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.2025.75385

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

Verification and Validation of Certificate Using Blockchain

Krutant Dongare[1], Shivani Waghmare[2], Shruti Bobade[3], Sakshi Gogulwar[4], Achal Gothe[5], Vaishnavi Jayshingkar[6], Amol Dhankar[7]
Department of Computer Science Engineering, GH Raisoni College of Engineering, Amravati University, Maharashtra, India

Abstract: ***The Verification and Validation of Certificate Using Blockchain system is designed to provide a secure, transparent, and tamper-proof mechanism for issuing and verifying educational and professional certificates. Traditional verification methods are often prone to forgery, delays, and administrative inefficiencies due to centralized databases and manual validation. This system leverages blockchain technology to store certificate data in an immutable distributed ledger, ensuring authenticity and preventing manipulation. Additionally, the integration of the InterPlanetary File System (IPFS) provides decentralized, low-cost storage for certificates, while an Android-based interface simplifies issuance and verification processes. By enabling decentralized trust, rapid verification, and cross-border accessibility, this system enhances transparency, reduces fraudulent activities, and establishes a reliable digital framework for secure credential management.***

Keywords: Blockchain, Certificate Verification, IPFS, Decentralized System, Digital Authentication, Smart Contracts, Data Security.

I. INTRODUCTION

In today's digital era, the authenticity and reliability of academic and professional certificates have become a major concern for institutions, employers, and individuals alike. Traditional certificate management systems, which rely on centralized databases and manual verification methods, are highly vulnerable to forgery, duplication, and unauthorized manipulation. As a result, fake degrees and falsified credentials have become increasingly common, causing significant challenges in recruitment, higher education admissions, and governmental verification processes. These issues highlight the urgent need for a secure, transparent, and tamper-proof mechanism that can ensure the originality and legitimacy of certificates issued by educational and professional institutions.

The Verification and Validation of Certificate Using Blockchain system addresses these challenges by introducing a decentralized framework for certificate issuance and authentication. Blockchain technology serves as the backbone of this system, providing an immutable ledger that securely records every transaction related to certificate creation, storage, and verification. Each certificate is assigned a unique cryptographic hash, making it impossible to alter or forge without detection. This ensures that only legitimate certificates issued by authorized institutions are recorded and accessible through the blockchain network. Furthermore, by eliminating third-party intermediaries, the system enhances trust and transparency among all stakeholders — students, institutions, and verifiers. Another critical component of this system is the InterPlanetary File System (IPFS), which provides decentralized and cost-efficient storage for certificate data. IPFS allows large files such as degree certificates and transcripts to be stored securely without depending on a single centralized server. The blockchain stores only the reference hash of the document, while the actual file resides on IPFS, ensuring efficiency, scalability, and data integrity. This dual-layer design not only enhances the overall performance of the system but also ensures that certificates remain accessible globally, even in the event of server failures or institutional changes. To ensure user convenience, the system includes an Android-based application that allows institutions to issue digital certificates, students to securely store and manage their credentials, and employers to instantly verify the authenticity of submitted documents. This mobile interface bridges the gap between blockchain technology and real-world users, offering a simple yet highly secure verification experience. The system automates verification processes, significantly reducing administrative costs and time delays while maintaining the highest level of security and transparency.

In conclusion, the Blockchain-Based Certificate Verification and Validation System provides a revolutionary solution to modern challenges in academic and professional credential management. By integrating blockchain and IPFS technologies, it ensures data immutability, decentralized trust, and efficient global accessibility. This system not only prevents forgery and fraud but also builds a foundation for a more reliable and transparent digital verification ecosystem, paving the way for the future of secure credential management across educational, governmental, and corporate sectors.

II. AIMS & OBJECTIVES

A. Aim

The main aim of the Verification and Validation of Certificate Using Blockchain system is to develop a secure, transparent, and decentralized platform for issuing, storing, and verifying educational and professional certificates. The system seeks to eliminate document forgery, reduce verification time and cost, and establish trust among institutions, employers, and individuals through blockchain technology and distributed storage mechanisms.

B. Objectives

1) To create a tamper-proof mechanism that guarantees the originality and legitimacy of certificates using blockchain's immutable ledger.
2) To protect academic and professional credentials from being altered, copied, or counterfeited by unauthorized individuals.
3) To promote trust among students, institutions, and organizations by providing a transparent verification process without reliance on a central authority.
4) To remove third-party dependency by enabling blockchain-based decentralized validation of credentials.
5) To ensure that verified certificates can be accessed and validated across borders, institutions, and industries in real time.
6) To automate and simplify the verification process, minimizing administrative workload and reducing the time required for authentication.
7) To empower individuals with full control over their digital certificates, allowing them to manage and share credentials securely.
8) To include a mechanism for institutions to revoke or update certificates (e.g., expired licenses or withdrawn degrees) transparently through blockchain.
9) To use IPFS (InterPlanetary File System) for efficient, decentralized, and reliable storage of certificate documents linked to blockchain transactions.
10) To establish a unified and universally verifiable format for digital certificates that can be adopted by multiple institutions and industries.

Overall, the system's aim and objectives align to create a robust, trustworthy, and future-ready digital certificate management framework that enhances security, accessibility, and efficiency in academic and professional verification processes.

III. LITERATURE SURVEY

1) Verification and Validation of Certificate Using Blockchain (2021): This paper proposes a blockchain-based system to prevent fake educational certificates in India. It converts paper certificates into digital files, generates hash values, and stores them on the blockchain for immutability and anti-forgery protection. QR codes allow easy verification via mobile or web, ensuring authenticity and transparency.
2) Performance Analysis of E-Certificate Generation and Verification Using Blockchain and IPFS (2022): The study introduces a blockchain and IPFS-based e-certificate system to eliminate fake degrees. Certificates are digitized, hashed, and stored on the blockchain, with unique IDs for each record. Verification is done by matching hash values, ensuring high security, efficiency, and eco-friendliness.
3) Certificate Verification and Validation Using Blockchain (2023): This paper focuses on managing academic certificates like SSLC, HSC, and degrees through blockchain. Certificates are digitized, hashed, and stored on the blockchain for tamper-proof storage. A mobile app enables fast and reliable verification anytime, improving accessibility and trust.
4) Blockchain Enabled Certificate Verification and Validation (2024): This research converts traditional certificates into secure digital forms using chaotic algorithms for unique hashing. Hashes are stored on the blockchain, and verification is done via QR scanning or online tools. The system ensures transparency, integrity, and trust between institutions and users.
5) Secure Academic Certificate Authentication Using Blockchain Technology (2025): The paper proposes a blockchain framework using Ethereum smart contracts and IPFS for decentralized certificate authentication. It ensures immutability, eliminates third-party involvement, and enables instant, tamper-proof verification. Results show improved efficiency, security, and trust over traditional methods.

IV. METHODOLOGY

The Verification and Validation of Certificate Using Blockchain system follows a structured and systematic methodology that combines blockchain technology, decentralized storage, and user-friendly digital interfaces to ensure secure and tamper-proof management of educational and professional certificates.

The methodology focuses on designing a system that provides transparency, efficiency, and authenticity in the certificate issuance and verification process. It involves multiple stages including system design, data acquisition, blockchain integration, application development, testing, and deployment. Each phase plays a critical role in achieving the project's overall objective of creating a reliable and decentralized certificate verification platform.

A. Requirement Analysis and System Design

The first stage of the methodology involves identifying the existing challenges in traditional certificate verification systems, such as forgery, delayed validation, and centralized data storage vulnerabilities. Once the requirements were gathered, a system design was formulated to address these problems using blockchain and IPFS. The design includes various modules such as certificate issuance, blockchain registration, certificate verification, and user authentication. The system architecture was structured to ensure smooth communication between the mobile interface, the blockchain network, and the decentralized storage component. Data flow diagrams and system architecture diagrams were developed to visualize interactions among components.

B. Blockchain Integration and Smart Contract Design

In this stage, blockchain technology serves as the backbone of the system. A smart contract is developed and deployed on the blockchain to handle the creation, verification, and storage of certificate hashes. Each certificate is represented by a unique cryptographic hash generated from its metadata (student name, course, institution, issue date, etc.). When a certificate is issued, its hash is stored permanently on the blockchain ledger, ensuring immutability. Any attempt to alter or forge the certificate will result in a mismatch between the stored hash and the modified document, thereby detecting tampering instantly. The blockchain also enables transparent and distributed verification, where trust is shared across multiple nodes rather than relying on a single authority.

C. Decentralized Storage Using IPFS

Since storing complete certificate files on the blockchain is inefficient, the system integrates InterPlanetary File System (IPFS) for decentralized and efficient document storage. IPFS breaks the certificate file into smaller chunks and distributes them across multiple nodes in the network, providing redundancy and faster retrieval. The blockchain stores only the hash reference to the certificate file on IPFS, which ensures that the data remains secure and verifiable without bloating the blockchain. This combination enhances both security and scalability while keeping storage costs low.

D. Android Application Development

The user interface is developed as an Android application to allow students, institutions, and employers to interact easily with the system. Institutions use the app to issue certificates, which are then automatically hashed and stored on the blockchain. Students can view and manage their verified certificates, while employers can scan a QR code or enter a transaction ID to validate authenticity. The application communicates with the blockchain network through APIs, ensuring real-time verification. It was designed with usability in mind, providing a simple layout while maintaining a high level of encryption and security for all operations.

E. Verification Process

When an employer or verifier wants to confirm a certificate's authenticity, they use the verification feature of the application. The verifier enters the unique hash or scans the QR code printed on the digital or physical certificate. The system then checks this hash against the blockchain records. If the hash matches the one stored on the blockchain, the system confirms the certificate as valid and untampered. If not, it alerts the verifier that the certificate has been modified or is fraudulent. This automated process eliminates manual verification steps and ensures quick, trustworthy results.

F. Testing and Validation

After implementation, the system undergoes rigorous testing to ensure it meets security, functionality, and performance requirements. Unit testing validates individual modules, integration testing checks communication between blockchain, IPFS, and the mobile app, and system testing evaluates the overall functionality under real-world conditions. User Acceptance Testing (UAT) ensures that the application meets end-user needs, providing a seamless experience for all stakeholders. The validation results confirm the accuracy, speed, and immutability of blockchain-stored certificates.

G. Deployment and Maintenance

Once fully tested, the system is deployed on a cloud-supported blockchain network to ensure scalability and reliability. Regular maintenance updates are planned to enhance smart contracts, improve user interfaces, and upgrade security protocols. Institutions can continuously issue new certificates through the app, while verifiers and students can access and verify them globally. The decentralized architecture ensures that the system remains operational even if one or more nodes fail, maintaining high system availability.

The methodology effectively combines modern technologies — blockchain, IPFS, and mobile application development — to create a decentralized, secure, and efficient certificate verification system. Blockchain ensures data integrity and transparency, IPFS provides scalable decentralized storage, and the Android app enables real-time user interaction. This integrated approach eliminates the possibility of forgery, reduces verification time, and promotes global trust in digital certificates, marking a major advancement in the modernization of credential management systems.

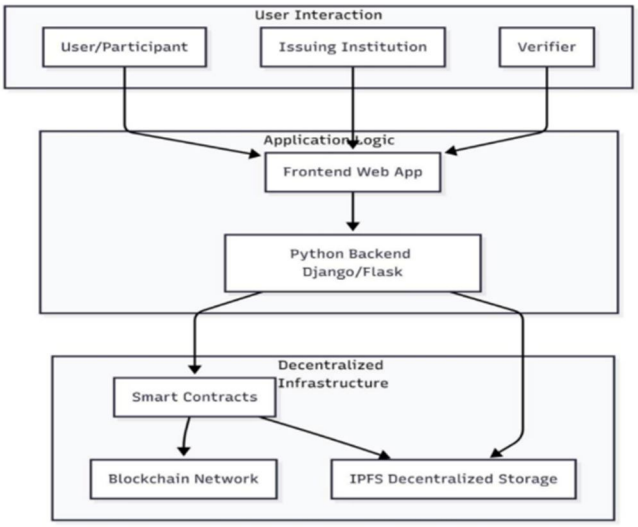


Figure 1: Block Diagram

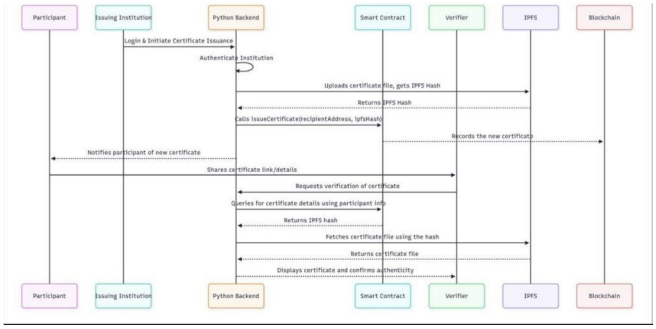


Figure 2: Sequence Diagram

V. RESULTS

The implementation of the Verification and Validation of Certificate Using Blockchain system yielded highly positive results, demonstrating its effectiveness in providing a secure, transparent, and decentralized solution for digital certificate management. The system successfully prevented certificate forgery and unauthorized modification through the use of blockchain's immutable ledger and cryptographic hashing. Testing confirmed that certificates could be verified within seconds, significantly reducing the time and cost associated with traditional manual verification methods. The integration of IPFS enabled efficient, low-cost decentralized storage, ensuring that certificate files remained accessible and tamper-proof even during network failures. User feedback from institutions, students, and employers indicated high satisfaction with the system's simplicity, accuracy, and reliability, confirming its potential for large-scale adoption across educational and professional sectors.

VI. CONCLUSION

In conclusion, the Blockchain-Based Certificate Verification and Validation system effectively addresses the critical challenges of authenticity, transparency, and efficiency in digital credential management. By integrating blockchain and IPFS technologies, the system ensures tamper-proof storage, decentralized verification, and global accessibility of certificates. It eliminates the risk of forgery, minimizes administrative workload, and enhances trust among educational institutions, employers, and individuals. The Android-based interface further simplifies the issuance and validation process, making the system both user-friendly and secure. Overall, this project establishes a strong foundation for the future of digital credential verification, paving the way for a more reliable, transparent, and decentralized ecosystem in education and professional certification.

REFERENCES

[1] Said, A.G. & Ashtaputre, R.P. & Bisht, Bivas & Bandal, S.S. & Dhamale, P.N.. (2019). E-Certificate Authentication System Using Blockchain. International Journal of Computer Sciences and Engineering. 7. 191-195. 10.26438/ijcse/v7i4.191195.

[2] Nyaletey, E., Parizi, R. M., Zhang, Q., & Choo, K. K. R. (2019, July). BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 18-25). IEEE.

[3] R. Kumar, N. Marchang and R. Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), 2020, pp. 1-5, doi: 10.1109/COMSNETS48256.2020.9027313.

[4] Gayathiri, A., Jayachitra, J., & Matilda, S. (2020, July). Certificate validation using blockchain. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-4). IEEE.

[5] Pawar M.K., Patil P., Hiremath P.S. (2021) A Study on Blockchain Scalability. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore.

[6] M. K. Pawar, P. Patil, M. Sharma and M. Chalageri, "Secure and Scalable Decentralized Supply Chain Management Using Ethereum and IPFS Platform," 2021 International Conference on Intelligent Technologies (CONIT), 2021, pp. 1-5, doi: 10.1109/CONIT51480.2021.9498537.

[7] More, S. S., Patel, N., Parab, S., & Maurya, S. (2021, May). Blockchain based Tamper Proof Certificates. In Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021).

[8] Song, Z., Wang, G., Yu, Y., & Chen, T. (2022). Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior. Security and Communication Networks, 2022.

[9] N. Nousias, G. Tsakalidis, G. Michoulis, S. Petridou, K. Vergidis, “A process-aware approach for blockchain- based verification of academic qualifications,” Simul. Model. Pract. Theory, vol. 121, Art. 102642, Dec. 2022.

[10] Avni Rustemi et al., “A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification,” IEEE Access, 2023.

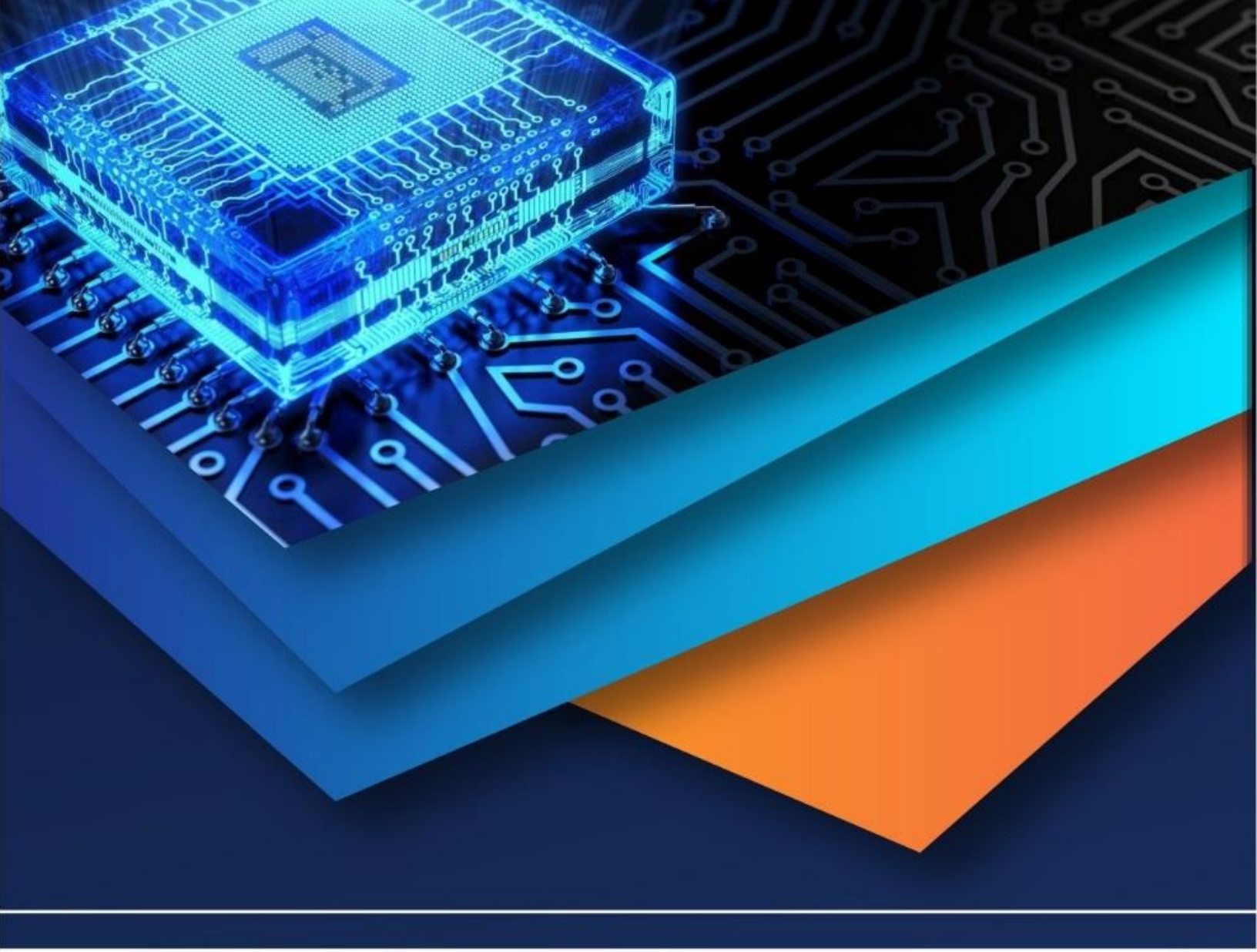
[11] Ruqaya Abdelmagid, Mohamed Abdelsalam, Fahad Kamal Alsheref, “A Blockchain Framework for Academic Certificates Authentication,” Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 7, pp. 297–305, 2024.

[12] Olaiya S. Oluwaseyi, R.O. Akinyede, “Utilizing Blockchain Technology for University Certificate Verification System,” Int. J. Appl. Inf. Syst., vol. 12, no. 45, Aug 2024.

[13] S. Venkatramulu, K.V. Kumar, Md. S. Waseem,S.Mahveen, V. Vaidya, T.R. Reddy, S.T. Devarakonda,“A Secure Blockchain-Based Student CertificateGeneration and Sharing System,” J. Sensors, IoT&Health Sci., vol. 2, no. 1, pp. 17–27, Mar. 2024.

[14] Ayush Mishra et al., “Blockchain-Based Decentralized Document Verification and Its Applications,” J. Inf. Syst. Eng. & Management, vol. 10, no. 10 s, pp. 137–151, Feb 2025.

[15] J. Patel, A. Vishwakarma, M. Kaif, S. Ali,“Leveraging Blockchain Technology for GovernmentCertificate Authentication and Validation,”IJRASET,vol. 13, no. 6, Art. 69312, Apr. 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY