iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4010

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: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Certificate Verification System using Blockchain

Nitin Kumavat[1], Swapnil Mengade[2], Dishant Desai[3], Jesal Varolia[4]
[1,2,3,4]*Computer Engineering Department, Mumbai University*

Abstract*—During the course of education the students achieve many certificates. Student produce these certificates while applying for jobs at public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce the fake certificate and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. Because it is possible to create such certificates at low cost and the process to verify them is very complex, as they are manually needed to be verified. This problem can be solved by storing the digital certificates on the Blockchain. The Blockchain technology provides immutability and publicly verifiable transactions, these properties of Blockchain can be used to generate the digital certificate which are anti-counterfeit and easy to verify.

Keywords*—Blockchain, Decentralization, Smart Contract, Ethereum, Ledger, Interplanetary File System.

I. INTRODUCTION

A. Background

Certificates distributed in colleges or universities are mostly in the form of hard copy. Whenever applicants apply for the job at any public or private sector they have to produce those hard copies, while the organizations have to verify all certificates manually which is very time-consuming process and there are chances that some may have produce the certificate which is not legit and that may get unnoticed by the verifier during the process because of this ineligible candidate will get a chance. There had been lots of cases in past where people are caught selling fake certificates of different organization at low cost. To eradicate such problem and diminish the production of fake certificates we can use the Blockchain technology. Blockchain can be used to store the data of the certificate that can be validated by anyone from any place. The blockchain is a decentralized shared distributed ledger; the data stored in the blockchain is almost un-modifiable. It is a type of database which is not centralized and governed by the set of rules.

B. Objectives

In this study, we are going to develop the decentralized certificate verification application on the Ethereum Blockchain. We are selecting this technology because it is traceable, tamper proof and encrypted. By integrating the blockchain technology we will be able to eradicate the problem of fake certificates.

We will use smart contract at backend to interact with the blockchain and the encrypted hash value of each document will be stored in blockchain which will be verified against the user document.

II. LITERATURE REVIEW

Blockchain is the system that does not rely on trust for electronic transaction. It shows how the problem of double spending can be solve using the peer-to-peer network using proof-of-work algorithm to record the history of each transactions which later become computationally impractical for intruder to change if legit nodes of computer control the majority of CPU power. The nodes can join or leave network whenever required. They vote with their CPU power, when majority is achieved that block is considered as the valid block which added to the current longest chain and invalid blocks are rejected by not working on them [1].

Blockchain can be used as Key exchange protocol for authentication of the document called Blockchain-based Authenticated Key Exchange Protocol (BAKE). This can meet the security needs and the computational demands of scenarios that require strangers to bootstrap trust in an untrustworthy environment. Multiple unfamiliar parties authenticate common secret holders through Blockchain transactions and complete the exchange of session keys on the premise of privacy protection [2].

Blockchain technology can be used as a new solution based on public ledgers that is actually able to remove any single. It also provides high reliability and security in the distribution of certificate and revocation of information [3].

Along with the crypto currency and the certification system this technology can be used in cyber security, Health care, Identity management of the citizens, supply chain to track the product, finance industry and many other areas. All this because of its secure and transparent way of managing the information [4].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

A. Blockchain

The concept of blockchain was first proposed by a person (or a group of persons) named Satoshi Nakamoto in 2008. It is a shared distributed ledger governed by the set of rules where each node participating in the blockchain network keeps record of all the data in network.

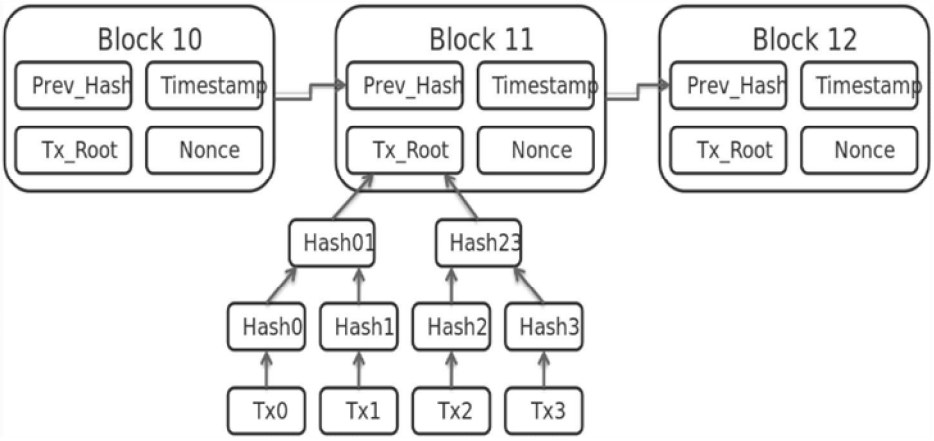


Fig. 1 from https://en.wikipedia.org/wiki/Blockchain shows the basic structure how the blocks in blockchain are connected with each other and content in them.

The data of multiple transactions is stored in the form of blocks along with its timestamp, each transaction can be separately verified by using its hash value, since it is open, publicly verifiable and the data once entered cannot be altered which help in preventing forgery. In blockchain each block of transactions is linked to the previous block by the hash value of preceding block. Hence if anyone tries to change any data in the blockchain the hash value of that block will be changed.

B. Ethereum

Ethereum is an open source computing platform based on Blockchain and operating system featuring smart contract. Ether is the crypto-currency which is generated on Ethereum blockchain that can be transferred between different accounts. It also provides decentralized Ethereum virtual machine which can execute the scripts using network of public nodes which is thought to be Turing complete and gas is the internal transaction pricing mechanism. Ethereum provides the platform for creating the decentralized application based on smart contract.

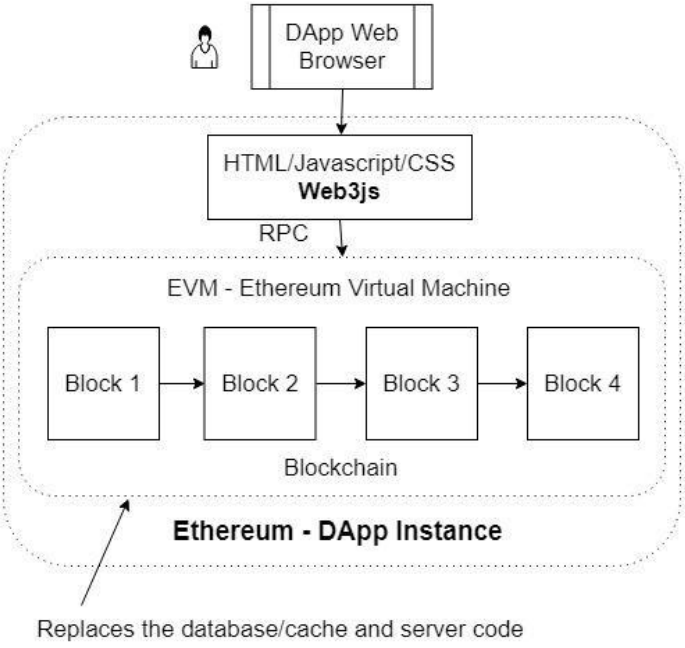


Fig. 2 Ethereum Dapp Architecture

Decentralized Application (Dapp) is the application also a type of blockchain enabled website that runs on peer to peer network of computers.
In this the smart contract act as a backend code. Dapp is connected to smart contract using web3js.
Web3js is a collection of libraries that allows user to interact with the local or remote Ethereum node using HTTP or IPC connection.

C. Smart Contract

Smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to the smart contract agree to interact with each other on certain conditions. The code in contract will execute on occurrence of particular event.

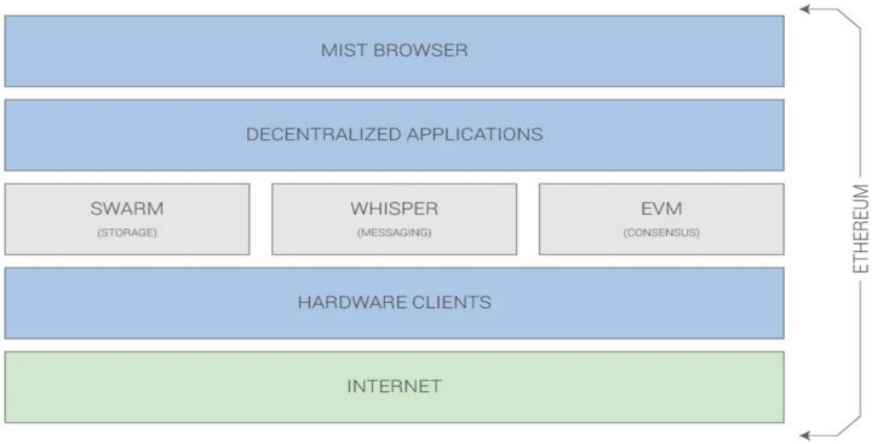


Fig. 3 Web 3.0 Tech Stack

D. Ethereum Virtual Machine

Ethereum sense refers to a suite of protocols that define a platform for decentralized applications. At the core of it is the Ethereum Virtual Machine ("EVM"), which execute code of arbitrary algorithmic complexity. In computer science, Ethereum is "Turing complete". Developers can create applications that run on the EVM using programming languages modified on existing languages like JavaScript.

III. PROPOSED WORK

A. System Design

In this study, a blockchain certificate system will be developed based on relevant technology. The system's application will be programmed on the Ethereum platform and will be run by the EVM. In the system, three groups of users will be involved, (Fig. 4). Schools or certification units will grant certificates, will have access to the system, and will be able to browse the system database. When students will fulfill certain requirements, the authorities will grant a certificate through the system. After the students have received their certificate, they will be able to inquire about any certificate they have gained. The service provider will be responsible for system maintenance [5].

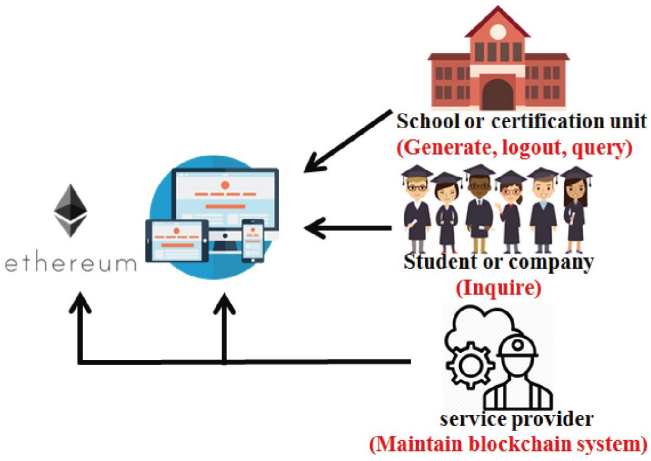


Fig. 4 Configuration of Blockchain Based System

B. Process

To create the blockchain based unmodifiable certificates, initially the university needs to get registered. Each university will be having its wallet address from which it is going to send transaction. University can be added only by the owner of the smart contract. Once added the university can access the system and can create certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS) which in turn will return the unique hash generated using SHA-2S6 algorithm. This will serve as unique identity for each document. Along with this generated hash and detail of certificates, all this data will be stored in the blockchain and the resultant transaction id will be sent to the student. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it is almost impossible to modify this certificate or to create fake certificate with same data. Hence with this we can solve the problem of counterfeit certificates.

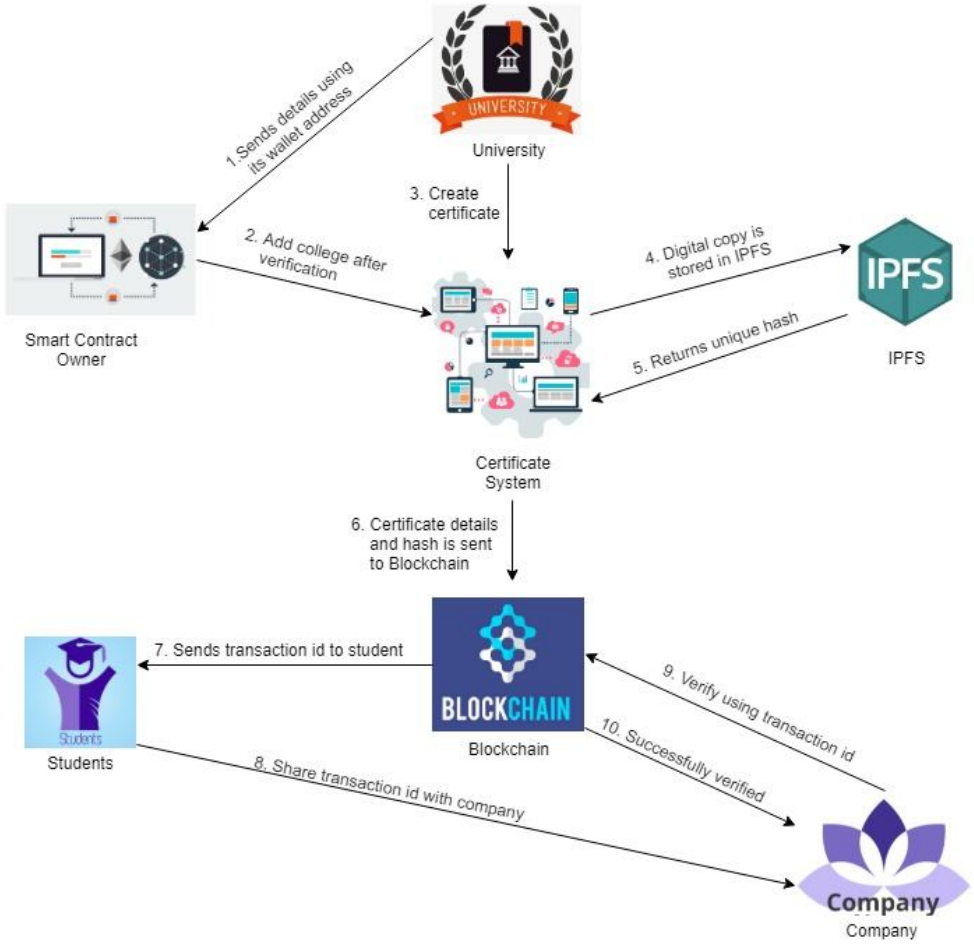


Fig. 5 This figure shows the data flow diagram of the system.

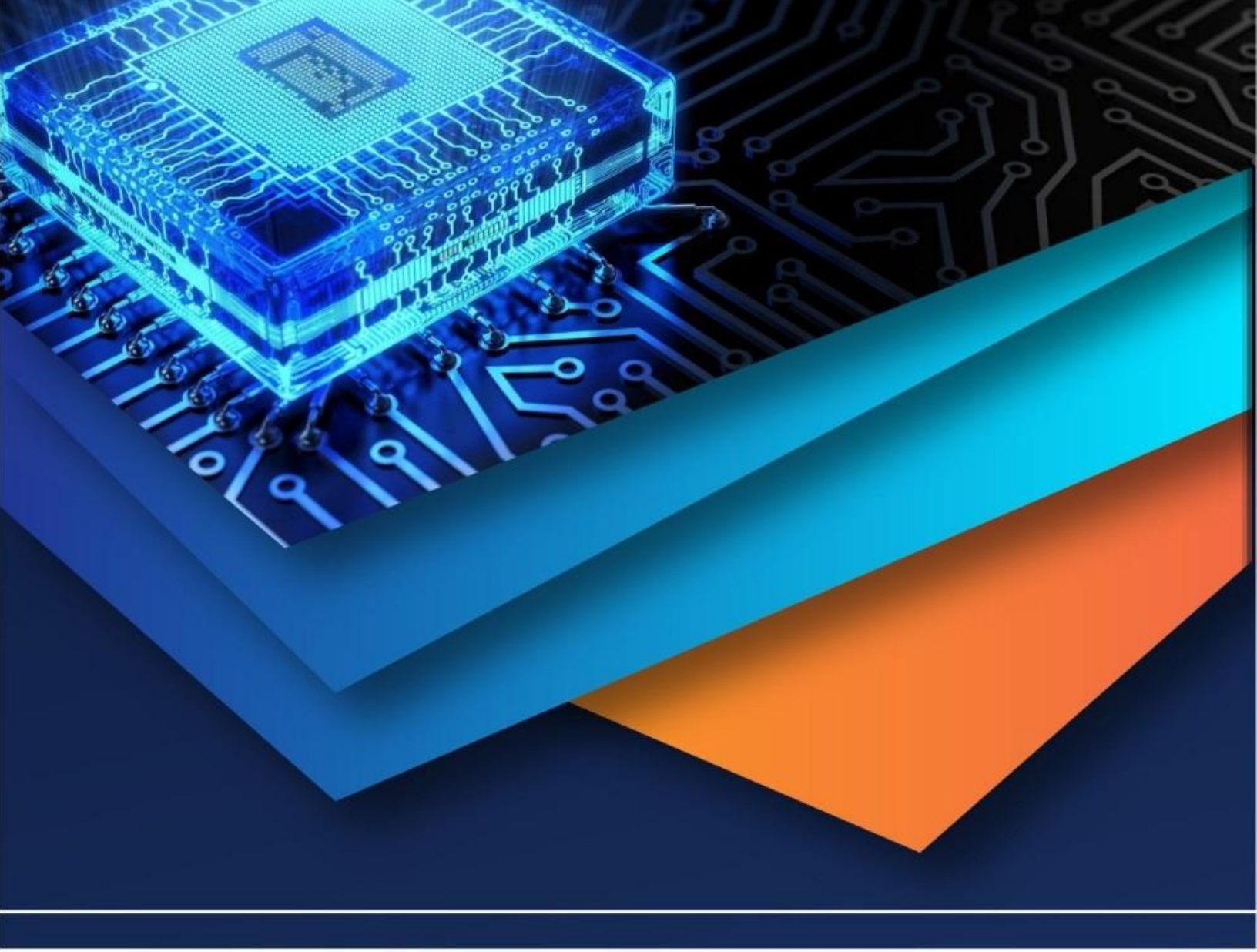
IV. CONCLUSION

Data immutability is one of the main features of blockchain. It serves as a large public ledger where node in network verifies and save the same data. The process of certificate generation is open and transparent system where any organization can verify information of any certificate using this system. In conclusion the system helps in eradicating problems of fake certificates.

REFERENCES

[1] Satoshi Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* www.bitcoin.org.
[2] Hailong Yao, Caifen Wang, *"A Novel Blockchain-Based Authentication Key Exchange Protocol and Its Applications,"* 2018 IEEE Third International Conference on Data Science in Cyberspace.
[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi, *"Certificate Validation through Public Ledgers and Blockchains,"* In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.
[4] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, Ben Amaba, *"Blockchain Technology Innovations,"* 2017 IEEE Technology & Engineering Management Conference (TEMSCON).

[5] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, *"Blockchain and Smart Contract for Digital Certificate,"* Proceedings of IEEE International Conference on Applied System Innovation 2017.
[6] W. Diffie, P. C. Van Oorschot, M. J. Wiener, *"Authentication and authenticated key exchanges,"* Designs, Codes and cryptography 2(2), 107-125 (1992).
[7] G. O. Karame, E. Androulaki, S. Capkun, *"Double-spending fast payments in bitcoin,"* Proceedings of the 2012 ACM conference on Computer and communications security, pages 906-917. ACM, 2012.
[8] T. Bui, T. Aura, *"Key Exchange with the Help of a Public Ledger,"* F. Stajano, J. Anderson, B. Christianson, V. Matyáš (eds) Security Protocols XXV. Security Protocols 2017. Lecture Notes in Computer Science, vol 10476. Springer (2017).
[9] Benyuan He, *"An Empirical Study of Online Shopping Using Blockchain Technology,"* Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
[10] Zhenzhi Qiu, *"Digital certificate for a painting based on blockchain technology,"* Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
[11] Xiuping Lin, *"Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain,"* Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.
[12] Yong Shi, *"Secure storage service of electronic ballot system based on block chain algorithm,"* Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
[13] S. Underwood, *"Blockchain beyond bitcoin,"* Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.
[14] G. Hurlburt, *"Might the Blockchain,"* no. April, pp. 12–16, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY