International Journal of Computer Techniques–IJCT Volume 13 Issue 3, May-June - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

# Blockchain-Based Academic Certificate Verification System: A Secure Web Application for Certificate Authentication Using Java, Spring Boot, Ethereum, MetaMask

Prof. Narde S. A., Yadav N.S., Ghodake D.T., Patil S.J., Salunkhe S. S.

(Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, Maharashtra, India
Under the Guidance of Prof. S. A. Narde)

**Abstract**—In recent years, the rapid growth of digital technologies in education has increased the importance of academic certificates for employment, higher studies, and professional validation. However, the issue of fake and forged certificates has become a serious challenge for institutions and organizations. Traditional certificate verification systems are manual, time-consuming, and often lack transparency and security. These systems are also vulnerable to data manipulation and unauthorized access due to centralized storage.

To address these challenges, this paper proposes a blockchain-based academic certificate validation system. The system uses blockchain technology to securely store certificate data in the form of cryptographic hash values generated using the SHA-256 algorithm. Since blockchain is decentralized and immutable, once data is stored, it cannot be altered or deleted.

The system allows administrators to upload student data and issue results, which are then stored on the blockchain. Each certificate is associated with a unique verification ID and can be validated using QR codes or direct input. The proposed system improves efficiency, enhances data security, and reduces the risk of fraud. The results demonstrate that the system is faster, more reliable, and more secure than traditional methods.

## I. INTRODUCTION

The verification of academic certificates is a critical process in education, recruitment, and institutional validation. In today's digital era, the increasing number of fake and forged certificates has become a serious issue, especially in developing regions where verification processes are still manual or semi-digital. Institutions and organizations often rely on traditional methods, which are time-consuming, inefficient, and prone to human errors.

Traditional certificate verification systems involve manual checks, physical document validation, and centralized databases. These methods often lead to problems such as data tampering, duplication, lack of transparency, and delays in verification. As a result, there is a strong need for a secure, reliable, and automated system that ensures authenticity and prevents fraud.

This project focuses on developing a Blockchain-Based Academic Certificate Verification System using Java, Spring Boot, React.js, MySQL/MongoDB, and Ethereum blockchain (Ganache, MetaMask). The system uses SHA-256 hashing and smart contracts to store certificate data securely on the blockchain. Since blockchain data is immutable, it ensures that once the certificate is issued, it cannot be altered.

Additionally, the system integrates a Machine Learning module for result analysis and prediction based on student performance metrics such as marks, CGPA, and attendance. It also includes an AI chatbot, which assists users by answering queries related to results, verification, and system usage. The system is designed to be secure, user-friendly, and scalable, ensuring efficient certificate management and verification.

### A. Problem Statement

Educational institutions face several challenges due to the lack of a secure and automated certificate verification system. Manual verification processes are time-consuming and prone to errors, leading to delays and inefficiencies. There is a high risk of certificate forgery, duplication, and unauthorized

modifications due to reliance on centralized systems.

Organizations often find it difficult to verify certificates quickly, as they must depend on institutions for validation. Additionally, there is no real-time verification mechanism, and existing systems lack transparency and traceability. These issues create a need for a secure, decentralized, and automated solution that ensures authenticity and prevents fraud.

### B. Objectives

The key objectives of the proposed system are: (1) To develop a secure web-based application for academic certificate verification using blockchain technology.(2 To implement SHA-256 hashing and smart contracts for tamper-proof storage of certificate data. (3) To enable instant verification of certificates through hash comparison and blockchain validation. (4) To provide role-based access for Admin and Student for efficient system usage. (5) To integrate a Machine Learning module for performance analysis, prediction, and insights. (6). To implement an AI chatbot for assisting users and improving system usability.

## II. LITERATURE REVIEW

The rapid growth of digital technologies has significantly transformed the education sector, particularly in the area of academic record management and verification. Traditional certificate verification systems rely on centralized databases and manual validation processes, which are prone to errors, delays, and security vulnerabilities. Several researchers have explored the use of blockchain technology to address these challenges. Studies by Sharples and Domingue [1] highlight the use of blockchain for secure and decentralized educational record management, ensuring data immutability and transparency. Similarly, research by Grech and Camilleri [2] emphasizes the role of blockchain in preventing certificate forgery and improving trust in academic credentials.

Various works have focused on implementing blockchain-based certificate systems. Research by Turkanović et al. [3] introduced a blockchain-based framework for issuing and verifying educational certificates using smart contracts. Another study by Chen et al. [4] demonstrated how decentralized systems can eliminate dependency on centralized authorities and enable instant verification. The use of cryptographic hashing techniques such as SHA-256 has been widely adopted for ensuring data integrity and tamper detection in such systems [5].

Smart contracts play a crucial role in automating verification processes on blockchain platforms. Solidity-based smart contracts on Ethereum have been used effectively for storing and validating certificate hashes [6]. Tools like Ganache and MetaMask provide a development and testing environment for deploying blockchain applications, making the implementation process more efficient [7]. Spring Boot has been widely used for developing secure and scalable backend services, while REST APIs enable seamless communication between frontend and backend systems [8].

Machine Learning techniques have also been integrated into modern academic systems for performance analysis and prediction. Algorithms such as Linear Regression, Decision Trees, and classification models are commonly used to analyze student performance trends and provide insights [9], [10]. These models help in identifying weak areas and predicting future academic outcomes. Additionally, AI-based chatbots have been widely adopted in educational platforms to provide automated assistance and improve user interaction [11].

Despite these advancements, many existing systems lack a fully integrated solution that combines blockchain-based verification, AI-driven analytics, and intelligent user assistance. Most systems either focus only on certificate storage or basic verification without incorporating performance analysis or chatbot support. The proposed system aims to bridge these gaps by providing a secure, intelligent, and user-friendly platform for academic certificate verification and analysis.

## III. METHODOLOGY

The proposed Blockchain-Based Academic Certificate Verification System is developed using a modular SDLC approach. The system is implemented as a web-based application accessible through modern browsers. The React.js frontend provides role-specific user interfaces for Admin and Student. The Spring Boot backend handles business logic, database operations (MySQL/MongoDB), blockchain interaction (Ethereum using Ganache and MetaMask), authentication (JWT), and external integrations.

The system integrates multiple modules through REST APIs with Role-Based Access Control (RBAC) enforced at every level. Certificate data is processed using SHA-256 hashing and stored on the blockchain using smart contracts, ensuring data immutability and security. Additionally, Machine Learning models are integrated for result analysis, and an AI chatbot is included for user assistance.

### A. System Architecture

The system follows a four-layer architecture. The Presentation Layer is built using React.js and provides interfaces such as Admin Dashboard, Student Dashboard, and Verification screens. The Application Layer is implemented using Spring Boot (Java) and includes services such as Authentication (JWT), Student Management, Result Management, Blockchain Service, Verification Service, ML Analysis Service, and Chatbot Service.

The Blockchain Layer uses Ethereum (Ganache) with Solidity-based smart contracts to store and retrieve certificate hashes securely. MetaMask is used for transaction handling and wallet interaction.

The Data Layer consists of MySQL/MongoDB databases for storing student records, results, and metadata. External services include QR Code Generator, AI Chatbot API, and REST API communication between frontend and backend.

### B. Modules

The system consists of the following integrated modules:

(1) Admin Module: Manages student records, issues results, and stores certificate hashes on blockchain.(2) Student Module: Allows students to view results, download certificates, and access verification features.(3) Result Management Module: Handles marks entry, grade calculation, and result generation.(4) Blockchain Module: Generates SHA-256 hash and stores/retrieves it using smart contracts.(5) Verification Module: Performs certificate validation by comparing generated hash with blockchain-stored hash (auto database verification).(6) QR Code Module: Generates QR codes for quick verification access. (7) Machine Learning Module: Analyzes student performance and provides predictions such as CGPA, rank, and improvement suggestions. (8) Chatbot Module (CertBot): Assists users with queries related to results, verification, and system usage.(9) Authentication Module: Implements secure login using JWT for Admin and Student roles.

### C. Data Flow

The Level 0 DFD (Context Diagram) represents the system as a single process interacting with external entities such as Admin and Student. Data inputs include login credentials, student details, marks entry, and verification requests. Outputs include verified results, blockchain hash data, and analysis reports.The Level 1 DFD decomposes the system into multiple sub-processes:User Authentication (P1), Student Management (P2), Result Generation (P3), Blockchain Storage (P4), Verification Process (P5), QR Code Generation (P6), ML Analysis (P7), and Chatbot Interaction (P8).The data flow ensures secure transmission of data between frontend, backend, database, and blockchain layers, maintaining integrity and transparency throughout the system.

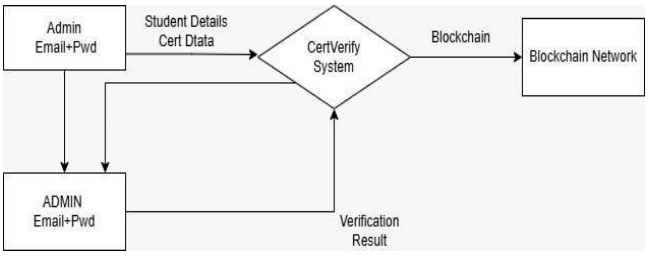


*Fig. 5. DFD Level-0 (Context Diagram) — Certificate Verification System*

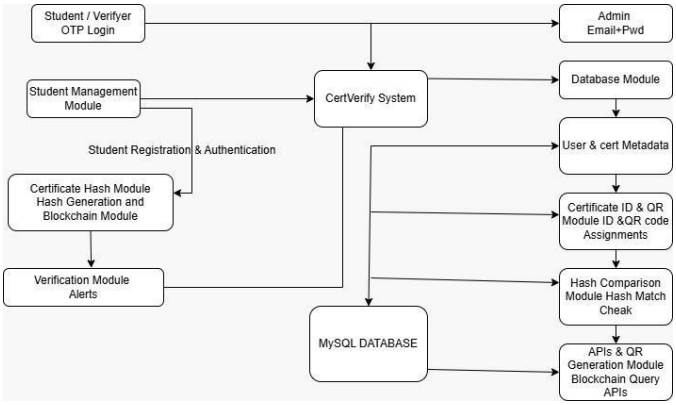


*Fig. 6. DFD Level-1 Decomposed Process View of Certificate Verification System*

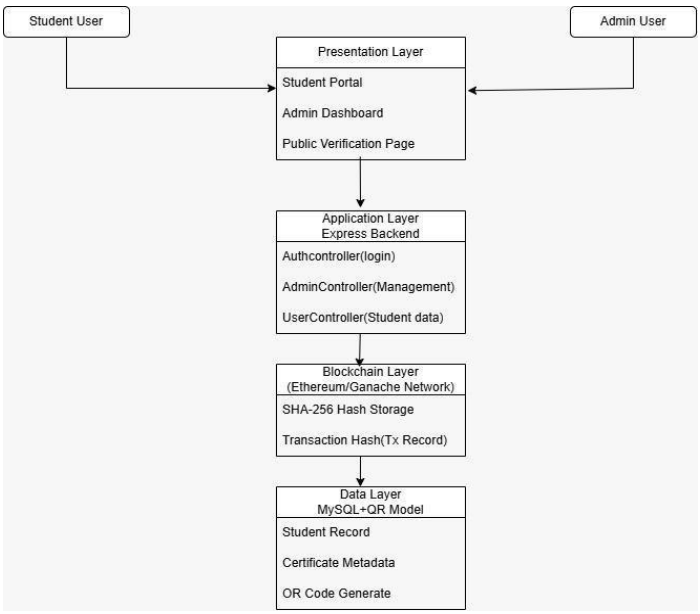


*Fig. 7. System Architecture of Blockchain Based Academic Certificate Verification System showing presentation, Application, Blockchain and Data Layers.*

## IV. SYSTEM REQUIREMENTS

The The proposed Blockchain-Based Academic Certificate Verification System implements multiple functional requirements to ensure secure, efficient, and reliable certificate management and verification. The system includes the following key functionalities:

(1) User Authentication with RBAC: Secure login system using JWT for Admin and Student roles, ensuring controlled access to system functionalities.(2) Admin Dashboard: Provides features for managing student records, issuing results, and monitoring blockchain transactions.(3) Student Dashboard: Allows students to view results, access verification features, and generate QR codes. (4) Result Management: Enables entry of marks, calculation of grades, and generation of academic results.(5) Blockchain Integration: Uses Ethereum (Ganache) and smart contracts to store certificate hashes securely.(6) Hash Generation: Implements SHA-256 algorithm to generate unique hash values for certificate data.(7) Certificate Verification: Performs auto-database verification by comparing generated hash with blockchain-stored hash (no file upload required).(8) QR Code Integration: Generates QR codes for quick and easy certificate verification.(9) Machine Learning Module: Provides student performance analysis and prediction based on marks, CGPA, and attendance using ML algorithms.(10) AI Chatbot Module: Assists users by answering queries related to verification, results, and system usage.

The system includes the following data models :User Model: Stores login credentials, roles (Admin/Student), and session information. Student Model: Contains student details such as ID, name, course, and academic records. Result Model: Stores marks, grades, CGPA, and result status. Blockchain Model: Stores transaction hash, block number, and verification ID.Verification Model: Handles verification requests and hash comparison results. QR Code Model: Stores generated QR code data linked with verification ID. ML Model: Stores input features (marks, CGPA, attendance) and prediction outputs. Chatbot Model: Handles user queries and responses for system assistance.

## V. TESTING RESULTS

Testing was conducted on the web-based Blockchain-Based Academic Certificate Verification System using functional testing, validation testing, and performance testing. The system was tested across Admin and Student modules, blockchain integration, and verification processes. All test cases passed successfully,

confirming system reliability and readiness for deployment.

### A. Admin Module – Dashboard and Student Management

Upon login as Admin, the system displays the dashboard with key metrics such as Total Students, Results Issued, Pending Results, and Blockchain Status (Connected).The Admin can successfully: Add new student records ,View and manage student data, Navigate through dashboard features. All functionalities worked correctly, and data was stored in the database without errors. Test cases TC-001 to TC-006 passed successfully.

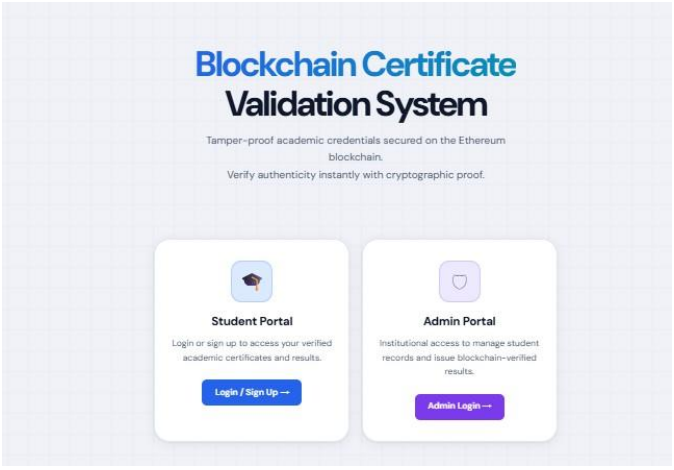


Fig. 1. System Home Page – Student/Admin Portal Access

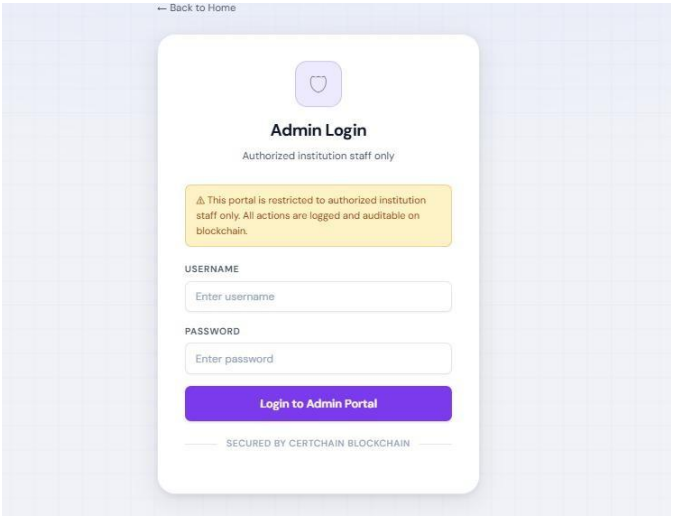


Fig. 2. Admin Login Screen – Secure Authentication

### B. Result Generation and Blockchain Storage Module

The Admin enters student marks, subjects, and grades through the result entry form. Upon submission: The system generates a SHA-256 hash of the certificate data. The hash is stored on the blockchain using smart contracts. A unique Verification ID and transaction details are generated. The blockchain connection was successfully established using Ganache and MetaMask, and all transactions were recorded correctly. Test cases TC-007 to TC-012 passed successfully.

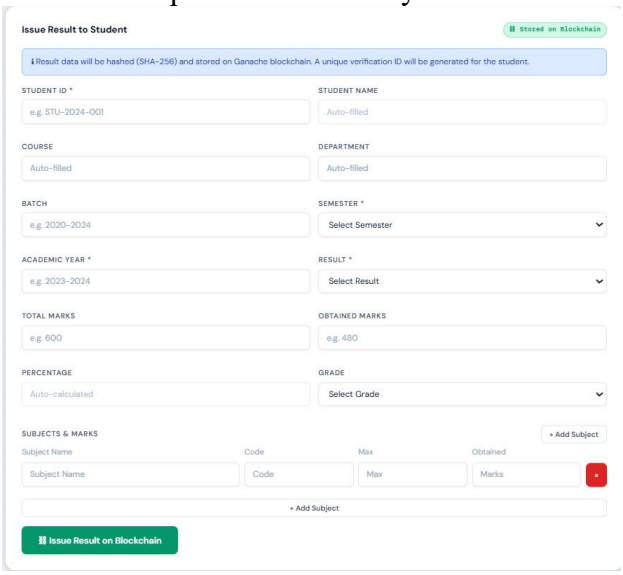


Fig. 3. Issue Result Interface – Blockchain Storage Process hi kay pages

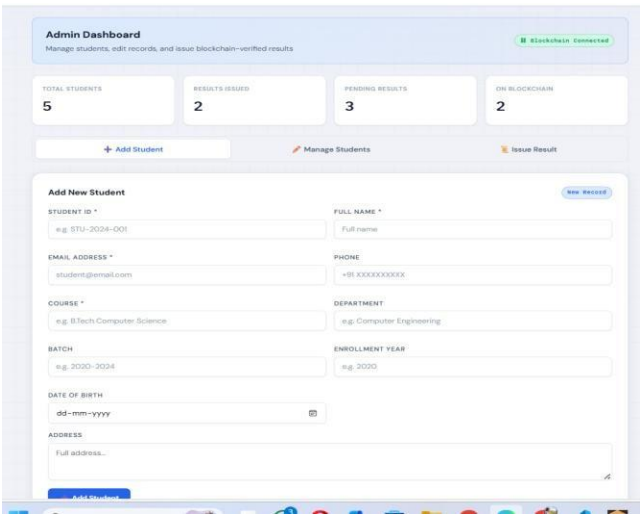


Fig. 4. Admin Dashboard – Student and Result Management

### C. Student Module – Dashboard and Result Viewing

The Student Module allows users to: Login using credentials. View academic results. Access blockchain verification details. Generate QR codes for verification. The student dashboard displayed accurate data retrieved from the database and blockchain. Test cases TC-013 to TC-017 passed successfully.

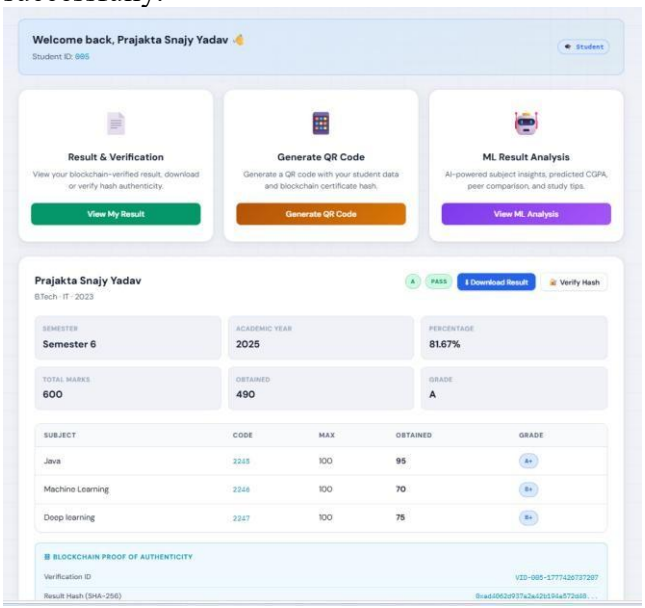


Fig. 5. Student Dashboard – Result and Verification Access

### D. Certificate Verification Module

The verification module performs auto-database verification without requiring file upload. The user enters a verification ID or scans a QR code.

The system: Generates a new hash from stored data. Retrieves the corresponding hash from the blockchain. Compares both hashes. If matched → Valid Certificate. If not matched → Invalid Certificate. The verification process was fast and accurate, confirming system integrity. Test cases TC-018 to TC-022 passed successfully.

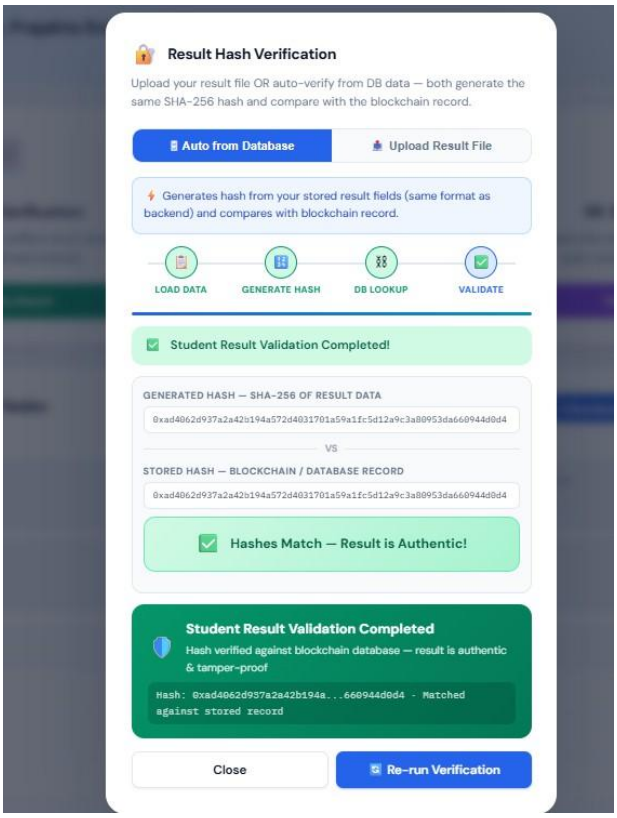


Fig. 6. Verification Interface – Enter Verification ID / QR Scan

## VI. CONCLUSIONS

The Blockchain-Based Academic Certificate Verification System developed using Java (Spring Boot backend), React.js (frontend), MySQL/MongoDB (database), and Ethereum blockchain (Ganache, MetaMask, and Smart Contracts) successfully addresses the major challenges associated with traditional certificate verification systems. The system ensures secure, tamper-proof, and instant verification of academic certificates using SHA-256 hashing and blockchain technology.The Admin Dashboard enables efficient management of student records and result generation, while the blockchain integration ensures that certificate data cannot be altered once stored. The verification module provides reliable validation through auto-database hash comparison, eliminating the need for manual verification or file uploads.

The Student Dashboard provides easy access to results, blockchain proof of authenticity, and QR code-based verification, enhancing usability and

accessibility. The integration of the Machine Learning module enables performance analysis, prediction of CGPA, and insights for improvement. Additionally, the AI chatbot (CertBot) improves user interaction by providing instant responses to queries related to results and verification.The system demonstrates high reliability, accuracy, and efficiency during testing, making it suitable for real-world academic institutions and digital verification platforms.

Future work includes deployment on a live Ethereum network, enhancement of smart contract security, integration with national academic databases, support for multi-language interfaces, mobile application development, and advanced AI models for deeper performance analytics and recommendations.

## VII. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Prof. Supriya S. Chougule, Assistant Professor, Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, for her valuable guidance, continuous support, and encouragement throughout the development of the project “Blockchain-Based Academic Certificate Verification System.”The authors are also thankful to the founder Chairman Late Dr. J. J. Magdum and Chairman Mr. Vijayraj J. Magdum of Dr. J. J. Magdum Trust, for providing the necessary infrastructure and academic environment to carry out this work successfully. Special thanks are extended to Principal Dr. G. V. Mulgund, Prof. Dr. A. M. Chougule (Head, Department of CSE), and the DRC Committee for their support, suggestions, and valuable feedback during the project development. The authors also acknowledge the support of faculty members, friends, and colleagues who directly or indirectly contributed to the successful completion of this project.

## VIII. REFERENCES

[1] ACFE (Association of Certified Fraud Examiners). (2023). Report to the Nations: 2023 Global Study on Occupational Fraud and Abuse. Austin, TX: ACFE.

[2] ACFE (Association of Certified Fraud Examiners). (2023). Report to the Nations: 2023 Global Study on Occupational Fraud and Abuse. Austin, TX: ACFE.

[3] Allen, C., Brock, A., Buterin, V., Callas, J., & Dorman, D. (2017). Decentralized Public Key Infrastructure. IETF Internet Draft.R. Heeks, "Reinventing Government in the Information Age," Routledge, London, 1999.

[4] Bacis, E., De Capitani di Vimercati, S., Foresti, S., Paraboschi, S., Rosa, M., & Samarati, P. (2020). Distributed Shuffle Index in the Cloud: Implementation and Evaluation. IEEE Transactions on Cloud Computing, 8(4), 1244–1257.

[5] Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint Archive, 2018/046.

[6] Benarroch, D., Gurkan, K., Lubarov, V., Nitulescu, A., & Sonnino, A. (2020). Zk-Proof Community Reference Document. zkproof.org.

[7] Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In EUROCRYPT 2001, LNCS 2045, 93–118.

[8] Canetti, R. (2001). Universally Composable Security: A New Paradigm for Cryptographic Protocols. In 42nd IEEE Symposium on Foundations of Computer Science (FOCS 2001), 136–145.

[9] Chen, G., Xu, B., Lu, M., & Chen, N.S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1.

[10] Finck, M. (2018). Blockchains and Data Protection in the European Union. European Data Protection Law Review, 4(1), 17–35.

[11] ] Gabizon, A., Williamson, Z.J., & Ciobotaru, O. (2019). PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. IACR ePrint Archive, 2019/953.

[12] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186–208.

[13] Groth, J. (2016). On the Size of Pairing-based Non-interactive Arguments. In EUROCRYPT 2016, LNCS 9666, 305–326.

[14] [19] V. Ravi and H. Pramod, “Patient Referral Management in Government Hospitals: A Systematic Review,” Indian Journal of Community Medicine, Vol. 46, No. 3, pp. 388–393, 2021.

[15] [20] G. Shortliffe and J. Cimino, Eds., Biomedical Informatics: Computer Applications in Health Care and Biomedicine, 4th ed., Springer, London, 2014.

[16] [21] P. Narayana and K. Reddy, “Automated Pharmacy Inventory Management System for Hospitals,” International