iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79791

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 14 Issue IV Apr 2026- Available at www.ijraset.com

Digital Certification Using DSS and Blockchain

Aantonio Vivin A, Aldrin Graceson C, Bala Subramanian S, Prof. Aravind Swaminathan G
Computer science Engineering (CSE), Francisxavier Engineering college, Tirunelveli, Tamilnadu, India

Abstract: ***The increasing demand for secure, transparent, and tamper-proof digital credential management systems has highlighted the limitations of traditional certificate verification approaches, which rely on centralized storage, manual validation, and third-party authentication. These conventional methods are often vulnerable to forgery, data manipulation, and verification delays. To address these challenges, this research proposes a Blockchain-Based Digital Certificate Generation and Validation System integrated with Digital Signature Scheme (DSS) and Decentralized Identity (DID) to provide a secure, automated, and trustless verification platform.***

The proposed system employs cryptographic hashing techniques to convert certificate data into unique digital fingerprints, which are then securely anchored on the Ethereum blockchain through smart contract execution. Digital signature mechanisms ensure certificate authenticity and non-repudiation, while decentralized identity frameworks enable privacy-preserving credential ownership and selective information sharing. A web-based portal facilitates certificate issuance by authorized institutions and enables real-time verification by employers or third-party verifiers without requiring direct communication with the issuing authority.Certificate validation is performed by recalculating the hash of submitted credential data and comparing it with immutable blockchain records. The system provides instant verification results, significantly reducing operational delays and eliminating the risk of fraudulent certificates.

Index Terms: Blockchain, Digital Certificate Verification, Smart Contracts, Cryptographic Hashing, Digital Signature Scheme (DSS), Decentralized Identity (DID), Ethereum, Secure Credential Management.

I. INTRODUCTION

In recent years, the rapid growth of digital technologies has significantly transformed the way academic and professional credentials are issued, stored, and verified. Educational institutions and organizations increasingly rely on digital certificate management systems to handle large volumes of credentials efficiently. However, traditional certificate verification methods are still dependent on centralized databases, manual validation procedures, and third-party verification processes. These approaches are often time-consuming, prone to forgery, and vulnerable to data manipulation or loss.Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized, transparent, and tamper-resistant platform for secure data management. With the integration of cryptographic hashing and smart contract mechanisms, blockchain enables the creation of immutable digital records that can be verified without the need for intermediaries. This ensures authenticity, integrity, and trust in the certificate verification process.

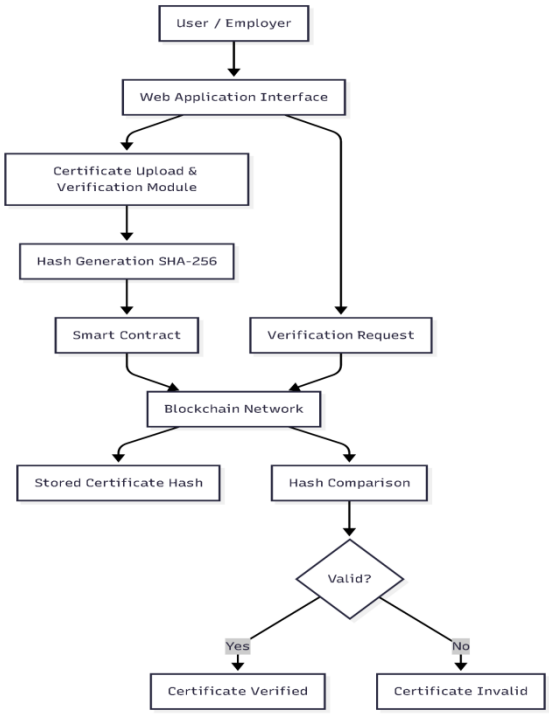
The proposed Digital Certificate Generation and Validation System using Blockchain and Digital Signature Scheme (DSS) aims to modernize traditional credential management by introducing a secure and automated verification framework. In this system, certificates are issued by authorized institutions and converted into cryptographic hash values, which are then stored on the blockchain network. Digital signatures further enhance security by ensuring that certificates cannot be altered or forged after issuance.

II. LITERATURE SURVEY

In recent years, blockchain technology has gained significant attention in the field of digital credential management due to its decentralized, transparent, and tamper-resistant characteristics. Researchers have explored various blockchain-based solutions to overcome challenges associated with traditional certificate verification systems, such as forgery, data manipulation, lack of interoperability, and time-consuming manual verification processes

Early studies on digital certificate management primarily focused on centralized database systems, where educational institutions stored student records and certificates in local servers or cloud platforms. Although these systems improved accessibility compared to paper-based certificates, they still suffered from security vulnerabilities, single-point failure risks, and dependency on third-party verification. Unauthorized access or database breaches could lead to certificate tampering or data loss.

Several researchers proposed blockchain-based certificate repositories that store certificate hashes on distributed ledgers to ensure immutability and transparency. These systems demonstrated the potential of blockchain in preventing certificate forgery and enabling remote verification without contacting the issuing authority. However, many existing solutions lacked comprehensive identity management mechanisms and privacy-preserving data sharing features.



More recent approaches have integrated smart contracts to automate certificate issuance and validation processes. Smart contracts enable predefined rules for certificate generation, verification, and revocation, thereby reducing manual intervention and improving efficiency. Some studies also explored the use of decentralized identity (DID) frameworks to allow users to control and share their credentials securely.

III. METHODOLOGY

The methodology of the Digital Certificate Generation and Validation System using Blockchain and Digital Signature Scheme (DSS) describes the systematic approach followed to design, develop, and implement a secure decentralized credential management platform. The proposed system integrates blockchain technology, cryptographic hashing, smart contracts, and decentralized identity mechanisms to enable secure certificate issuance, storage, and verification.

A. Certificate Data Generation and Issuance

The first step in the system involves generating digital certificates by authorized institutions such as universities or organizations. Certificate details including student name, course, issue date, certificate ID, and institution credentials are collected and structured into digital format.

The issuing authority authenticates itself through a blockchain wallet (such as MetaMask), ensuring that only authorized entities can issue certificates. Once validated, the certificate data is prepared for secure storage and blockchain integration.

B. Cryptographic Hash Generation

After certificate creation, the system applies a secure hashing algorithm (such as SHA-256) to convert certificate data into a unique cryptographic hash value. This hash acts as a digital fingerprint of the certificate.Even a minor change in certificate data results in a completely different hash value, thereby ensuring data integrity and preventing tampering or forgery tampering or forgery.

C. Digital Signature Application (DSS)

To enhance authenticity, the issuing authority digitally signs the certificate using cryptographic key pairs. The digital signature scheme ensures that the certificate originates from a trusted source and cannot be altered without invalidating the signature.This step provides an additional security layer beyond blockchain storage by embedding cryptographic proof directly within the certificate.

D. Certificate Verification Process

When a verifier (such as an employer or institution) needs to validate a certificate, the system recalculates the hash from the provided certificate data and compares it with the hash stored on the blockchain.If both values match, the certificate is considered authentic and valid. This automated verification process eliminates the need for manual validation or third-party involvement, thereby reducing time and operational cost.

E. User Interface and Feedback Mechanism

The system provides an interactive web interface for certificate issuance, viewing, sharing, and verification. Users receive real-time feedback regarding the status of certificate validation.Successful verification confirms authenticity, while mismatched hash values indicate possible tampering or invalid credentials. This feedback mechanism improves transparency and user trust in the system.

IV. PROPOSED METHODOLOGY

The proposed methodology focuses on designing and implementing a secure decentralized digital certificate generation and validation platform using Blockchain technology, Smart Contracts, Digital Signature Scheme (DSS), and Decentralized Identity (DID). The system enables authorized institutions to issue tamper-proof digital certificates, while allowing users and verifiers to perform real-time authentication without relying on third-party intermediaries.

A. Certificate Issuance by Authorized Authority

The process begins with certificate generation by an authorized institution such as a university or organization. The institution enters certificate details including student information, course details, issue date, and unique certificate ID through a web-based interface.The issuing authority authenticates itself using a blockchain wallet (e.g., MetaMask), ensuring that only verified entities can create and register certificates in the system.

B. Cryptographic Hashing of Certificate Data

Once certificate details are submitted, the system generates a secure cryptographic hash using algorithms such as **SHA-256**. This hash serves as a unique digital fingerprint representing the certificate data.Any modification in the certificate content results in a completely different hash value, thereby ensuring strong data integrity and protection against tampering or forgery.

C. Application of Digital Signature Scheme (DSS)

To provide proof of authenticity, the issuing authority digitally signs the certificate using public–private key cryptography. The Digital Signature Scheme ensures that the certificate originates from a trusted source and prevents unauthorized alterations.This layer of cryptographic security enhances trust even before blockchain verification is performed.

D. Blockchain Registration using Smart Contracts

The generated certificate hash along with essential metadata is stored on the blockchain network through Ethereum smart contracts. Smart contracts define automated rules for certificate storage, validation, and retrieval.Since blockchain operates in a decentralized and immutable manner, once the certificate hash is recorded, it cannot be modified or deleted. This guarantees transparency and long-term reliability of credential records.

E. Certificate Verification Mechanism

During verification, the verifier uploads or enters the certificate details into the system. The platform recalculates the hash of the provided certificate and compares it with the hash stored on the blockchain.If the hash values match, the certificate is declared valid and authentic. If not, the system identifies the certificate as tampered or invalid. This automated verification eliminates manual checking and reduces dependency on issuing authorities.

F. User Access, Sharing, and Feedback

The platform provides a user-friendly interface for students to view, download, and securely share their certificates. Selective disclosure mechanisms allow users to share only required credential information while maintaining privacy.

Real-time verification results and system feedback enhance transparency, improve user trust, and ensure efficient interaction between institutions, students, and employers

V. IMPLEMENTATION RESULT

The implementation of the Digital Certificate Generation and Validation System using Blockchain and Digital Signature Scheme (DSS) was carried out to evaluate the system's effectiveness in securely issuing, storing, and verifying digital certificates. The system was developed by integrating blockchain technology, cryptographic hashing, smart contracts, decentralized identity mechanisms, and a web-based user interface.During implementation, the platform was deployed in a controlled environment where authorized institutions could issue digital certificates and users could verify their authenticity. Certificate details such as student information, course name, issue date, and unique certificate ID were entered through the issuance interface. Once the certificate data was submitted, the system generated a cryptographic hash using the SHA-256 algorithm. This hash was then digitally signed by the issuing authority and recorded on the blockchain using Ethereum smart contracts.

The blockchain integration played a crucial role in ensuring immutability and transparency. Since the certificate hash was stored on a decentralized ledger, it could not be modified or deleted after registration. This feature effectively prevented certificate forgery and unauthorized alterations. MetaMask wallet authentication was used to verify the identity of issuing authorities before allowing certificate registration on the blockchain network.The verification module was tested using multiple certificate validation scenarios. When a verifier uploaded or entered certificate details, the system recalculated the hash value and compared it with the corresponding hash stored on the blockchain. In valid cases, the system successfully confirmed certificate authenticity in real time. In cases where certificate data was intentionally modified, the system correctly detected mismatched hash values and flagged the certificate as invalid or tampered.

Performance testing showed that the system provided fast verification responses due to automated smart contract execution and optimized backend processing. The decentralized storage mechanism eliminated dependency on centralized servers and reduced the need for manual verification by institutions. The results demonstrated that the proposed system improved security, reduced verification time, enhanced transparency, and increased user trust in digital credential management.Overall, the implementation validated that blockchain-based certificate systems can effectively replace traditional verification methods by providing a secure, scalable, and fraud-resistant platform for issuing and validating academic and professional credentialsFurthermore, the implementation demonstrated improved transparency and traceability of certificate records. Since all transactions were recorded on the blockchain, certificate issuance history could be audited securely without modifying existing data. The user interface design also enhanced usability by providing clear workflows for certificate issuance, preview, sharing, and verification.

Overall, the implementation results confirmed that the proposed blockchain-based certificate platform provides a robust, scalable, and fraud-resistant solution for digital credential management. The system significantly reduces manual verification effort, strengthens data security, and builds trust among institutions, students, and employers by enabling instant and tamper-proof certificate validation.

OUTPUT:

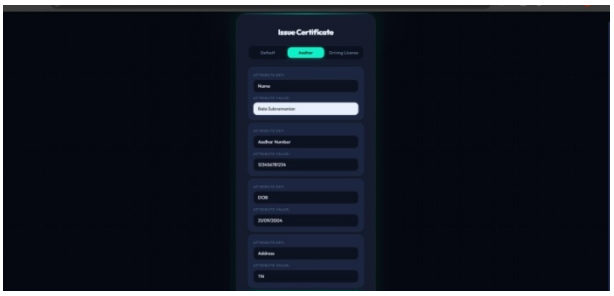


Fig: 5.1 Output screen showing the Blockchain Certificate Verification Panel

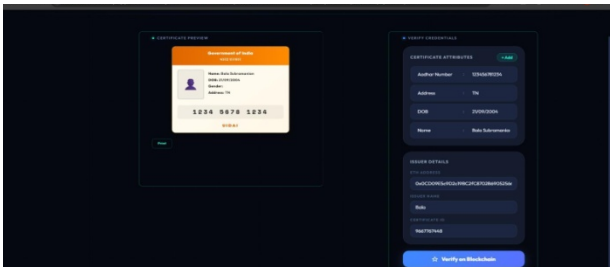


Fig 5. 2 Certificate Issuance Interface displaying Attribute Entry Form

VI. CHALLENGES FACED

During the development and implementation of the Digital Certificate Generation and Validation System using Blockchain and Digital Signature Scheme (DSS), the team encountered several technical and practical challenges. Since the system integrates blockchain technology, cryptographic mechanisms, decentralized identity, and web-based interfaces, careful planning and optimization were required to ensure secure and efficient operation.One of the major challenges faced was understanding and implementing blockchain smart contracts for certificate storage and validation. Developing smart contracts that securely store certificate hash values while preventing unauthorized access required multiple testing iterations. Gas fee management and transaction confirmation delays in the Ethereum network also affected system performance during initial testing.

Another significant challenge involved generating secure cryptographic hashes and digital signatures. Ensuring that certificate data was properly structured before hashing was important to maintain consistency during verification. Even small formatting differences in certificate data could lead to hash mismatches. The team had to implement standardized data formatting techniques to achieve reliable verification results.The integration of MetaMask wallet authenticationand decentralized identity mechanisms also posed practical difficulties. Configuring wallet connectivity, handling transaction approvals, and ensuring secure user session management required additional development effort.User unfamiliarity with blockchain wallets created usability challenges, which were addressed by simplifying the interface and providing clear interaction steps.

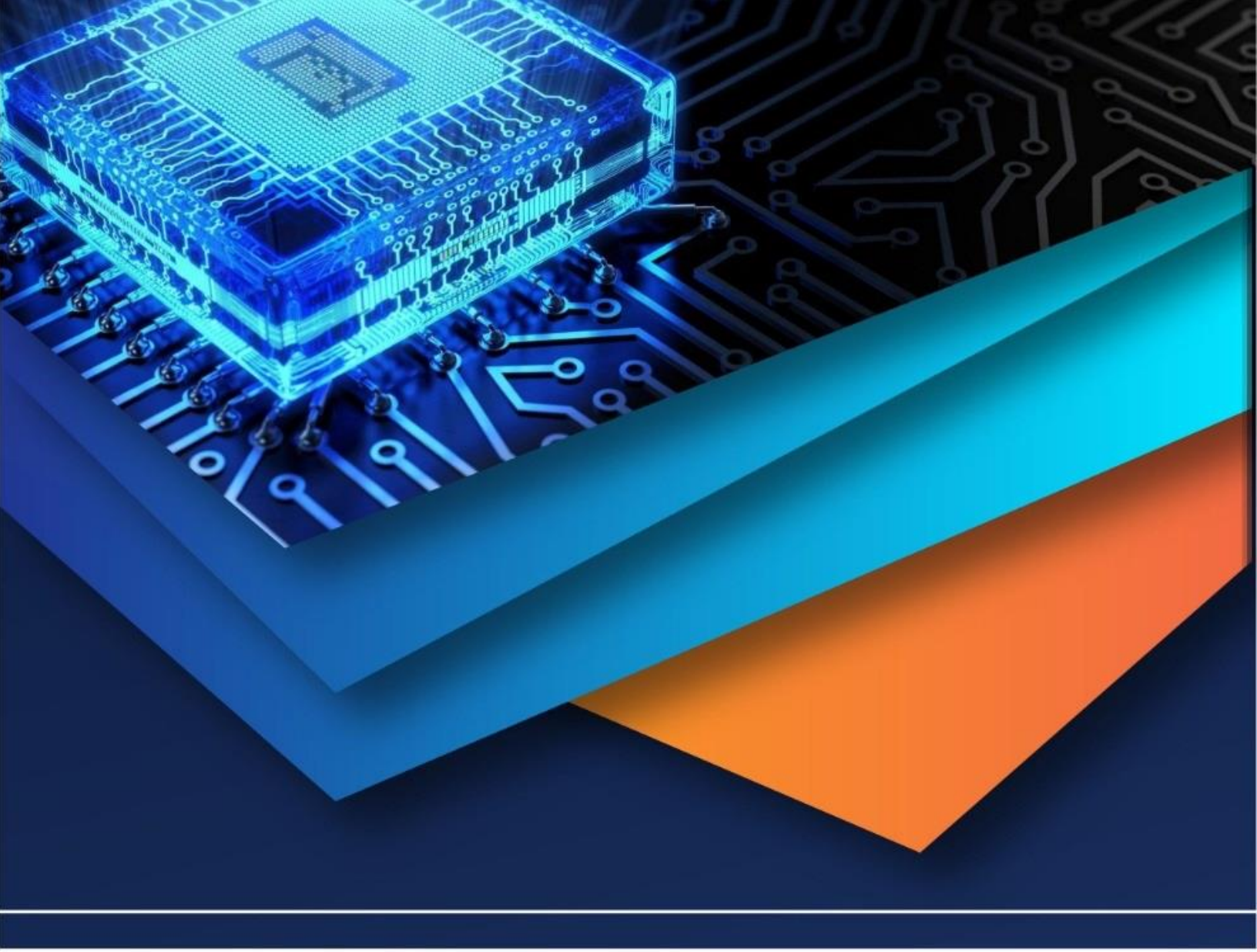
System scalability and response time were also important concerns. Blockchain transactions require network confirmation, which may introduce delays compared to traditional centralized systems. The team worked on optimizing backend processes and minimizing unnecessary blockchain interactions to improve verification speed and overall system efficiency.Another challenge was designing a user-friendly interface suitable for institutions, students, and verifiers. The platform needed to provide simple workflows for certificate issuance, viewing, sharing, and validation. Multiple interface redesigns and usability testing were conducted to ensure smooth user interaction and reduce operational complexity. Additionally, ensuring data privacy and selective disclosure required careful architectural design. The system needed mechanisms to allow users to share only necessary credential information while keeping sensitive data protected. Implementing this privacy-aware credential sharing model required additional logic and validation procedures.Through continuous testing, debugging, and optimization, these challenges were gradually resolved, resulting in a secure, reliable, and efficient blockchain-based digital certificate platform capable of addressing real-world credential verification problems.

VII. CONCLUSION

The testing and evaluation of the Digital Certificate Generation and Validation System using Blockchain and Digital Signature Scheme (DSS) demonstrated that the platform can securely issue, store, and verify digital certificates in a decentralized environment. The system successfully generated cryptographic hash values for certificate data, recorded them on the blockchain through smart contracts, and enabled real-time verification without the need for manual validation or third-party involvement.The integration of blockchain technology ensured immutability, transparency, and resistance to certificate forgery, while digital signature mechanisms provided strong proof of authenticity. The verification module accurately detected both valid and tampered certificates by comparing recalculated hash values with blockchain records. Although challenges such as blockchain transaction delays, user wallet integration, and interface usability were encountered during development, continuous optimization and testing improved system performance and reliability. In conclusion, the proposed blockchain-based certificate platform provides a secure, scalable, and efficient solution for digital credential management. It establishes a strong foundation for future advancements such as integration with decentralized identity frameworks, cross-institution credential sharing, and large-scale adoption in academic and professional verification ecosystems.

REFERENCES

[1] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[2] G. Wood, Ethereum: A Secure DecentralisedGeneralised Transaction Ledger, Ethereum Project Yellow Paper, 2014.
[3] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Penguin, 2016.
[4] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.
[5] C. Cachin, “Architecture of the Hyperledger Blockchain Fabric,” in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016
[6] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” in European Conference on Technology Enhanced Learning, 2016.
[7] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, “BERT: Pre-training of deep bidirectional transformers for language understanding,” in Proc. NAACL-HLT, 2019.
[8] A. Grech and A. Camilleri, Blockchain in Education, European Commission Joint Research Centre, 2017.
[9] J. Chen et al., “Blockchain-Based Electronic Certificate Validation System,” IEEE Access, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY