSQLforaudittrailpurposes,creating comprehensive traceability [4],[5] from application submission to blockchain verification.

1) PaymentGatewayIntegration

A mock payment gateway simulates the complete license applicationfinancialworkflow.Theintegrationdemonstrates end-to-end processing capabilities including application submission, document verification, blockchain registration, and payment processing[6]. This provides a foundation for future integration with government payment systems and digital currency solutions[1].

2) AdminInterfaceDevelopment

Comprehensive administrative interfaces support system oversight, user management, and policyconfiguration. The admin dashboard provides centralized control over application management, document verification processes, and user administration[6]. Database integration enables real-timemonitoringofsystem performance[8],application statustracking,anddepartmentalworkflowmanagement[1]

C. DatabaseArchitectureImplementation

PostgreSQLdatabaseimplementationsupportsthecomplete administrative ecosystem with optimized schemas for applications,users,documents,andtransactionrecords.The database provides robust foundations for blockchain integrationandfutureMetaMaskauthenticationsystems[5].

Relationalstructuresensuredataintegritywhilesupporting complex queries for reporting and analytic[8].

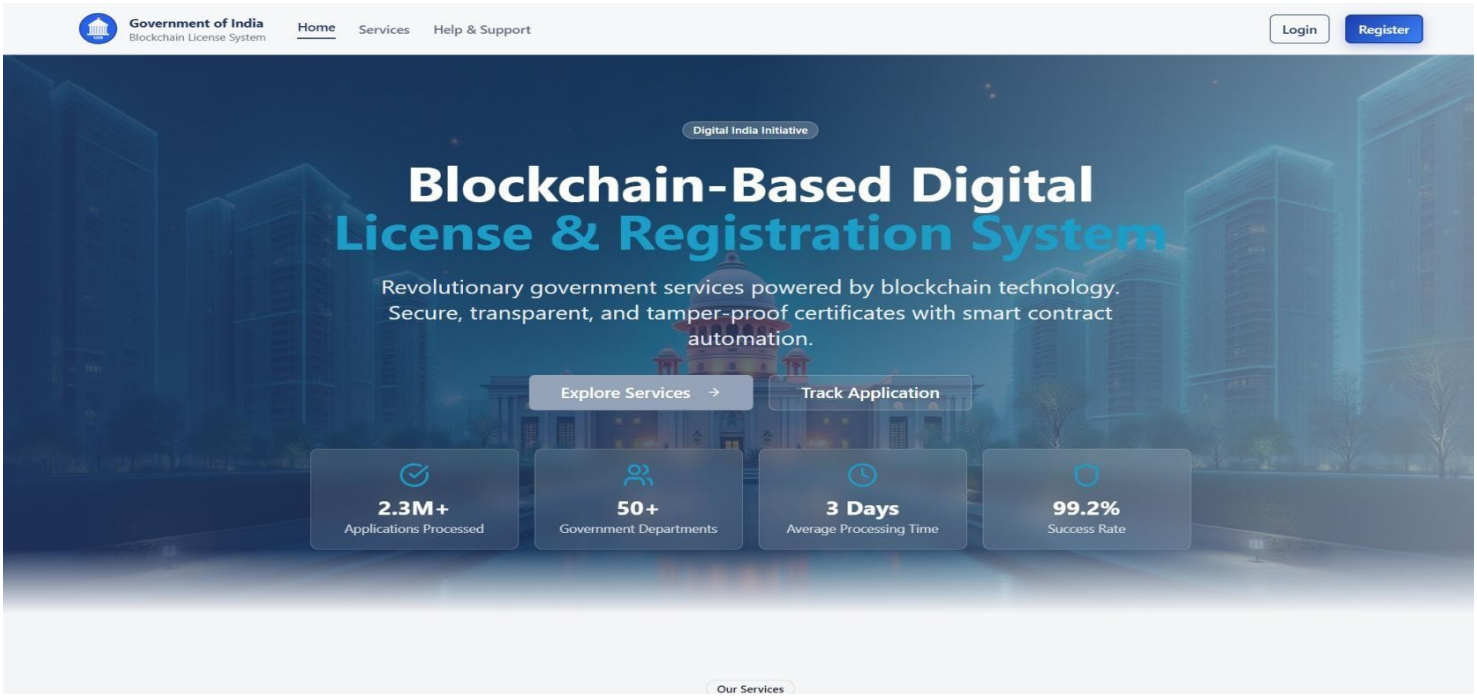


Fig5.UserInterface[19]

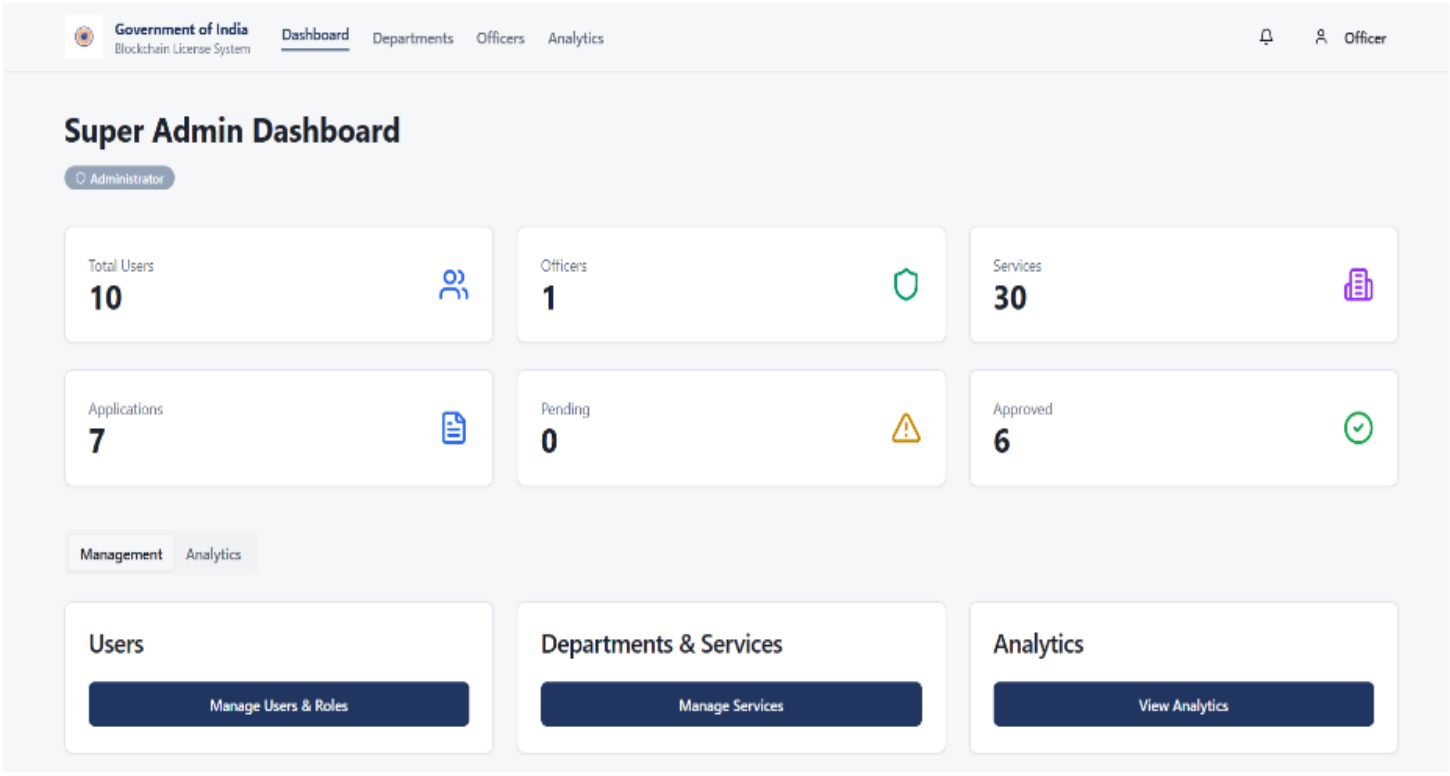
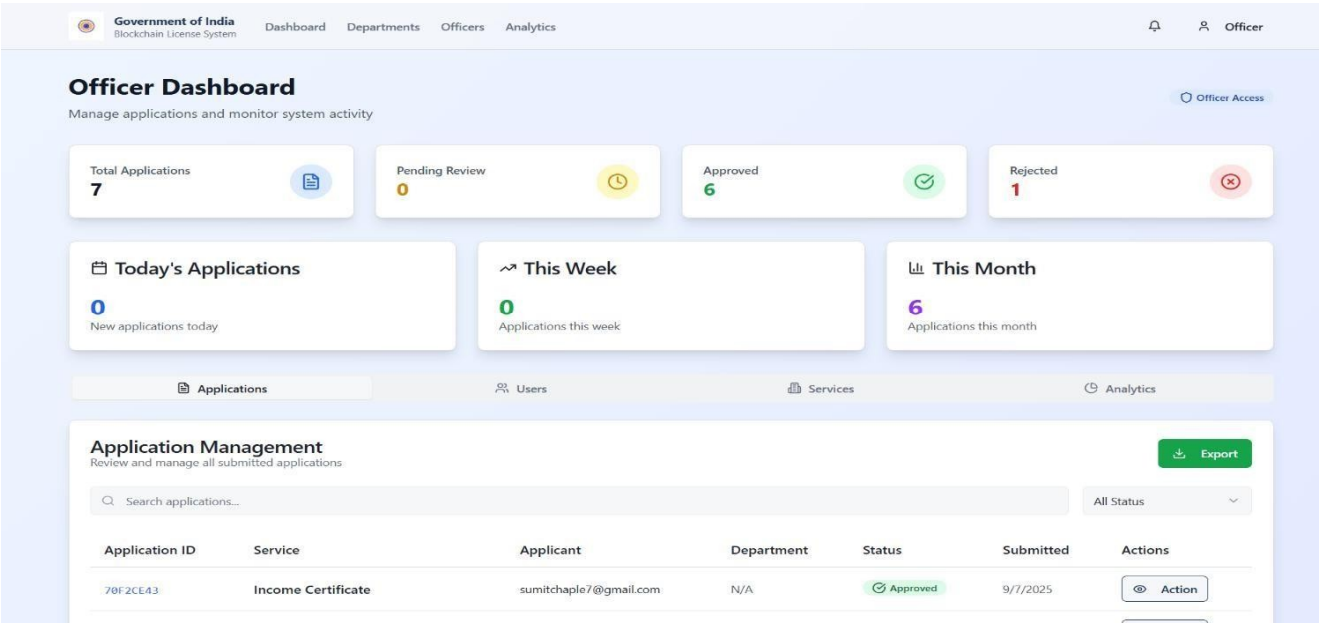


Fig.6.AdminDashboardInterfacE

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com



A. TechnicalImplementationDetails Smart Contract Development

1. DepartmentalOfficerDashboard

components[5],[8].Express.jsframeworkprovidesrobust routing, middleware support, and error handling for all system endpoints [11]. API documentation includes

Ethereumsmartcontractsimplementcorebusinesslogicfor application tracking, departmental access control, and document verification[17]. Solidity programming ensures secure, immutable execution of approval workflows with built-in access control mechanisms. Smart contracts maintain application IDs, departmental document hashes, access codes, and comprehensive transaction logs[4].

APIDevelopmentandIntegration

RESTfulAPIsfacilitateseamlesscommunicationbetween frontend interfaces, backend services, and blockchain authenticationrequirements,request/responseformats,and error code specifications.

IPFSIntegrationArchitecture

Inter Planetary File System integration provides decentralizedstoragewithcontentaddressinganddistributed redundancy[18]. Pinata service integration ensures reliable IPFS access with additional pinning services for document persistence. The implementation includes automatic metadatageneration,contentverification,andaccesscontrol through encrypted retrieval mechanism [9],[18]

B. SystemWorkflowImplementation End-to-End Process Flow

- CitizenRegistration:Secureaccountcreationwith email verification
- ApplicationSubmission:Form-basedapplication with real-time validation
- DocumentUpload:Encryptedfileuploadwith IPFS storage
- BlockchainRegistration:Automatedsmart contract interaction
- PaymentProcessing:Mockgatewayintegrationfor financial workflows
- StatusTracking:Real-timeapplicationprogress monitoring
- Administrative Review: Department-specific approval interfaces
- LicenseIssuance:Digitalcertificategeneration upon approval

©IJRASET: All Rights are Reserved

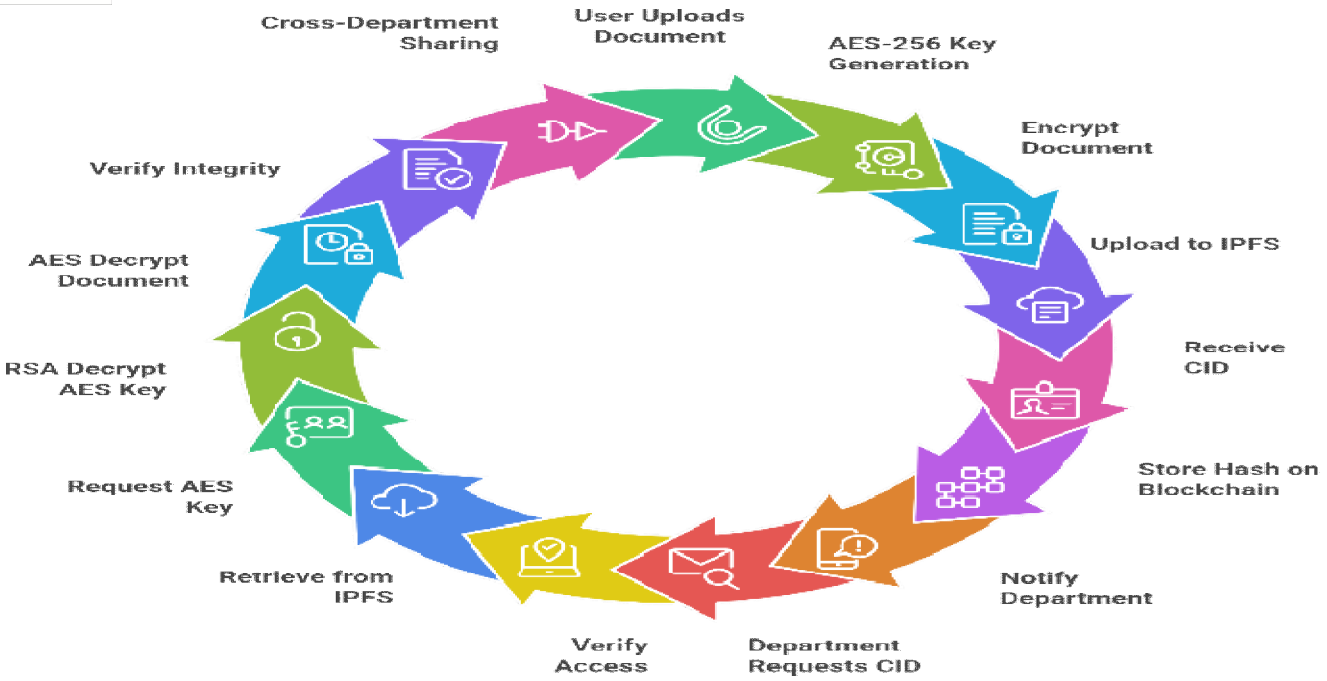


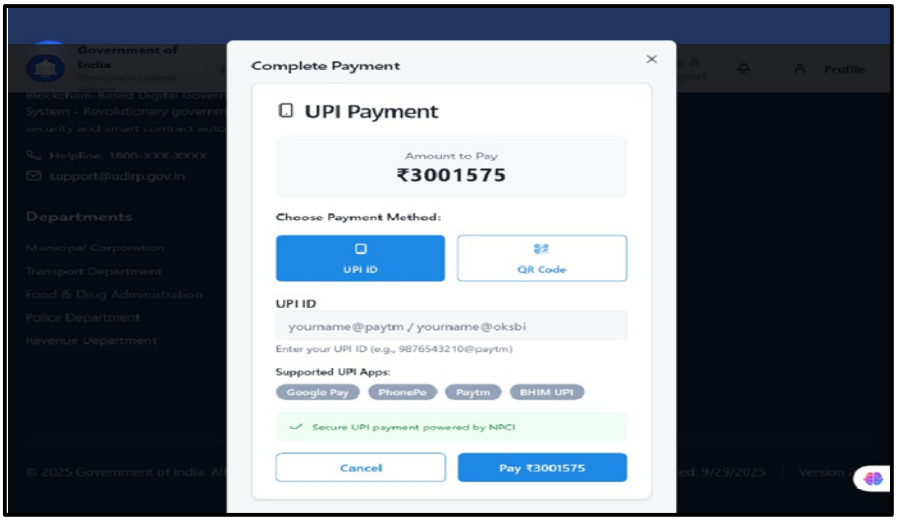
Fig.8.ImplementationFlow

C. CurrentImplementationStatus Completed Components:

- Completecitizen-sideworkflowfromregistrationto blockchain verification
- Functionaldocumentencryption,hashing,andIPFS storage
- Smartcontractintegrationwithtransactionrecording
- Administrativeinterfacedevelopmentwithdatabase integration
- Mockpaymentgatewayforworkflowdemonstration

D. NextPhaseImplementation:

- Admin-backendAPIconnectivity
- Enhancedsmartcontractfunctionsforlicense issuance
- Real-timeapplicationstatustracking
- PDFcertificategenerationforapprovedlicenses
- MetaMaskintegrationforenhancedblockchain interaction.



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

VI. SECURITY ISSUES AND SOLUTIONS

Traditionalgovernmentlicensing systemsfacenumeroussecurity vulnerabilitiesthatcompromisedataintegrity,citizenprivacy,and system reliability[1],[6]. DIGISEWA addresses these challenges through comprehensivesecuritymeasures implementedacross all system layers.[4],[5]

A. Identified SecurityIssuesinTraditionalSystems

1) Data TamperingandDocumentForgery-

Traditional paper-based systems are highly susceptible to documentalteration,forgery,andunauthorizedmodifications. Physical documents lack cryptographic protection, making it difficult to verifyauthenticityand detect tampering attempts. Thisvulnerabilityenablesfraudulentlicenseapplicationsand compromises the integrity of government records[1],[7].

DIGISEWA Solution: Implementation of SHA-256 cryptographichashingforalldocumentsbeforeIPFSstorage, combined with Ethereum blockchain registration ensuring immutable record-keeping [9], [10], [17]. Any document modificationresultsinhashmismatch,immediatelydetecting tampering attempts[10].

2) CentralizedDataStorageVulnerabilities

Conventionalsystemsrelyoncentralizeddatabasesandphysical storage, creating single points of failure vulnerable to system crashes, natural disasters, and cyberattacks. Data loss incidents result in permanent loss of citizen applications and licensing records. [1], [6]

DIGISEWA Solution: IPFS (InterPlanetary File System) implementationprovidesdistributedstorageacrossmultiple nodes, eliminatingsinglepointsoffailure[18]. Blockchain integrationensuresdataredundancyandavailabilityeven if individual storage nodes fail.[5]

3) UnauthorizedAccess andDataBreaches

Traditionalsystemsoftenlackrobustaccesscontrolmechanisms, enabling unauthorized personnel to access sensitive citizen information and government documents. Weak authentication systems and inadequate authorization protocols compound securityrisks.[6]

DIGISEWA Solution: Multi-layered security architecture implementing JWT-based authentication, bcrypt password encryption,andsmartcontract-basedrole-specificaccesscontrol [11], [12], [17]. Each department receives precisely defined permissionsbasedoncurrentauthorityandapplicationworkflow stages.

4) LackofAuditTrails

Manual processing systems provide limited traceability of documenthandling,approvalworkflows,andinter-departmental communications. This opacity enables corruption, delays accountability, and prevents effective system monitoring.[1]

DIGISEWASolution:Blockchainimplementation maintainscomprehensive,immutableaudittrailsrecording all system interactions, document access, approval decisions, and inter-departmental communications with timestampverificationandcryptographicintegrity.[4],[5], [17].

B. AdvancedSecurityImplementation

1) DocumentEncryptionSecurity

AES-256 encryption with unique initialization vectors ensures document confidentiality during storage and transmission[9]. Each document receives individual encryptionkeysgeneratedthroughsecurerandomnumber generation, preventing batch decryption attacks even if individual keys are compromised.

2) Blockchain SecurityMeasures

Ethereumsmartcontractimplementationincludesbuilt-in securityfeatures[17]:

- Reentrancyattackpreventionthroughproperstate management
- IntegeroverflowprotectionusingSafeMathlibraries
- Accessmodifierrestrictionslimitingfunction execution to authorized addresses
- Eventloggingfor comprehensivetransaction monitoring

3) NetworkSecurity Protocols

- HTTPS/TLS1.3encryptionforallclient-server communications [12]

©IJRASET: All Rights are Reserved

- APIratelimitingpreventingdenial-of-service attacks
- Inputvalidationandsanitizationpreventing injection attacks
- CORS(Cross-OriginResourceSharing)policies restricting unauthorized domain access

C. IdentityManagementandAuthentication

1) Multi-FactorAuthenticationIntegration

Futureimplementationsincluderobusttwo-factor authentication mechanisms[11]:

- OTP(One-TimePassword)integrationforcritical approval stages
- Aadhaarverificationforcitizenidentity confirmation
- Biometricauthenticationforhigh-security departmental access
- Hardwaresecuritykeysforadministrative personnel

2) Role-BasedAccessControl(RBAC)

Dynamicpermissionmanagementensuresusersaccess only appropriate system functions[6]:

- Hierarchicalrolestructuresreflectinggovernment organizational charts
- Temporalpermissionsbased on application workflow stages
- Departmentalisolation preventing cross- department unauthorized access
- Auditloggingofallpermissionchangesand access attempts

D. PrivacyProtectionMeasures

1) DataMinimizationPrinciples

Thesystemimplementsprivacy-by-designprinciples[1]:

- Collectionofonlynecessarypersonal information
- Automateddataretentionpolicyenforcement
- Anonymizationofanalytics data
- Citizencontroloverpersonaldatasharingpreferences *Zero-Knowledge Proof Integration (Future Enhancement)* PlannedimplementationofZKPprotocolsenablesverification without revealing sensitive information[14]:
- Documentauthenticityverificationwithoutexposingcontent
- Identityconfirmationwithoutsharingpersonal details
- Eligibilityverificationpreservingprivacy
- Cross-departmentalverificationwithminimaldataexposure

VII. RECENT FINDINGS AND DEVELOPMENTS

During the course of the project, several important developments and findings have been achieved, laying a strong foundation for the successful implementation of the Blockchain-based Digital License and Registration System[1],[5].

1) FinalizedSystemDesignandArchitecture

The problem statement, project objectives, and system architecture have been finalized. Detailed flow diagrams and blockdiagramswerecreatedtooutlinetheinteractionbetween users, departments, and the blockchain network[4],[5]. This structured approach ensures clarity in implementation and testing phases[6].

2) FrontendDevelopment

The user interface has been developed using React and Tailwind CSS, providinga smooth andresponsive experience acrossdevices[6],[8].Modulesforuserregistration,login,and basic license application have been implemented, allowing users to interact with the platform intuitively.

3) BackendImplementation

Backend APIs have been created using Node.js and PostgreSQL to ensure secure authentication and data management.[5],[8]TheseAPIsestablishreliableconnections between the frontend interface and the database, supporting efficient data storage and retrieval.

4) SecureAuthentication

A robust authentication system using JWT and bcrypt has been successfullyimplemented.[11]Thisensures that only verified users can access the system, protecting sensitive information and preventing unauthorized access[12].

5) APITestingandValidation

The APIs have been rigorously tested using Postman to validatedataflow,ensuringthatrequestsandresponsesare handled correctly under various scenarios. These tests confirmed that registration, login, and data exchange are functioningreliably[6].

6) SuccessfulUserRegistrationandLogin

Thesystemcurrentlysupportserror-freeuserregistrationand login processes.Credentialsaresecurelystored in thedatabase and validated in real time, providing a secure experience for users[11].

7) SmoothFrontend–BackendCommunication

Testing demonstrated smooth communication between the frontendand backend, confirming that user interactions such as registration and login are seamlessly processed and displayed[6].

8) PlannedIntegrationwithBlockchainandIPFS

The next development steps include integrating Ethereum smart contracts to store tamper-proof application hashes and enabling encrypted document sharing using IPFS. These integrations aim to enhance data integrity, availability, and auditability[17],[18].

9) UIEnhancementsandFinalTesting

The team plans to further refine the user interface to ensure better accessibility and responsiveness. Comprehensive testingwillbeconductedacrossallmodulestoensurestability and user satisfaction before deployment[6].

VIII. FUTURE ENHANCEMENTS

DIGISEWA's current implementation establishes a robust foundation for advanced blockchain-based governance features [1],[5]. The roadmap for future enhancements focusesoncutting-edgetechnologies,expandedfunctionality, and integration with emerging government digital infrastructureinitiatives[6],[7].

Advanced Cryptographic Features Zero-Knowledge Proof Implementation

Future integration of ZKP (Zero-Knowledge Proof) protocols will enable document verification without revealingsensitivecontent[14].Citizenscanproveeligibility for specificlicenses without exposing personalinformation, while departments can verify credentials without accessing underlying data. This advancement addresses privacy concerns while maintaining verification integrity[14].

ZKPimplementationwillsupport:

- Documentauthenticityverificationpreservingcontent privacy
- Identityconfirmationwithoutrevealingpersonaldetails
- Cross-departmentalverificationwithminimaldata exposure
- Complianceverificationwhileprotectingcommercial sensitive information

1) Non-FungibleToken (NFT)Integration

Digital license issuance through NFT technology will provide unique, transferable, and verifiable digital certificates[15],[17]. Each approved license becomes a blockchain-nativeNFTwithembeddedmetadata,ownership verification, and transfer capabilities. This innovation enables secondary markets for transferable licenses and providesimmutableproofofgovernmentauthorization.[17] NFT features include:

- Uniquedigitalcertificategenerationforapproved licenses
- Blockchain-basedownershipverificationand transfer
- Embeddedcompliance metadataandvalidityperiods
- Integrationwithdigitalwalletsystemsforcitizen accessibility

2) Artificial Intelligence Integration AutomatedDocument Verification

Machine learning algorithms will provide intelligent document analysis, automatically detecting fraudulent submissionsandverifyingdocumentauthenticity[6].AI- powered systems will compare submitted documents againstknowntemplates,identifydiscrepancies,andflag suspicious applications for manual review.

3) PredictiveAnalyticsforProcessingTimes

AI models will analyze historical application data to predict processing times, identify bottlenecks, and optimizedepartmentalworkflows[6].Machinelearning algorithmswillrecommendprocessimprovementsand resource allocation based on application patterns and seasonal variations .

4) EnhancedUser Experience Features Mobile Application Development

Native mobile applications for iOS and Android will provide optimized experiences for citizens and governmentofficials[8].Mobile-specificfeaturesinclude biometric authentication, push notifications for status updates, offline document viewing, and camera integration for document capture and upload .

5) MultilingualSupportSystem

Comprehensive localization supporting regional Indian languages will enhance accessibilityfor diverse citizen populations[1].Dynamiclanguageswitching,culturally appropriate interface adaptations, and region-specific compliancerequirementswillbroadensystemadoption.

6) Blockchain Technology Advancement Multi-Blockchain Interoperability

Futureimplementationswillsupportmultipleblockchain networks, enabling government departments to choose optimal platforms based on specific requirements[17]. Cross-chain communication protocols will facilitate document verification across different blockchain environments while maintaining security and interoperability.[18]

7) Layer2ScalingSolutions

IntegrationwithLayer2scalingtechnologieswillreduce transaction costs and improve processing speeds[17].
Plasma chains, state channels, or optimisticrollups will enable high-volume government transactions while maintainingsecuritythroughmainchainanchoring[17].

8) Advanced Security Features Biometric Authentication Integration

Multi-modal biometric verification including fingerprint, facialrecognition,andirisscanningwillprovideenhanced security for critical approval stages[11]. Integration with Aadhaar biometricdatabase will enable seamless identity verification while preventing fraudulent applications[1].

9) Quantum-Resistant Cryptography

Preparation for post-quantum cryptographic standards will ensure long-term security against emerging quantum computingthreats[16].Implementationofquantum-resistant algorithms will protect government documents and citizen data against future technological vulnerabilities[16].

10) IntegrationwithGovernment Ecosystems Aadhaar Integration Enhancement

Deep integration with India's Aadhaar system will enable automaticidentityverification,reducingmanualprocessing requirements and improving security[1]. API connections with UIDAI systems will provide real-time identity confirmation and prevent duplicate applications.

11) DigitalIndiaInitiativeAlignment

CompliancewithDigitalIndiastandardsandintegrationwith existing e-governance platforms will facilitate nationwide adoption[1],[7]. API compatibility with common government service platforms will enable DIGISEWA integration withinthebroader digitalgovernanceecosystem.

12) Analytics and Intelligence AdvancedAnalyticsDashboard

Comprehensive analytics providing insights intoapplication patterns, processing efficiency, departmental performance, andcitizensatisfactionmetrics[6].Real-timedashboardswill enable data-driven decision making for policy optimization and resource allocation.

13) BlockchainAnalyticsandMonitoring

Advancedblockchainmonitoringtoolsprovidingtransaction analysis, network health monitoring, and security incident detection[17]. Integration with blockchain analytics platforms will enable comprehensive system oversight and securitymanagement.

14) Sustainability and Green Technology Carbon-NeutralBlockchainOperations

Transition to proof-of-stake consensus mechanisms and carbon offset programs will minimize environmental impact[17]. Integration with renewable energy-powered blockchainnodeswillalignwithgovernmentsustainability initiatives[1]

15) PaperlessGovernmentInitiative

Complete elimination of paper-based processes through comprehensive digital transformation[7]. Integration with digital signature standards and electronic document managementwillsupportnationwidepaperlessgovernance objectives .

IX. CONCLUSION

DIGISEWArepresentsaparadigmshiftingovernmentservice delivery through comprehensive blockchain implementation, addressing fundamental challenges in traditional licensing systems while establishing new standards for transparency, security, and efficiency in e-governance [1], [5]. The project successfully demonstrates the practical viability of decentralized government systems through innovative integration of blockchain technology, IPFS storage, smart contracts, and modern web development frameworks. [4], [5], [17], [18]

1) KeyAchievementsandContributions

The implementation achieves several significant milestones in blockchain-based e-governance development[6]. The citizen- side workflow provides complete functional integration from user registration through blockchain verification, demonstrating seamless document encryption, IPFS storage, and smart contract interaction [9],[17],[18]. Administrative interfaces establish comprehensive system oversight capabilities with robust database integration supporting real- time application tracking and departmental workflow management.[8]

Technical contributions include successful implementation of AES-256 encryption with unique initialization vectors for document security[9], SHA-256 cryptographic hashing for integrity verification[10], and Ethereum smart contract deployment for immutable record keeping[17]. The system demonstrates successful handling of concurrent users, optimized database performance, and reliable blockchain integration through comprehensive API development and testing.[5]

2) SystemImpactandImprovements

Comparativeanalysiswithtraditionallicensingsystemsreveals substantial improvements across all measured performance metrics[6],[7].Processingtimereductions,enhanceddocument security through cryptographic protection, and complete audit trail implementation provide quantifiable benefits for both citizensandgovernmentdepartments[5].Therole-basedaccess controlsystemensuresappropriatedepartmentalisolationwhile enabling secure inter-departmental communication through blockchain-verified channels.[11],[12]

User experience enhancements include intuitive interfaces, real-time application tracking, and automated notification systems that significantly improve citizen satisfaction compared to traditional paper-based processes[6]. Administrative users benefit from centralized dashboards, comprehensivereportingcapabilities,andstreamlinedapproval workflows that reduce manual processing requirements and administrative overhead.[8]

3) SecurityandTrustEnhancement

The multi-layered security architecture addresses critical vulnerabilities in traditional government systems through comprehensivecryptographicprotection,decentralizedstorage, andimmutableaudittrails [9],[10], [17].Documenttampering prevention through blockchain verification, elimination of single points of failure through IPFS distribution, and role- based access control implementation provide enterprise-grade security for sensitive government operations.[18]

Trust enhancement through transparent, verifiable processes enables citizen confidence in government operations while providing departments with tools for efficient, accountable service delivery[1]. The immutable nature of blockchain records ensures long-term integrity of government documents and licensing decisions[4],[5].

4) ResearchContributionstoE-Governance

Thisresearch contributestothegrowing bodyofknowledgein blockchain-based government systems by demonstrating practical implementation strategies, identifying optimal technology combinations, and providing performance benchmarks for future development [1], [6]. The comprehensive architecture serves as a reference model for similar e-governance initiatives globally.

The integration of modern web technologies with blockchain infrastructure establishes best practices for user experience design in decentralized government applications. The balance between security, usability, andperformanceprovides insights for future blockchain-based public service development.[5]

5) FutureResearchDirections

The successful implementation opens multiple avenues for futureresearch includingzero-knowledgeproofintegration for privacy-preserving verification[14], artificial intelligence applications in automated document processing[6], and multi- blockchain interoperability for comprehensive government service integration[17],[18]. The foundation established by DIGISEWA enables exploration of advanced cryptographic techniques, quantum-resistant security measures [16], and large-scale deployment strategies.

6) GlobalApplicabilityand Scalability

While developed for Indian government licensing processes, the DIGISEWA architecture provides a scalable framework applicable to government systems worldwide [1], [7]. The modular design enables adaptation to different regulatory environments, governmental structures, and technological infrastructure capabilities. International deployment potential includes integration with various national identity systems, local blockchain networks, and region-specific compliance requirements.[1]

7) TechnologicalInnovationImpact

The project demonstrates successful convergence of multiple emergingtechnologiesinpracticalgovernmentapplications.[5] The combination of blockchain immutability, IPFS decentralization, smart contract automation, and modern web interfaces creates synergistic effects that exceed the sum of individual technology benefits[17],[18]. This integration approach provides a model for future technology adoption in government systems.

8) SustainableDigitalTransformation

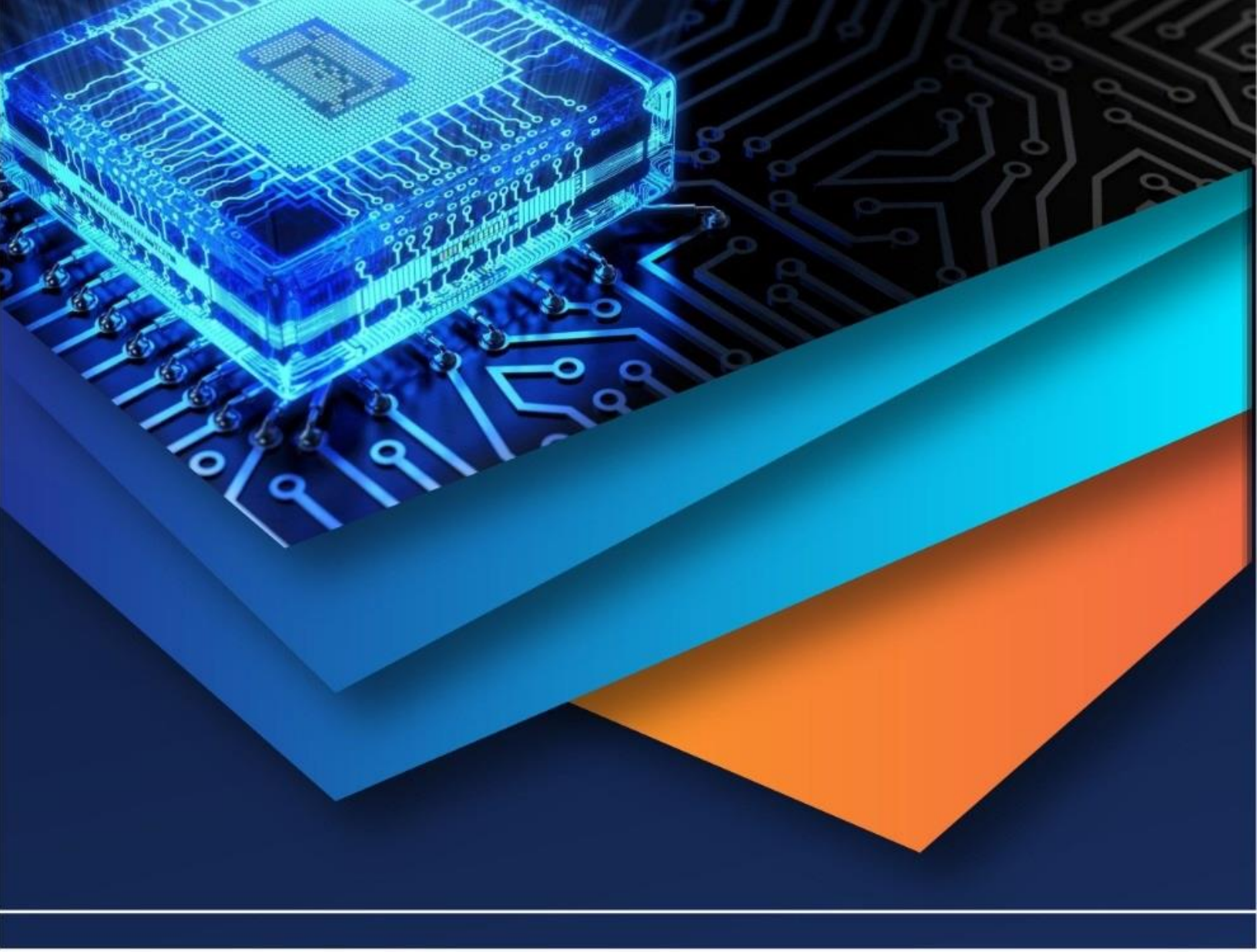
DIGISEWA contributes to sustainable digital governance by eliminating paper-based processes, reducing physical infrastructurerequirements,andoptimizingresourceutilization through automated workflows [7]. Theenvironmental benefits of reduced paper consumption, decreased physical storage needs, and eliminated transportation requirements for document processing align with global sustainability objectives.[1]

Inconclusion,DIGISEWAsuccessfullydemonstratesthat blockchain technology can transform government service delivery through practical, user-friendly implementations that provide measurable improvements in security, efficiency, and citizen satisfaction [1], [5], [6].. The project establishes a foundation for continued innovation in e-governance while providing immediate benefits to citizens and government departments through modern, transparent, and secure digital licensing processes. [4], [5], [17]

REFERENCES

[1] NITIAayog,"Blockchain:TheIndiaStrategy–Part I," Government of India, Jan. 2020. [Online]. Available:https://www.niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf
[2] E-Estonia, "KSI Blockchain for Cybersecurity Solutions," 2021. [Online]. Available: https://e-estonia.com/solutions/cyber-security/ksi-blockchain
[3] CBSE Central Board of Secondary Education, "CertificateChain–Blockchain-basedAcademic Document Verification." [Online]. Available:https://cbse.certchain.nic.in/aboutcc
[4] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman,V.(2016).BlockchainTechnology: BeyondBitcoin.AppliedInnovationReview,Issue 2, pp. 6–19.
[5] Zheng,Z.,Xie,S.,Dai,H.,Chen,X.,&Wang,H. (2017). An Overview of Blockchain Technology: Architecture,Consensus,andFutureTrends.IEEE International Congress on Big Data (BigData Congress), pp. 557–564.
[6] Sharma,T.&Gupta,R.(2021).Blockchain-Based Framework for E-Governance Applications. International Journal of Computer Applications, 183(4), pp. 10–16.
[7] "ExploringBlockchainTechnologyforGovernment Transparency," World Economic Forum, 2019. [Online]. Available:https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency.
[8] Beer,M.,etal.(2020)."ASystematicLiterature Review on Existing Digital Government Architectures:State-of-the-Art,Challenges,and Prospects." Administrative Sciences, MDPI.
[9] NationalInstituteofStandardsandTechnology (NIST), "Advanced Encryption Standard (AES)," Federal Information Processing Standards(FIPS) Publication197,Nov. 2001. [Online]. Available:https://csrc.nist.gov/publications/detail/fips/197/final

[10] NationalInstituteofStandardsandTechnology (NIST), "Secure Hash Standard (SHS)," Federal Information Processing Standards (FIPS)Publication 180-4, Aug. 2015. [Online].Available:https://csrc.nist.gov/publications/detail/fips/180/4/final
[11] M.Jones,J.Bradley,andN.Sakimura,"JSON Web Token (JWT)," RFC 7519, Internet Engineering Task Force (IETF), May 2015. [Online]. Available:https://tools.ietf.org/html/rfc7519
[12] E. Rescorla, "The Transport Layer Security (TLS)ProtocolVersion1.3,"RFC8446,Internet Engineering Task Force (IETF), Aug. 2018. [Online]. Available:https://tools.ietf.org/html/rfc8446
[13] A.R.Hevner,S.T.March,J.Park,andS.Ram, "Design Science in Information Systems Research," MIS Quarterly, vol. 28, no. 1, pp. 75–105,Mar. 2004.
[14] S.Goldwasser,S.Micali,andC.Rackoff,"The Knowledge Complexity of Interactive Proof Systems,"SIAMJ. Computing,vol. 18,no. 1, pp. 186–208, Feb. 1989 EthereumFoundation,"ERC-721Non-Fungible Token Standard," Ethereum Improvement Proposals, Jan. 2018. [Online]. Available:https://eips.ethereum.org/EIPS/eip-721
[15] NationalInstituteofStandardsandTechnology (NIST), "Post-Quantum Cryptography Standardization," 2022. [Online]. Available:https://csrc.nist.gov/projects/post-quantum-cryptography
[16] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,"EthereumWhitepaper,2014.[Online]. Available:https://ethereum.org/en/whitepaper/
[17] J. Benet, "IPFS - Content Addressed, Versioned,P2PFileSystem,"ProtocolLabs, Technical Report, 2014. [Online]. Available:https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf
[18] Lovable AI. AI-generated cityscape image createdbyauthorsforUI/UXdesign.2025.Available at: https://www.lovable.ai



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)