iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68159

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 IV Apr 2025- Available at www.ijraset.com

Digital Document Verification using Blockchain

Devika Sawant[1], Suvarna Potdukhe[2], Vaishnavi More[3], Prathamesh Apsingekar[4], Ashutosh Mahadik[5]
Department of Information Technology, RMD Sinhgad School of Engineering, Pune, India

Abstract: ***The Blockchain technology is used in the Digital Document Verification using Blockchain project to improve the security, authenticity, and integrity of digital documents. Conventional document verification techniques are frequently ineffective, expensive, and susceptible to fraud or manipulation. In order to overcome these difficulties, this system stores the cryptographic hash values of documents in a decentralised ledger, guaranteeing that once they are recorded, they cannot be changed or modified. A hash of the document is created at the moment of verification and compared to the hash that has already been saved on the blockchain as part of the verification process. The document is unaltered and legitimate if the hashes match; if not, any differences suggest possible changes or manipulation. By lowering reliance on centralised authority and making unauthorised alterations immediately identifiable, this technique greatly improves document security. The solution provides more openness and confidence by utilising the decentralised and irreversible characteristics of blockchain technology, guaranteeing that all verification records are permanent and available for auditing purposes. In industries including education, healthcare, law, finance, and government agencies that need strong document verification, the method is very advantageous. Additionally, automating verification procedures improves efficiency and dependability by cutting down on the time and effort needed for manual authentication. In addition to reducing the dangers of document fraud, this initiative promotes a safer and more reliable digital document management environment***

Keywords: Document Authentication, Blockchain, Transparency, Decentralization, Tamper-proof Verification.

I. INTRODUCTION

In today's digital era, ensuring the authenticity and integrity of documents is a critical requirement across multiple industries, including education, healthcare, finance, and legal sectors. Traditional document verification methods often rely on manual inspection, physical seals, and centralized databases. While these methods have been used for decades, they come with significant limitations, such as inefficiency, susceptibility to human error, and vulnerability to forgery or unauthorized alterations. The growing number of fraudulent activities, including document counterfeiting and identity fraud, further highlights the urgent need for a more secure, transparent, and efficient solution for document verification. Blockchain technology presents a transformative approach to addressing these challenges by providing a decentralized and immutable ledger for document authentication. Unlike conventional systems where records are stored in centralized databases that can be manipulated or compromised, blockchain ensures data integrity through cryptographic hashing and distributed consensus mechanisms. Each document is converted into a unique hash value, which is then recorded on the blockchain. If the hashes match, the document remains unchanged and valid; however, if any discrepancies are detected, it indicates potential tampering or unauthorized modifications. This project, Digital Document Verification using Blockchain, aims to revolutionize document verification by offering a secure, efficient, and fraud-resistant solution. The proposed system is designed to be scalable and adaptable across various applications, catering to industries that require stringent document verification standards. .By integrating blockchain technology into digital document verification, this project lays the foundation for a more secure and trustworthy digital ecosystem. It not only enhances security but also streamlines the verification process, reducing operational costs and the burden on organizations that traditionally rely on labor-intensive authentication methods. With its ability to ensure document authenticity and prevent fraud, the system paves the way for a future where digital trust and data integrity are paramount.

II. MOTIVATION

Traditional document verification systems face several challenges, such as forgery, tampering, centralization risks, and inefficiency. Blockchain technology offers a decentralized, secure, and tamper-proof solution, making it an ideal choice for digital document verification. Here are the key motivations for using blockchain in this domain:

A. Immutability & Tamper-Proof Records

Traditional systems store documents in centralized databases, making them vulnerable to data manipulation, unauthorized access, or loss. With Blockchain: Documents are hashed and stored on a blockchain ledger, ensuring that once recorded, they cannot be altered or deleted. Any modification creates a new hash, making tampering easily detectable.

B. Decentralization & Trustless Verification

Centralized verification authorities (e.g., universities, government agencies) can be slow, expensive, or even corrupt.With Blockchain: Verification becomes decentralized, eliminating the need for a third party. Anyone can verify document authenticity without relying on a central authority.

C. Security & Fraud Prevention

Digital documents stored in centralized systems are vulnerable to hacking, duplication, and fraud.With Blockchain: Cryptographic hashing (e.g., SHA-256) ensures documents cannot be forged. Digital signatures (e.g., ECDSA) provide authenticity, proving that a document is issued by a legitimate source.

D. Transparency & Auditability:

Traditional verification methods lack transparency, leading to disputes and inefficiencies. With Blockchain: Every transaction on the blockchain is time-stamped and publicly verifiable, ensuring complete transparency. Audits can be conducted in real time without altering historical records.

E. Cost & Time Efficiency

Manual document verification is time-consuming and costly, especially when verifying across borders.Blockchain Verification is instant, automated, and does not require intermediaries, reducing costs and processing time.

F. Self-Sovereign Identity & Ownership

Users often lack control over their own credentials, relying on centralized entities to store and manage their documents. Blockchain Users can store their documents on a blockchain-based decentralized identity system, allowing them to share and control access as needed. By leveraging blockchain, digital document verification becomes more secure, efficient, and universally accessible, eliminating fraud while enhancing trust and transparency.

III. LITERATURE SURVEY

In this paper [1]addresses the issue of credential fraud, which undermines fraud is a widespread issue that undermines trust in higher education systems and leads to significant economic and social consequences. Traditional credential verification methods are often slow, expensive, and bureaucratic, making them ineffective against sophisticated fraud tactics. To address these challenges, we propose *Cerberus*, a blockchain-based credential verification system designed to enhance security, efficiency, and ease of use. Unlike existing solutions, Cerberus seamlessly integrates with current verification ecosystems, addressing real-world fraud scenarios while improving efficiency. It employs on-chain smart contracts for credential revocation, eliminating the need for students or employers to manage digital identities or cryptographic credentials. The system also prioritizes data privacy, offering features such as transcript verification and selective data disclosure. By streamlining the verification process and reducing fraud risks, Cerberus provides a robust, scalable solution for institutions and employers. This innovation aims to restore confidence in credential authenticity, ensuring a more reliable and trustworthy verification process.

In this paper [2] blockchain technology has made significant advancements, offering transformative potential for the education sector. It can revolutionize learning by providing cost-effective and innovative solutions, enhancing collaboration between teachers and students. One of the most promising applications of blockchain in education is the issuance of immutable digital certificates. Traditional certificate verification systems are often slow, unreliable, and dependent on centralized authorities, whereas blockchain-based verification ensures speed, security, and independence. This emerging field has garnered considerable scientific interest, yet research on the adoption of blockchain for academic credential verification remains in its early stages. This paper presents a comprehensive review of blockchain-based systems for academic certificate verification, compiling relevant research into a systematic literature review. By employing the PRISMA framework, we identified 34 key studies from 1,744 papers published between 2018 and 2022. Our analysis highlights six major themes explored in these studies and identifies critical research gaps that require further investigation. Additionally, we provide recommendations for future research and practical implementations that can benefit researchers, policymakers, and educational institutions. By addressing these gaps, blockchain can significantly improve the reliability and efficiency of credential verification, ultimately fostering a more secure and transparent educational ecosystem.

In this paper [3] Educational data is traditionally controlled by institutions, making it vulnerable to risks such as natural disasters, political instability, and war.

Additionally, accessing academic records for exchange programs or lifelong learning remains a challenge. While blockchain-based solutions for certification, verification, and data sharing exist, a fully decentralized system has yet to be developed. To address this, PublicEduChain is proposed as a decentralized framework that shifts data ownership to students instead of institutions. Built on the public Ethereum network, it enables students to store their academic records in smart contracts, allowing seamless data sharing with educational institutions and administrative bodies. Learning Management Systems (LMS) can interact with these smart contracts to read and update student records securely. PublicEduChain ensures complete decentralization, enhancing security, accessibility, and control over educational data. In this paper [4] Document verification plays a crucial role in various aspects of life, including births, marriages, legal matters, job applications, and academic achievements. Organizations, government agencies, and educational institutions face challenges in securely storing and verifying documents. To address this, we propose a blockchain-based document verification system, primarily designed for educational institutions to securely store certificates. In the proposed system, cryptographic techniques convert document content into a one-way hash function, which is then stored on the blockchain. This hash serves as a unique identifier for the document, ensuring its authenticity. When verification is required, an entity can reprocess the document's content into a hash and compare it with the blockchain-stored value. If they match, the document is authentic; if not, it has been altered. This system enhances security, prevents document fraud, and simplifies verification for employers and institutions. By leveraging blockchain, we ensure an immutable and transparent verification process, making document authentication more reliable and efficient.

IV. GAPS IN EXISTING RESEARCH

Despite significant advancements in blockchain-based digital document verification, several research gaps remain. Identifying these gaps can help in improving security, scalability, interoperability, and adoption. Here are some key areas where further research is needed:

A. Scalability & Performance Limitations

Issue: Many blockchain networks, especially public ones (e.g., Ethereum, Bitcoin), suffer from scalability issues due to high transaction times and costs.

Gap: Limited research on optimizing blockchain networks for high-volume document verification, especially in large-scale systems (e.g., national ID verification).

B. Privacy & Confidentiality Concerns

Issue: Public blockchains store transaction data transparently, which raises concerns about document privacy.

Gap: Lack of robust privacy-preserving mechanisms in document verification, such as Zero- Knowledge Proofs (ZKPs) or Homomorphic Encryption.

C. Standardization & Interoperability Issues

Issue: Different blockchain implementations follow different protocols, making it difficult to achieve cross-platform document verification. Gap: Limited research on interoperable blockchain frameworks that work across different networks .

This research seeks to integrate these methodologies to address existing gaps and develop a robust tampering detection system that is scalable, secure, and adaptable to various judicial frameworks.

V. PROPOSED METHODOLOGIES

The following methodologies outline a structured approach to enhancing security, efficiency, and scalability in blockchain-based document verification systems utilizing IPFS.

A. Hybrid Blockchain & IPFS Model

The system records document hashes on the blockchain (Ethereum/Polygon) while storing the actual documents in the IPFS network. IPFS is integrated using Infura API, ensuring decentralized storage and retrieval.

B. Smart Contract-Based Verification

Solidity smart contracts are deployed to handle document verification. These contracts store document hashes on-chain and validate integrity using Web3.js.Remix IDE is utilized for contract development and deployment.

.

C. Role-Based Access Control (RBAC)

Smart contracts define roles such as Owner, Exporter, and Verifier, ensuring controlled access. Only authorized users can upload and verify documents.

MetaMask authentication is employed to validate user permissions.

D. Secure Document Retrieval & Verification

Documents are retrieved from IPFS using their Content Identifier (CID).A new hash is computed upon retrieval and compared with the one stored on the blockchain.The system determines whether the document remains authentic or has been tampered with.

E. Integration with Decentralized Identity (DID)

The document verification system integrates with Decentralized Identifiers (DIDs).W3C Verifiable Credentials are used for identity authentication, linking verified documents to trusted identities.

F. Optimization with Layer 2 Scaling Solutions

To reduce blockchain transaction costs, the system employs Layer 2 solutions such as Polygon, Optimistic Rollups, or zk-Rollups. These technologies help offload verification processes from Ethereum's main chain.

The methodologies presented ensure a decentralized, secure, and efficient document verification system using blockchain and IPFS. By leveraging smart contracts, Layer 2 scaling, Zero-Knowledge Proofs, and decentralized identity management, the system addresses challenges related to scalability, security, and user accessibility. Future research can further explore cross-chain interoperability and regulatory compliance to improve adoption across industries.

VI. PROPOSED SYSTEM ARCHITECTURE

The system architecture for the blockchain-based document verification system encompasses several interconnected components designed to facilitate secure and efficient document verification processes. At its core, the system includes a user interface providing a user-friendly platform for individuals and organizations to interact with the system. Users can upload documents for verification, access verification results, and manage document-related tasks through this interface. The document verification module processes verification requests submitted by users, leveraging the blockchain network for validation. The blockchain network, composed of decentralized nodes, maintains a shared ledger of verified documents, ensuring transparency and immutability.

The Blockchain-Based Document Verification System is designed to provide secure, transparent, and efficient document authentication by integrating multiple interconnected components. The User Interface (UI) serves as the primary interaction point, enabling individuals and organizations to upload documents, access verification results, and manage document-related tasks. The Document Verification Module processes user-submitted requests by generating a cryptographic hash of the document, storing it on the blockchain, and later comparing it during verification to ensure integrity. The Blockchain Network, consisting of decentralized nodes, maintains a tamper-proof ledger of document hashes, ensuring transparency and security through consensus mechanisms and smart contracts. Furthermore, Layer 2 scaling solutions optimize performance and reduce costs, making the system more practical for real-world applications. Compared to traditional centralized methods, this approach eliminates intermediaries, reduces verification time, and enhances transparency. Future improvements, such as Zero-Knowledge Proofs (ZKPs) and cross-chain interoperability, can further enhance security, privacy, and scalability, making blockchain-based document verification a viable solution for various industries.

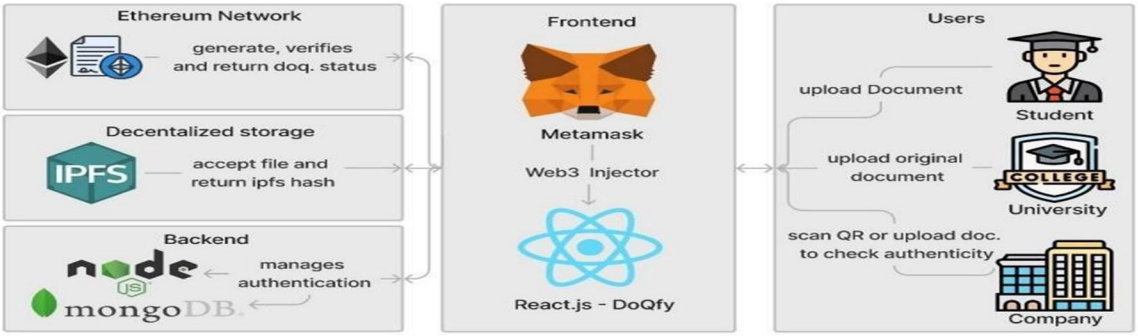


Figure 2: System Architecture

VII. ADVANTAGES

The Blockchain-Based Document Verification System ensures security, transparency, and efficiency by leveraging immutability, decentralization, and automation. It eliminates tampering, reduces fraud, and speeds up verification while lowering costs by removing intermediaries. The system is scalable, interoperable, and privacy-focused, allowing seamless integration with various industries. Smart contracts automate processes, minimizing errors and ensuring a verifiable audit trail. This makes it an ideal solution for secure, fast, and tamper-proof document authentication across sectors like education, finance, and healthcare.

VIII. APPLICATIONS

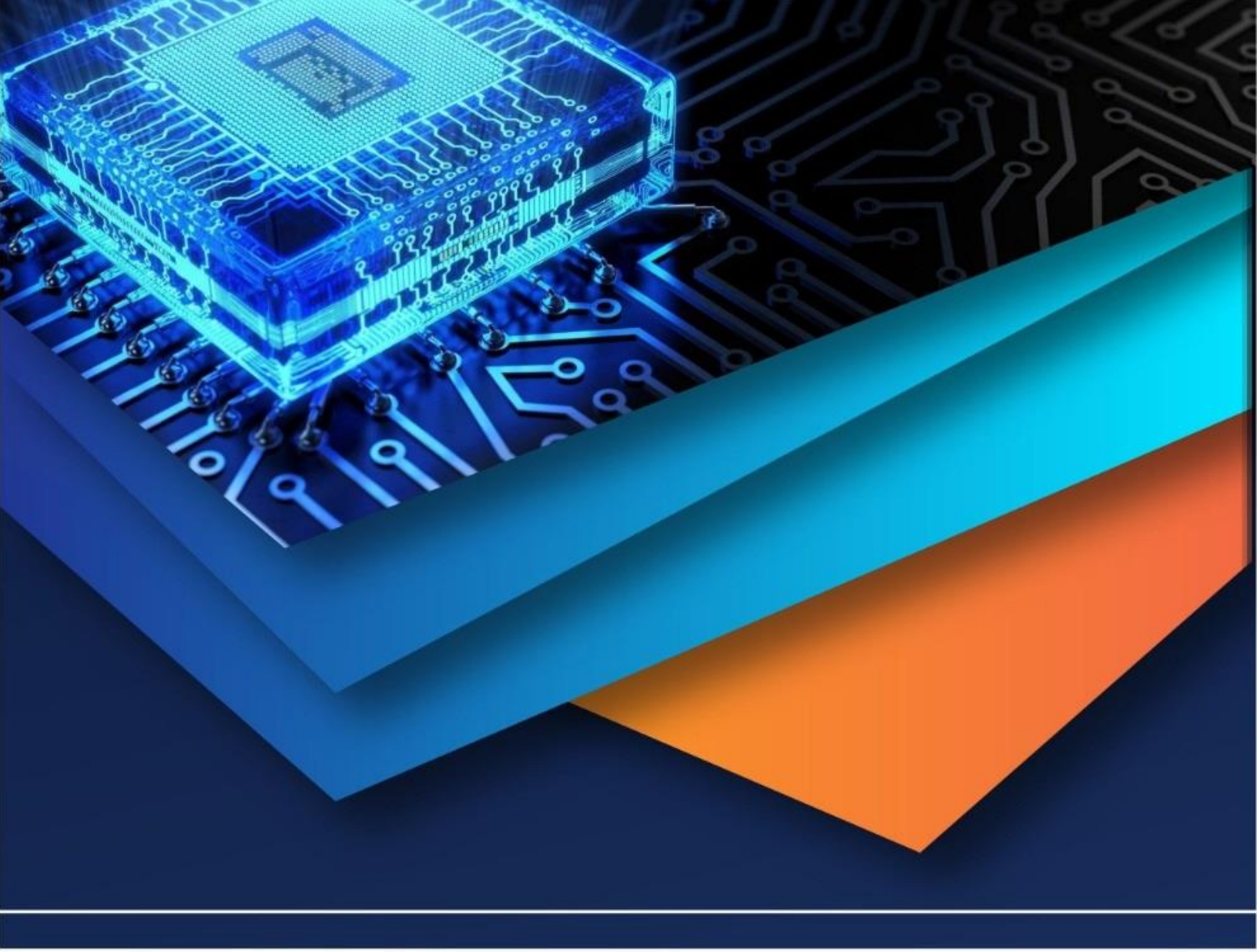
The Blockchain-Based Document Verification System has widespread applications across various industries that require secure and tamper-proof document authentication. In the education sector, it ensures the authenticity of academic certificates and transcripts, preventing forgery and aiding employers in verifying credentials. Financial institutions use it to secure loan agreements, KYC documents, and financial records, reducing fraud and ensuring compliance. In healthcare, it protects patient records, prescriptions, and insurance claims, maintaining data integrity and privacy. The legal sector benefits from secure verification of contracts, property deeds, and notarized documents, minimizing disputes. Government and public services rely on blockchain to secure identity documents such as passports and national IDs, reducing identity theft. The corporate sector uses it for employee credential verification and HR documentation, ensuring transparency in hiring. Supply chain management leverages blockchain to authenticate invoices, shipping records, and compliance certificates, preventing counterfeit goods. It also aids in intellectual property protection, securing patents, copyrights, and trademarks. Voting systems benefit from blockchain's security features to verify voter identities and prevent election fraud. Additionally, real estate transactions become more secure with tamper-proof property ownership records. By providing a reliable, immutable, and transparent verification system, blockchain enhances trust and security across multiple industries

IX. CONCLUSIONS

For digital document authentication in a variety of businesses, the Blockchain- Based Document Verification System offers a safe, open, and effective solution. It guarantees that papers are tamper-proof and verifiable in real time by utilising immutability, decentralisation, and cryptographic hashing. By cutting out middlemen, the approach lowers expenses, cuts down on verification time, and eradicates fraud. Because of its scalability and interoperability, it may be used to a variety of industries, including government services, healthcare, education, and the legal profession. This blockchain-based method transforms document verification by increasing automation, security, and trust, opening the door to a more dependable and secure digital future.

REFERENCES

[1] Dimitrov, D. Blockchain-Based Solutions for Digital Copyright Management: A Systematic Review. Journal of Information Science Theory and Practice, 8(1), 28-49.
[2] Y. G. Sucahyo, Y. Ruldeviyani, A. Gandhi et al., "An empirical study on factors that influence the digital startup sustainability: The mixed methods approach in indonesia," in 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS). IEEE, pp. 119–124.
[3] Storonsky, S., & Simpson, I. Blockchain: Opportunities for Private Enterprises in Copyright Management. International Journal of Innovation Management, 22(1), 1850005.
[4] G. Dusil and D. Cerny, "The next evolution in funding innovation," in Inter- national Joint Conference on Neural Networks (IJCNN). IEEE, pp. 1–4.
[5] R. Ji, Y. Tian, and M. Ma, "Collaborative filtering recommendation algorithm based on user characteristics," in 2020 5th International Conference on Control, Robotics and Cybernetics (CRC), 2020, pp. 56–60.
[6] S. C. Mana and T. Sasipraba, "A machine learning based implementation of prod- uct and service recommendation models," in 2021 7th International Conference on Electrical Energy Systems (ICEES), 2021, pp. 543–547.
[7] N. Raju and A. Patra, "A study on investor's attitude towards investment in eq- uity stocks with reference to east godavari, west godavari & vijayawada districts of andhra pradesh," International Journal of Control Theory and Applications (IJCTA) Volume, vol. 9.
[8] P. A. Verma and V. Singhal, "Data analysis of startups investments and funding trends in india".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY