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.2025.68683

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

Server Security in Cloud Computing Using Blockchain

Mrs. K. Rashmi[1], K. Akhil[2], Mohammad Reyaz[3], B. Dathu[4]
[1]*Cyber Security School of Engineering, Malla Reddy University Hyderabad, India*
[2, 3, 4]*School of Engineering, Malla Reddy University, Hyderabad, India*

Abstract: ***Cloud Computing is one of the most convenient, scalable, low-cost, accessible, and highly available technologies for delivering a variety of services in the era of digitalization. However, security concerns such as data breaches, privacy issues, and integrity risks remain significant challenges in cloud environments. This paper explores the integration of blockchain technology into Cloud Computing as a potential solution to these security concerns. Blockchain is a decentralized and cryptographically secure system of linked records, known as blocks, which provides an immutable ledger that enhances data integrity and transparency. The paper will discuss the disruptive potential of blockchain in addressing the vulnerabilities of cloud services and how blockchain-based electronic wallets can ensure protection of user data in cloud environments. In addition, the paper will provide a detailed overview of applications and recent technological advancements in combining blockchain with cloud computing. This approach promises to revolutionize cloud security by leveraging blockchain, providing enhanced protection and trust for cloud users.***

Keywords: Cloud Computing; Blockchain Technology; Data Security; Data Integrity; Decentralization; Cryptography

I. INTRODUCTION

It is due to such fast-paced digitalization in different sectors that Cloud Computing has emerged as a very vital technology. Scalable resources, ease of access, and changes in the management, storage, and processing of data in business and individuals' ways have transformed all of these. Since cloud computing works on- demand without the physical need for infrastructure, the benefits have been significant in cost savings, operational flexibility, and reach into global markets. Despite these advantages, several security issues have emerged as pressing concerns for users and service providers. Key issues range from compromising data privacy to security breaches with regards to sensitive information integrity. Taking into consideration such issues, block chain has emerged as a developing solution in response to these issues. It presents a decentralized, cryptographically secure form of data storage, with the records, or "blocks," being linked and therefore immutable, ensuring integrity and transparency. Integrating blockchain with cloud computing can significantly enhance security in cloud services. Its distributed ledger system gives greater transparency while reducing the risks associated with centralized control and even in cases where data may be tampered with during a breach.

This paper explores the potential of blockchain technology in improving security in cloud computing. It examines how blockchain can enable decentralization to safeguard user data in environments requiring high degrees of trust and integrity in data. It also considers how blockchain-based electronic wallets further improve transactions and the details of a user in the cloud environment. Based on the analysis of recent developments, this paper introduces a conceptual framework of how blockchain can revolutionize security perspectives in cloud computing, and it further provides an elaborate discussion of applications and challenges involved with the use of these technologies.

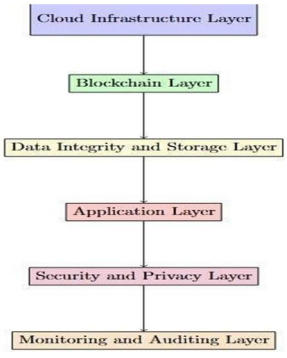


Fig 1: System Architecture

II. LITERATURE SURVEY

1) Blockchain-based Cloud Manufacturing: The Decentralization

Authors: A. Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang, G. Q. Huang (2019) The authors in the paper suggest the use of blockchain for the decentralization of cloud manufacturing systems. Traditional centralized servers in cloud manufacturing pose risks such as data manipulation and loss of data integrity as well as lack of transparency. In summary, by decentralizing such processes via blockchain, a safer, transparent, and trustworthy system is promised by facilitating numerous stakeholders' interactions on one immutable shared ledger. Such a contribution extends the body of knowledge for blockchain use in cloud manufacturing as trust, integrity, and transparency form some of its most basic critical values.

2) Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities

Authors: A. Harshavardhan, T. Vijayakumar, S. R. Mugunthan (2018)

This paper deals with the integration of blockchain in cloud computing to overcome vulnerabilities inherent in cloud infrastructures. Some of the issues, like data breaches, unauthorized access, and loss of data, that are still common in the cloud systems of olden times have not been eliminated. They intend to integrate blockchain into a decentralized, non-modifiable data structure so that transactions and data storage can improve privacy and security. The work stresses that blockchain can defend against internal and external threats and enhance overall trustworthiness in cloud services.

3) Blockchain and Supply Chain Management

Authors: A. Jabbari, P. Kaminsky (2018)

Jabbari and Kaminsky (2018) discuss the application of blockchain technology in supply chain management, which is an integral part of many cloud-based systems, especially in logistics and data management. Blockchain provides transparency and tamper-proof records that guarantee the authenticity of the transactions and the integrity of the supply chain. Their study is not directly on cloud computing, but it is very relevant because it shows how blockchain can be integrated into a system with a cloud in order to increase transparency, avoid fraud, and improve traceability across cloud-dependent industries.

4) Blockchain Technology in Cloud Computing: A Systematic Review

Authors: M. K. R. Ingole, M. S. Yamde (2018)

Ingole and Yamde provide a comprehensive review of the literature on blockchain applications in cloud computing. The paper systematically reviews various works that have integrated blockchain with cloud infrastructures and explores its application in securing the cloud storage of data, data privacy improvement, and automatic process by smart contracts. This work is a contribution to the field, as it will organize the knowledge on how blockchain is applicable to cloud computing, hence providing a clearer understanding of challenges and benefits through the use of blockchain to resolve common issues in cloud security.

III. METHODOLOGY

A. Core Components

The Secure File Sharing and Communication System (SSCCB) is built with four main components that work together seamlessly. The Admin Panel (adminapp) provides administrative control and monitoring capabilities, while the User Interface (userapp) offers a user-friendly platform for file operations. The File Management System handles all file- related operations, and the Security Layer ensures data protection throughout the system.

B. Basic Workflow

The system follows a straightforward workflow that begins with user registration. Once registered, users await admin approval before gaining full system access. After approval, users can upload files which are then processed through the security layer. The files can be securely shared with other users through the platform, and authorized users can access these files through a controlled interface. This workflow ensures proper authentication and authorization at each step.

C. Key Features

The system incorporates several essential features to provide a comprehensive file sharing solution. User authentication and authorization ensure that only legitimate users can access the system. The secure file upload and download functionality protects data during transfer.

Files are encrypted using RSA encryption for additional security. The URL shortening feature makes file sharing more convenient while maintaining security. The system also includes email notifications for important events and status tracking to monitor file operations.

D. Security Measures

Security is a top priority in this system, implemented through multiple layers of protection. RSA encryption ensures that files remain secure even if intercepted. Session management prevents unauthorized access, while access control mechanisms restrict file access to authorized users only. The secure file transfer protocol ensures data integrity during transmission.

E. User Roles

The system operates with two distinct user roles to maintain proper control and functionality. Administrators have the authority to manage users, monitor system activities, and maintain overall system security. Regular users can upload files, share them securely, and access files shared with them, all while operating within the system's security constraints.This methodology ensures a secure, efficient, and user-friendly file sharing system that prioritizes data protection while providing necessary functionality for both administrators and users.

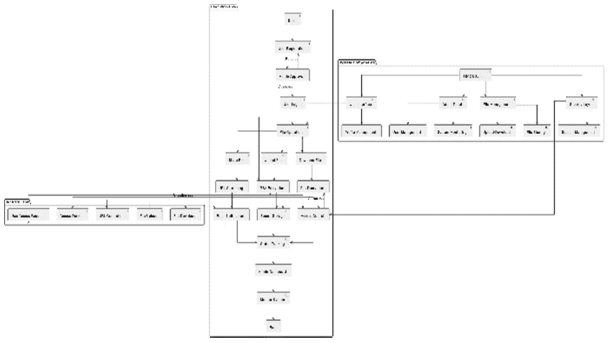


Fig : Methodology

IV. SYSTEM ANALYSIS

A. Existing System

The existing system for the project titled "Server Security in Cloud Computing Using Blockchain" addresses the prevalent challenges associated with data sharing and storage in the digital landscape. In the current scenario, where the majority of data sharing occurs digitally over the internet, Cloud Service Providers play a crucial role in facilitating this process. However, this convenience is accompanied by significant risks, including intentional and unintentional manipulation of vast amounts of data, leading to common threats such as Data Piracy and Hack Attacks. Recognizing the urgency to bolster the security of cloud systems and protect sensitive user data from potential misuse, the existing system proposes the integration of Blockchain technology. By anchoring Blockchain for securing data over the cloud, the system introduces a Controlled Access Mechanism.

Limitations Scalability Challenges: Blockchain systems, especially those based on public decentralized networks, may face scalability challenges as the number of users and transactions increases. This can potentially impact the performance of the system, leading to delays and higher resource requirements.

B. Proposed System

The proposed system titled "Server Security in Cloud Computing Using Blockchain" aims to revolutionize the security paradigm of cloud- based data storage and sharing. Building upon the recognition of vulnerabilities in the existing system, the proposed framework introduces a robust security architecture by leveraging Blockchain technology. The core innovation lies in the implementation of a Controlled Access Mechanism, facilitated by Blockchain, which grants users personalized hyperlinks for data access while ensuring the integrity and confidentiality of the stored information. Smart contracts play a pivotal role in automating and enforcing access control rules within the Blockchain network. The system not only addresses the pressing concerns of intentional and unintentional data manipulation but also enhances transparency and accountability by maintaining a detailed and immutable log of all user actions.

Through the integration of Blockchain, the proposed system offers heightened security features, such as tamper resistance and decentralized consensus, thereby establishing a more trustworthy and resilient cloud space for sensitive user data. The envisaged benefits encompass enhanced security, user privacy, and a streamlined approach to data management in the cloud.

Advantages

- Enhanced Data Security: By leveraging blockchain technology, the system provides a decentralized and tamper-proof ledger that ensures the integrity and authenticity of the stored and shared data. Blockchain's inherent security properties protect against unauthorized access and manipulation of data, offering stronger protection than traditional methods.
- Controlled Access: The use of personalized hyperlinks for data sharing ensures that only authorized users have access to specific data. This controlled access mechanism allows the data owner to selectively grant access to individuals, thus maintaining tight control over who can view or interact with the data.
- Immutable Audit Trails: Blockchain records every action or transaction made on the data, creating an immutable audit trail. This feature ensures full traceability of data usage and operations, which can be valuable for auditing, detecting suspicious activity, and maintaining accountability.
- Protection Against Data Breaches: The decentralized nature of blockchain makes it more resistant to centralized attacks, such as hacking or data piracy, which are common threats to cloud- based storage. With blockchain, the data is distributed across multiple nodes, making it significantly harder for malicious actors to manipulate or compromise the system.

V. FUTURE WORK

1) Implementation of Two-Factor Authentication (2FA) and biometric security features for enhanced user verification.
2) Development of mobile applications for iOS and Android platforms to enable secure file access on-the-go.
3) Integration of Artificial Intelligence for smart file categorization and automated security threat detection.
4) Cloud integration with multiple providers for improved scalability and storage optimization.
5) Real-time collaboration tools with instant messaging and file sharing capabilities.
6) Advanced analytics dashboard for better system monitoring and user activity tracking.
7) API development for seamless third-party application integration and extensibility.
8) Automated backup and disaster recovery system implementation.
9) Push notification system for real- time alerts and file sharing updates.
10) Performance optimization through load balancing and caching mechanisms.

VI. RESULTS

Fig1: User Login

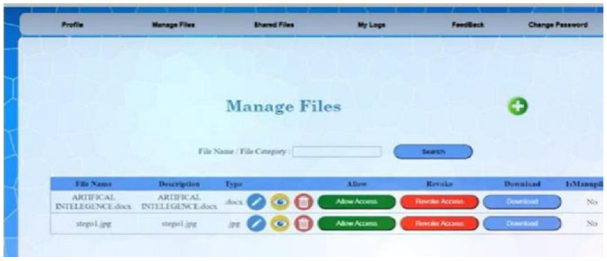


Fig2: Manage Files

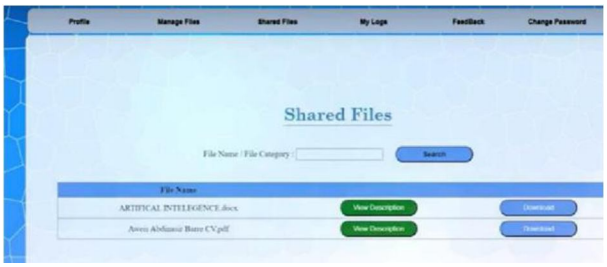


Fig3: Shared Files

Fig4: Admin Login

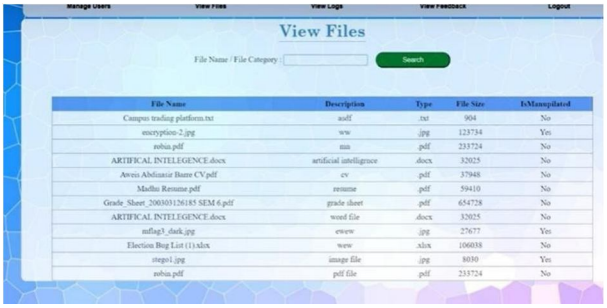


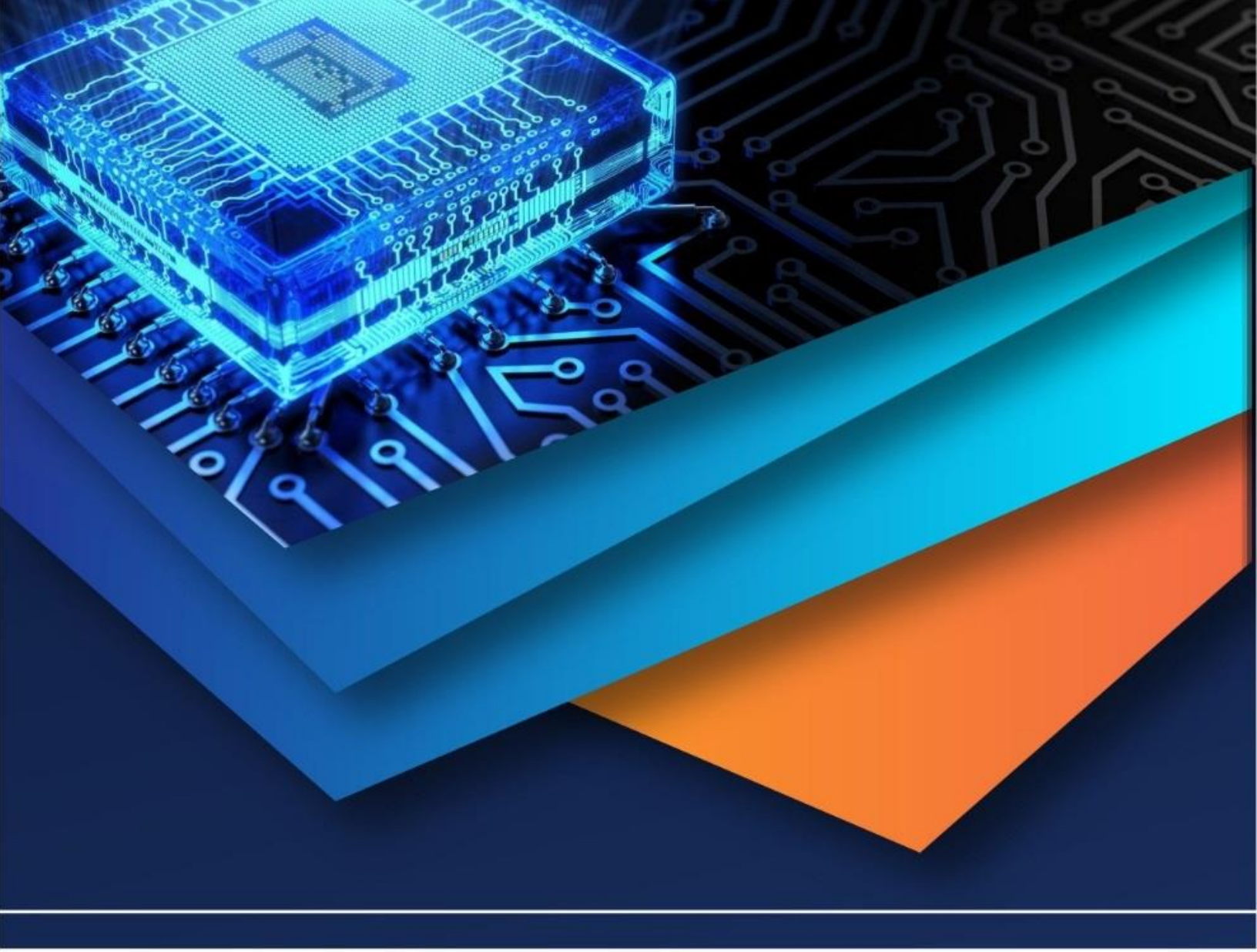
Fig5: View Files

Fig6: Log History

REFERENCES

[1] Vatankhah Barenji, H. Guo, Z. Tian, Z. Li, W. M. Wang and G. Q. Huang, "Blockchain- based cloud manufacturing: Decentralization", arXiv:1901.10403, 2019, [online]Available:http://arxiv.org/abs/1901.10 403.
[2] Harshavardhan, T. Vijayakumar and S. R. Mugunthan, "Blockchain technology in cloud computing to overcome security vulnerabilities", Proc. 2nd Int. Conf. I-SMAC (IoT Social Mobile Anal. Cloud)(I-SMAC) I SMAC (IoT Social Mobile Anal. Cloud)(I SMAC) 2nd Int. Conf., pp. 408-414, Aug. 2018.
[3] .A. Jabbari and P. Kaminsky, "Blockchain and supply chain management", 2018.
[4] M. K. R. Ingole and M. S. Yamde, "Blockchain technology in cloud computing: A systematic review", 2018.
[5] Qiu, H. Yao, C. Jiang, S. Guo and F. Xu, "Cloud computing assisted blockchain enabled Internet of Things", IEEE Trans. Cloud Comput., Jul. 2019.
[6] Dujak and D. Sajter, "Blockchain applications in the supplychain" in SMART Supply Network, Cham, Switzerland:Springer, pp. 21-46, 2019.
[7] A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire and P. R. Inácio, "Security issues in cloud environments: A survey", Int. J. Inf. Secur., vol. 13, no. 2, pp. 113-170, 2014. ISSN 2581 – 4575 Page 480 Volume 08, Issue 10, Dec 2024

[8] B. Rawat, V. Chaudhary and R. Doku, "Blockchain: Emerging applications and use cases", arXiv:1904.12247, 2019, [online] Available: https://arxiv.org/abs/1904.12247.
[9] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities", Proc. IEEE 8th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON), pp. 469-474, Oct. 2017.
[10] D. Tosh, S. Shetty, X. Liang, C. Kamhoua and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach", IEEE Consum. Electron. Mag., vol. 8, no. 4, pp. 38-44, Jul. 2019
[11] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain technology overview", arXiv:1906.11078, 2019, [online] Available: http://arxiv.org/abs/1906.11078.
[12] Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments", 2017.
[13] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities", Renew. Sustain. Energy Rev., vol. 100, pp. 143-174, Feb. 2019.
[14] D. Efanov and P. Roschin, "The all pervasiveness of the blockchain technology", Procedia Comput. Sci., vol. 123, pp. 116-121, 2018.
[15] Knirsch, A. Unterweger and D. Engel, "Implementing a blockchain from scratch: Why how and what we learned", EURASIP J. Inf. Secur., vol. 2019, no. 1, pp. 2, Dec. 2019
[16] S. Sharma, G. Gupta and P. R. Laxmi, "A survey on cloud security issues and techniques", arXiv:1403.5627, 2014, [online] Available: http://arxiv.org/abs/1403.5627.
[17] J. Katuwal, S. Pandey, M. Hennessey and B. Lamichhane, "Applications of blockchain in healthcare: Current landscape challenges", arXiv:1812.02776, 2018, [online] Available: http://arxiv.org/abs/1812.02776.
[18] Kaur, M. A. Alam, R. Jameel, A. K. Mourya and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment", J. Med. Syst., vol. 42, no. 8, pp. 156, Aug. 2018.
[19] L. Zhang, decentralized cloud "A blockchain-based resource scheduling architecture", Proc. Int. Conf. Netw. Netw. Appl. (NaNA), pp. 324-329, Oct. 2018.
[20] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey", Int. J. Web Grid Services, vol. 14, no. 4, pp. 352-375, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY