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.2025.68754

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

Blockchain-Driven E-Voting System

Prof. Mahadevi Namose[1], Teemira Bhale[2], Shivaranjani Darshale[3], Devashree Mali[4]
[1]*Faculty of Computer Science, International Institute of Information Technology, Pune, India*
[2, 3, 4]*Computer Engineering, International Institute of Information Technology, Pune, India*

Abstract: ***The use of electronic voting (e-voting) is becoming more common instead of traditional voting systems, but it still faces a big issue: trust. E-voting systems can be easily manipulated, with potential changes to election results from hacking or tampering by those who create the systems. In centralized networks, data is managed by one party, which raises trust concerns. However, this problem can be solved by using a distributed system where data is shared among all users. Blockchain technology serves this purpose well, as it keeps a shared record that cannot be changed, making it ideal for e-voting. This research introduces a Blockchain-based e-voting system using Ethereum and MetaMask, which meets six key principles of a fair election: secret ballots, one vote per person, voter eligibility, transparency, accurate recording and counting of votes, and reliability. Additionally, testing shows that using a slower gas price option results in the best value for costs. This introduces a Blockchain-based e-voting system utilizing Ethereum and MetaMask, ensuring adherence to essential electoral principles such as secret ballots, voter eligibility, and accurate vote recording. Performance evaluations indicate that using a slow gas price option offers the best cost-efficiency for this system. Overall, the proposed model not only addresses the vulnerabilities of traditional e-voting systems but also has potential applications beyond elections, including corporate governance and various voting scenarios.***
Keywords: Electronic voting, blockchain, smart contract, Ethereum

I. INTRODUCTION

The electoral process is the vital pillar of democratic societies, it gives power to people to make decisions and change governments through their votes. Voting is not only the formal way of the above act; it also represents the collective voice of the people and is a must for the proper functioning of the political system. Everyone, be it, from the international to local level, has used a variety of voting methods, including electronic ballots through time and across various cultures. Each of them has its benefits and disadvantages. In the past, standard forms of voting like those that propose them, rising votes, show of hands, or paper-based voting have been an essential change of the electorate in the voting process for hundreds of years. Conversely, the population increases and technological development as a fast pace, and the raising of the request to products of that kind has become an important factor.

In the last few years, electronic voting (e-voting) has become popular as a modern alternative to traditional voting methods. E-voting refers to the different technologies and procedures that enable voters to cast their votes electronically, either through designated voting machines or online platforms. The number one advantage of e-voting is the increase in voter participation, the decrease in operation costs related to the management of the electoral process and the accuracy of the vote tallying. To illustrate, e-voting could be the means that enables people to vote from remote places and also it could be the process where people could vote through personal digital gadgets like smartphones and laptops. Thanks to this, there would be a chance for better election results. This could be reached by providing convenience for every voter, especially for those people who cannot provide transportation because of a disability or live abroad. As society progresses into the digital era, there is an increased call for the voting infrastructure to be more robust and secure in order to fill the gap in available systems. Recent research and practice have focused on exploring innovative solutions to this problem. Blockchain technology is one such prominent solution that has received gigantic attention over the last few years for its potential to revolutionize many sectors of operations, including finance, healthcare, and supply chain management. At its core, it is decentralized and distributed ledger technology, which allows securing as well as recording transactions across many nodes in the network. Unlike other databases being controlled by a single organization, blockchain has no central authority, which minimizes the possibilities of tampering with data and makes it more resilient for the system. Some modern alternative has been identified in electronic voting systems. Voters can use electronic voting machines at the polling station or be able to vote online from their devices. This method is speedier and convenient since it will automatically count the results, saving time and resources in tallying. However, electronic voting is not without its challenges. There are also grave concerns about the security of the votes, where it is possible to manipulate or leak. Most electronic systems work like "black boxes," hence results cannot be checked or audited. Centralized systems are also not immune to denial-of-service attacks, that would disrupt the voting process and affect the public's trust.

The paper deals with the integration of blockchain technology into voting systems to achieve security, transparency, and accessibility in the electoral process. It is a review of different platforms on the block chain and their respective potential applications in voting situations. But by reviewing these existing implementations, challenges, and future directions for blockchain-based voting, we hope to help shed light on how this technology might be used to help address the ills of traditional and electronic voting systems. We will seize this opportunity to further contribute to the already seminal debate around improving electoral integrity and building greater public confidence in democratic processes.

II. PROPOSED SYSTEM

1) Registration: Before any person votes, each eligible voter receives a unique public address and with a private key. These two concepts are central to ensuring the voting system is secure and private. The public address is like an account number, while the private key is like the password. Each voter's account also loaded with a sufficient amount of ether, a form of cryptocurrency, to make one transaction. This configuration enables the voters to vote without anyone knowing their preference. The public address and the private key of the voters should remain private, thus ensuring that they get to vote anonymously.

2) Authentication: The process now moves on to voting, and authentication is at the very initial stage. In this, every voter needs to input the public address along with their private key in the system to authenticate himself or herself. This happens because only a registered voter has the right to vote. Whatever credentials entered by the user must be validated against the one that is registered with the system for any entry to vote. Authentication keeps frauds at bay and prevents only illegitimate people from voting in an election.

3) Voting: After getting authenticated, one goes through the voting phase and can then vote. They are presented with a list of accessible candidates on a friendly application. A voter may scrutinize the options and pick his preferred candidate. In essence, when the voter makes a request to a smart contract, which is truly a self-executing contract with the terms written directly into codes, they submit their vote officially. At the same time, the voter also includes the ID of the chosen candidate so that his or her vote can be recorded accurately for them through this request.

4) Results: After the voting has taken place, the results are processed. A vote is deemed successful when a miner—an individual who helps verify transactions—confirms the transaction ID associated with that vote. Furthermore, this confirmation must be acknowledged by all other miners in the network. This collective acknowledgment ensures that the voting process is secure and that the results are trustworthy. Only when all miners agree is the transaction finalized and added to the blockchain, making the voting results official.

This process also makes the election more secure and transparent and assures that every vote counts as well as anonymity is achieved in casting votes.

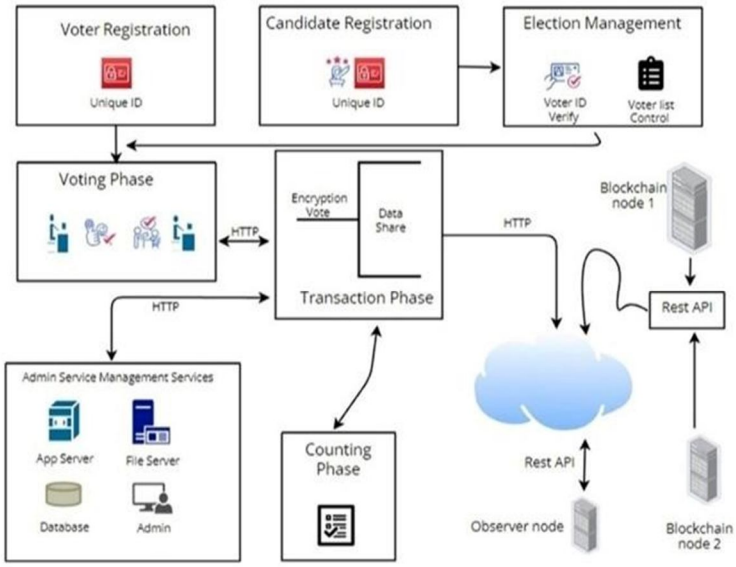


Fig 1. System Architecture

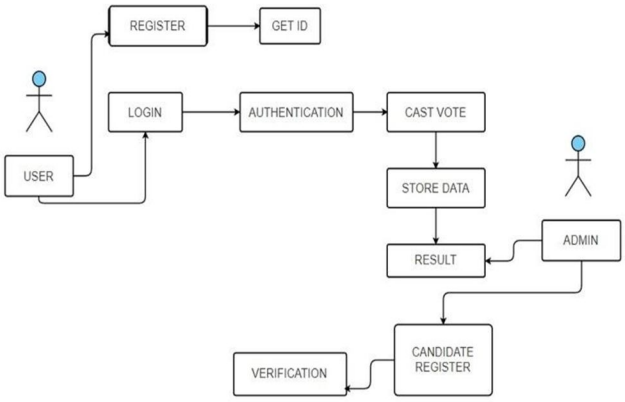


Fig 2. Detailed UML Diagram

III. METHODOLOGY

A. Requirement Gathering

Identify the core features: voter registration, candidate registration, vote casting, and result calculation. Analyze the need for security, transparency and decentralization in the voting system .

B. Design Phase

Design the system using a client-server model where the server is the Ethereum blockchain. Use Solidity to develop smart contracts that handle voting logic, candidate/voter registration, and result calculation. Design the frontend using React.js for user interaction.
Smart Contract Design: Define the structure of voters, candidates, and election status using Solidity. Implement key functionalities: adding voters and candidates, starting/ending the election, casting votes, and showing results.

C. Development Phase

Smart Contract Development: Develop the voting smart contract on the Ethereum blockchain using Solidity. Use Remix IDE to write, compile, and deploy the smart contract.
Frontend Development: Use React.js to create a user-friendly interface where users can register, vote, and view results. Establish a connection between the frontend and the smart contract using Web3.js to interact with the blockchain.
Blockchain Setup: Deploy the smart contract on Ethereum's test network or Ganache (local blockchain) for development and testing.

D. Testing Phase

Unit Testing of Smart Contracts: Test the smart contracts for bugs, ensuring that they perform correctly (voter registration, vote counting, etc.).
Functional Testing: Ensure the frontend interacts seamlessly with the deployed smart contract. Simulate various election scenarios and verify the integrity and security of the process.

E. Deployment

Deploy the frontend on a web hosting service. Deploy the smart contract on an Ethereum test net (e.g., Rinkeby, Ropsten) for further testing and presentation purposes.

F. Documentation and Presentation

Document the development process, testing results, and user manual. Prepare a demonstration of the system showcasing the key functionalities and blockchain integration. This methodology ensures a structured and organized approach to building a decentralized voting system on the Ethereum blockchain**.**

IV. IMPLEMENTATION

A voting system using the technology of Ethereum blockchain. An Ethereum blockchain network is used to implement this voting system. Ethereum is a decentralized and open-source network that supports smart contracts. In this platform, the cryptocurrency used is called Ether (ETH). It uses a method called Proof of Work, where those who can quickly solve complex problems with their computer power can add new blocks to the network. Setting up the blockchain provides a safeguard from vote tampering. Each block in the blockchain is linked to the previous and next blocks. This means any attempt of hackers to a particular block will be caught by the next block. Attempting on changes will also result in the corrupting of the following blocks, thus it would be extremely difficult to alter records without being detected. The hash value produced by the block is responsible for ensuring the data's integrity. Additionally, MetaMask is a well-known digital wallet that people use to manage crypto holdings and interact with blockchain apps, especially with the Ethereum network. Through MetaMask, it is possible for the users to connect to decentralized applications (DApps) directly from their web browsers simply, to send and receive funds, sign transactions, and to participate in blockchain activities without needing to run a full Ethereum node. Solidity is a programming language dedicated to developing smart contracts within the Ethereum blockchain. Solidity is typically used because it offers the necessary instruments to make fully decentralized applications (DApps) and transaction management in a secure way on the blockchain. Moreover, Remix IDE is an online development environment used for writing, testing, and deploying smart contracts written in Solidity. It gives a nice interface with features such as syntax highlighting, debugging tools, and a built-in Ethereum Virtual Machine (EVM) for testing contracts. Team Remix can prototype and perform quick tests on their smart contracts with Remix.

V. CONCLUSION

Electronic voting (e-voting) has been in existence since the 1970s, which on paper offers some advantages over the paper-based systems in terms of higher efficiency and fewer errors. Also, along with cybersecurity, there is more and more support for a fair market-free voting system from blockchain enthusiasts. The fast headway of blockchain technology is behind numerous attempts to investigate its suitability in the context of enlarged e-voting systems. This however does not rule out the fact that some crypto-currencies have difficulties as every true technology born is not perfect. This paper details one such project that leverages the powers of a blockchain that are cryptographically secure and transparent to make e-voting systems better. The proposed system is built using Multichain, and it was observed that it fully met the requirements for a reliable e-voting system.

This work is a continuation of the one pinpointing the focus on the strengthening of blockchain's "double spending" problem resistance that arises, for example, in e-voting by fear of the "double voting" case which is misuse of a particular token. Mostly, users rely on this technology for the regular interpretations of transactions. If there are any deviations, they follow them. It therefore means that the secure technology works; however, when weaknesses are demonstrated, a rethink is necessary. This is the driving force to the need for studying this problem in greater depth. We hold the view that soon we are going to witness the development of a trust assured vote-tracking model (provenance) that will help us implement secure and fully verifiable e-voting systems. Adding a provenance layer to the current blockchain infrastructure is one of our ongoing projects which are intended to help in this

VI. ACKNOWLEDGMENT

This research is supported by International Institute of
Information Technology College under the ' Savitribai Phule University '

REFERENCES

[1] U. Can Cabuk, E. Adiguzel, and E. Karaarslan, ‘‘A survey on feasibility and suitability of blockchain techniques for the E-voting systems,’’ 2020, arXiv:2002.07175.
[2] J. Ben-Nun, N. Fahri, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma, and D. Wikström, ‘‘A new implementation of a dual (paper and cryptographic) voting system,’’ in Proc. 5th Int. Conf. Electron. Voting (EVOTE), 2012, pp. 315–329.
[3] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, ‘‘E-voting systems using blockchain: An exploratory literature survey,’’ in Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), Jul. 2020, pp. 890–895.
[4] S. A. Adeshina and A. Ojo, ‘‘Maintaining voting integrity using blockchain,’’ in Proc. 15th Int. Conf. Electron., Comput. Comput. (ICECCO), Dec. 2019, pp. 1–5.
[5] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, ‘‘A reviewof E-voting: The past, present and future,’’ Ann. Telecommun., vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.
[6] R. Taş and Ö. Ö. Tanriöver, ‘‘A systematic review of challenges and opportunities of blockchain for E-voting,’’ Symmetry, vol. 12, no. 8, p. 1328, Aug. 2020.
[7] P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, ‘‘Prêt à Voter: A voter-verifiable voting system,’’ IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 662–673, Dec. 2009.

[8] S. Bell, J. Benaloh, M. D. Byrne, and D. DeBeauvoir, ‘‘STAR-Vote: A secure, transparent, auditable, and reliable voting system,’’ in Proc. Electron. Voting Technol. Workshop/Workshop Trustworthy Elections (EVT/WOTE), 2013, pp. 1–20.

[9] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, ‘‘E-voting system based on blockchain technology: A survey,’’ in Proc. Int. Conf. Inf. Technol. (ICIT), Jul. 2021, pp. 200–205

[10] Antoine Audras1, Louis Coudert1 “Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review” LIP6, CNRS, Sorbonne Université, 75005 Paris, France

[11] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, “An anti-quantum e-voting protocol in blockchain with audit function,” IEEE Access, vol. 7, pp. 115304–115316, 2019. https://doi. org/10.1109/ACCESS.2019.2935895

[12] B. Shahzad and J. Crowcroft, “Trustworthy electronic voting using adjusted blockchain technology,” IEEE Access, vol. 7,pp.24477–24488, 2019. https://doi.org/10.1109/ ACCESS.2019.2895670

[13] K. M. Khan, J. Arshad, and M. M. Khan, “Investigating performance constraints for blockchain based secure e-voting system,” Future Generation Computer Systems, vol. 105, pp. 13–26, 2020. https://doi.org/10.1016/j.future.2019.11.005

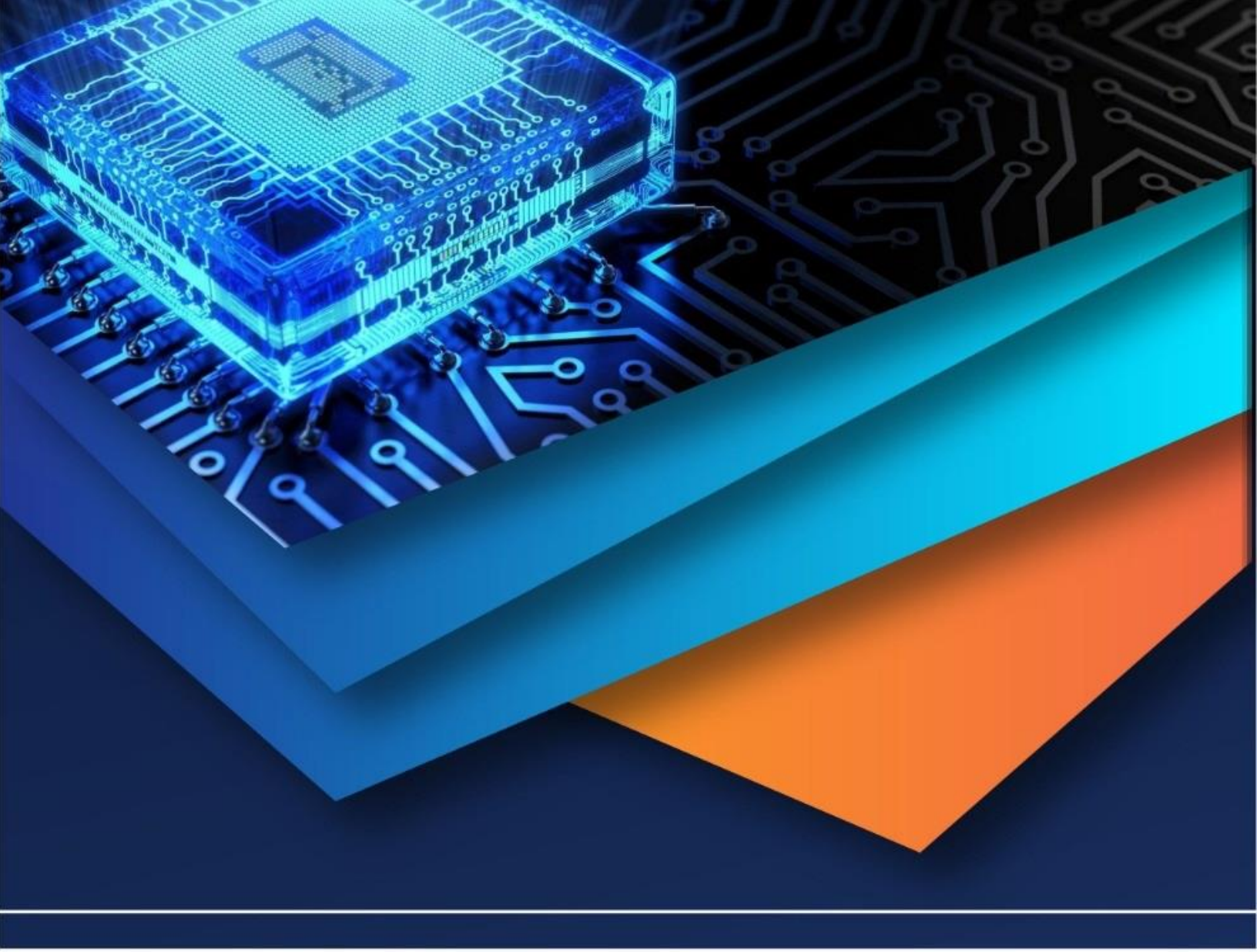
[14] C. K. Adiputra, R. Hjort, and H. Sato, “A proposal of blockchain-based electronic voting system,” in 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2018, pp. 22–27. https://doi.org/10.1109/ WorldS4.2018.8611593

[15] T. Dimitriou, “Efficient, coercion-free and universally verifiable blockchain-based voting,” Computer Networks, vol. 174, p. 107234, 2020. https://doi.org/10.1016/j.comnet. 2020.107234

[16] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, “A simple voting protocol on quantum blockchain,” International Journal of Theoretical Physics, vol. 58, no. 1, pp. 275–281, 2019. https://doi.org/10.1007/s10773-018-3929-6

[17] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, “Secure online voting system using biometric and blockchain,” in Data Management, Analytics and Innovation, N. Sharma, A. Chakrabarti, and V. E. Balas, Eds., in Advances in Intelligent Systems and Computing, vol. 1042. Singapore: Springer Singapore, 2020, pp. 93–110. https:// doi.org/10.1007/978-981-32-9949-8_7

[18] C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, and L. Mauri, “Towards blockchain-based E-voting systems,” in International Conference on Business Information Systems, Springer, 2019, pp. 274–286. https://doi.org/10.1007/978-3-030-36691-9_24



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY