iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43637

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 10 Issue VI June 2022- Available at www.ijraset.com

An Analysis of Ethereum-Based Healthcare Applications Using Blockchain Network

Monisha K[2], Vidhya K[1]

[1]*Student B.E,* [2]*Assistant Professor, Department of Information Science & Engineering, EWIT, Bangalore, Karnataka, India*

Abstract— Years of heavy regulation and bureaucratic ineffificiency have slowed innovation for electronic medical records (EMRs). We employ a security risk management (SRM) domain model and a methodology to investigate two security risks – Sybil and Double-spending – that have been identified and are regarded the most significant security issues in blockchain systems. We tested a newly developed framework by looking at the hazards of Sybil and Double-spending in Ethereum-based healthcare apps. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. Finally, we deploy the MIStore on the Ethererum blockchain and give the corresponding performance evaluation. We wrap off the study by laying out our plans for developing an ontology-based blockchain security reference model.

Keywords— Sybil risk, Double-spending risk, Ethereum-based healthcare apps, Electronic medical records, big data

I. INTRODUCTION

Blockchain is a distributed, immutable, and decentralised ledger technology[1]. When a new block (or transaction) occurs[2],[3], blockchain technology uses a peer-to-peer (P2P) network to disseminate a ledger across the whole P2P network. Every every transaction ever done[4] is recorded in a ledger, which is accurate and verifiable. Blockchain technology has the potential to address security concerns, improve data integrity, and convert the transaction process into one that is decentralised, transparent, and immutable. As a result, security is critical in ensuring blockchain adoption. Because of decentralised consensus, an immutable ledger, and encryption, blockchain systems are thought to be less susceptible.

We use the SRM domain model to provide a framework for investigating Sybil and Double-spending threats in blockchain systems[5],[6]. The SRM domain model allows for a systematic analysis of security risks from the standpoint of asset-related, risk-related, and risk treatment-related concepts. The asset can be characterised as a business asset or a system/information system asset. The business asset is valuable, and the system asset helps to sustain it. Business asset restrictions (C - Confidentiality, I - Integrity, and A - Availability) identify security needs. The risk is a mix of risk event and impact in risk-related concepts. The asset is harmed, and the security standards are violated.The danger plus one or more vulnerabilities make up the risk event. The threat agent triggers the threat, which is directed against the system asset. The threat agent employs a technique of attack and exploits the flaw. Decisions to treat security risks by setting security requirements are presented in the risk treatment-related concepts. Security controls are used to implement security requirements.

The rest of the paper is structured as follows: Section 2 presents the background of Sybil and Double-spending risks. Section 3 gives an overview of framework use. Section 4 concludes the paper. Section 5, we conferfuture work and threats to validity.

II. BACKGROUND

A. Sybil Risks

Douceur talked about the Sybil assault on peer-to-peer (P2P) networks[7]. P2P systems do not rely on a central trusted party chain of trust to validate the identity of each participating node, and identities on P2P systems that treat everyone equally on the network are also quite cheap to produce. Finally, the attacker use Sybil nodes and an attack technique to unleash a slew of threats that degrade a P2P network's reputation system[8],[9]. Sybil attacks are difficult to avoid, although there are precautions that may be taken to strengthen security against Sybil assaults.

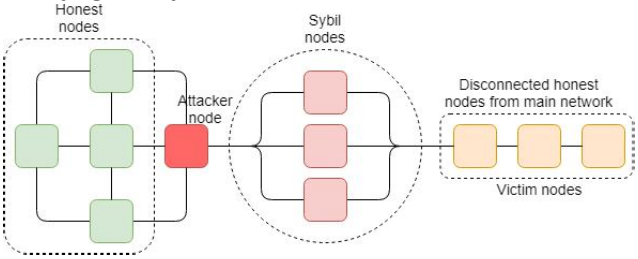


Fig. 1 Node isolation attack on honest nodes. The attacker divides the blockchain network into two disjoint groups.

1) *Nodes Isolation (Partition) Attack:* The attacker hijacks the honest nodes and divides the network into two or more fragmented groups[10],[11] in a nodes isolation attack. The attacker first identifies the target nodes, then replaces the victim nodes' peers with Sybil nodes, as seen in Fig. 1. The attacker then isolates the victim nodes and disconnects the transactions they've started. In their regulated blocks, attacker nodes are now involving victim nodes.

In this instance, the attacker gets proportionate control of the system and may prevent transaction and block propagation, validate false or double-spend transactions, and receive mining incentives, among other things. BGP is a routing protocol that does not check the routing origin. The attacker takes advantage of this flaw by utilising Sybil nodes to advertise certain genuine IP prefixes. When honest nodes link to Sybil nodes, the attacker can intercept communication and delay block propagation, causing transaction verification to fail. There are presently no mechanisms in place to completely counteract the Sybil-based nodes isolation assault, although there are some preventative measures in place. For example, according to the available nodes in the network, increase the computing power[12] in the blockchain network and monitor the nodes' computing power. Monitor the round-trip time to look for unusual trends during data exchange and transmission between nodes.

B. Double-Spending Risks

Double-spending is a digital currency risk in which an attacker can spend the same money twice for monetary gain[13]. The attacker may, for example, alter the transaction state and spend the same transaction twice. The possibility of double-spending compromises the ledger's integrity. There are several risks that might induce Double-spending, including Sybil-based Double-spending, 51 percent assault, and so on. We use the term blockchain systems that is combining the blockchain platforms (e.g., Bitcoin, Ethereum, Hyperledger Fabric) and blockchain-based applications (e.g., decentralised applications (dApps)).

1) *Eclipse-Based Double-Spending:* The Sybil assault attacks the whole network, whereas an eclipse attack just targets a single node(s)(Fig. 2.)[14]. To disconnect the target node from the blockchain network, the attacker floods it with his IP addresses and attaches himself directly to it. By refusing to communicate/gossip with other peer nodes, the attacker stops the victim node from knowing about the rest of the blockchain network. The eclipse assaults target a single node or nodes, such as powerful miners or merchants. The attacker uses 0-confirmations or N-confirmations in quick payments to cause double-spending in Eclipse-based Double-spending. The 0-confirmations technique is used to make rapid payments attractive for both the business and the customer. The 0-confirmation transaction (also known as an unconfirmed transaction) is stored in the honest nodes' mempool but has not yet been added to the blockchain.

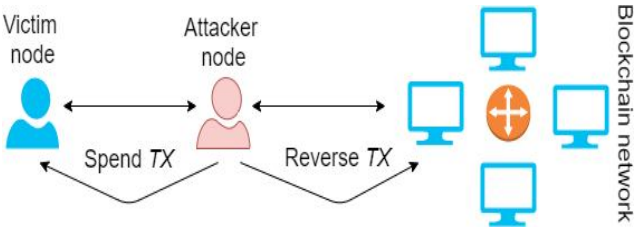


Fig. 2 Eclipse-based 0-confirmations Double-spending.

III. FRAMEWORKS

We'll talk about how to use a recently designed framework in this part. We chose two Ethereum-based healthcare decentralised applications (MedRec and MIStore).

A. Healthcare dApps

Healthcare information is private and confidential, and it must be protected. Health documents that have been falsified or lost might pose serious problems throughout the patient's treatment[15]. Several research projects have been undertaken in the past several years to assure data integrity, patient ownership of his data, simple interchange of medical data[16], and medical insurance claims utilising blockchain technology.

1) *MedRec dApp:* The MedRec[16] dApp is a decentralised electronic health record (EHR) and data management system for medical research (Fig. 3). Patients may use the dApp to manage their data and access their medical records across providers and treatment venues. It makes use of blockchain technology to enable quick access to medical data, system interoperability, and better data quality.As network participant nodes, MedRec comprises hospitals, patients, and researchers (e.g., physicians, institutions, and public health authorities).

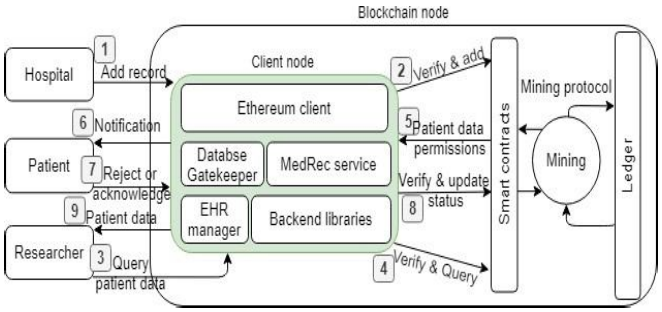


Fig. 3 MedRec system orchestration.

Client node, smart contracts, mining, mining protocol, and immutable ledger are all included in a blockchain node. Each participant node in MedRec is responsible for one client node, on which an Ethereum client (such as PyEthApp) implements the Ethereum platform standard (e.g., connection with P2P network, encoding and sending transactions). The MedRec service monitors real-time changes to alert the EHR manager, who then sends a patient notice and uses a database gatekeeper to sync the off-chain database. To make the MedRec service work, backend libraries interface with an Ethereum client. The hospitals are in charge of entering the patient's medical information.

The attacker can build Sybil nodes to launch a nodes isolation attack in MedRec since the nodes are restricted. The attacker employs honest nodes to participate in the attacker regulated blocks or consensus process while using a nodes isolation attack. This exploit might lead to the attacker validating incorrect data (for example, registering an invalid patient), stealing and selling patient medical data, or verifying unlawful medicine prescriptions.

2) *MIStore dApp:* The MIStore[17] dApp is a decentralised storage solution for medical insurance (Fig. 3). MIStore uses the immutability of blockchain ledgers to provide consumers with high-credibility insurance services. As network participant nodes, MIStore incorporates hospitals, patients, the insurance company, and n-servers. N-servers are nodes that validate a transaction's validity. A blockchain node combines an Ethereum client with smart contracts, mining, mining protocol, and an immutable ledger to execute the Ethereum platform specification. Access control governs the activities of the insurance company and other nodes accessing patients medical data, and other parameters let MIStore run well. The medical treatment costs of patients that initiate the insurance claim transaction are added by the hospitals. Double-spending can be utilised for insurance fraud in MIStore. To accomplish Double-spending using Eclipse-based Double-spending, the attacker will eclipse the node of a patient.The hospital begins and submits an insurance claim transaction (IT0) to an insurance company (IC). IT0 is sent to a patient for verification once IC confirms its authenticity.

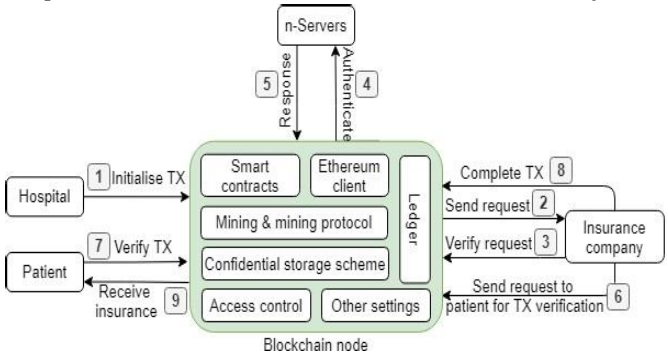


Fig. 4 MIStore system orchestration.

The attacker gets the IT 0 transaction and sends a patient a conflicting transaction (AT 1) for verification. The patient checks the AT 1 and responds to the IC with a response message. Because IC only understands IT 0, the IT 0 transaction is completed. The system then invalidates the conflicting transaction (AT 1), granting the attacker insurance. Furthermore, because the IC validates transactions with 0-confirmations, it is possible that the transaction will be double-spent owing to a 0-confirmations race attack.

B. Countermeasures

To minimise Sybil and Double-spending risks vulnerabilities inside MedRec and MIStore dApps, the countermeasures are set based on the framework. V#1 may, for example, be handled by increasing processing power. To get around V#2, keep an eye on the round-trip time to look for unusual patterns. Vulnerability V#3 is mitigated by requesting a network joining fee,

authenticating node connections, and monitoring node activity before entering the blockchain network. V#4 is managed via managing computing power, such as through the use of a computational constraint-based Sybil resistance approach, which demands expending computational resources according to the amount of identities created.Vulnerability V#5 may be managed by limiting incoming connections, introducing white-listed nodes for outgoing connections, and creating new connections using only random selection. To reduce V#6, increase confirmed blocks in Eclipse-based Double-spending. Using additional confirmed blocks, increasing a listening period, inserting an observer, notifying honest nodes, E-cash protocol, and upgraded observers, the V#6 might be neutralised in a 0-confirmations race attack.

IV. CONCLUSION

This study proposes a methodology for investigating Sybil and Double-spending vulnerabilities in blockchain systems based on the security risk management domain model. We tested a newly developed approach by looking at the hazards of Sybil and double-spending in Ethereum-based healthcare dApps. Finally, we discuss future research directions and validity risks. The conclusions of this study might help software engineers and decision-makers understand the hazards of Sybil and Double-spending while developing blockchain systems.

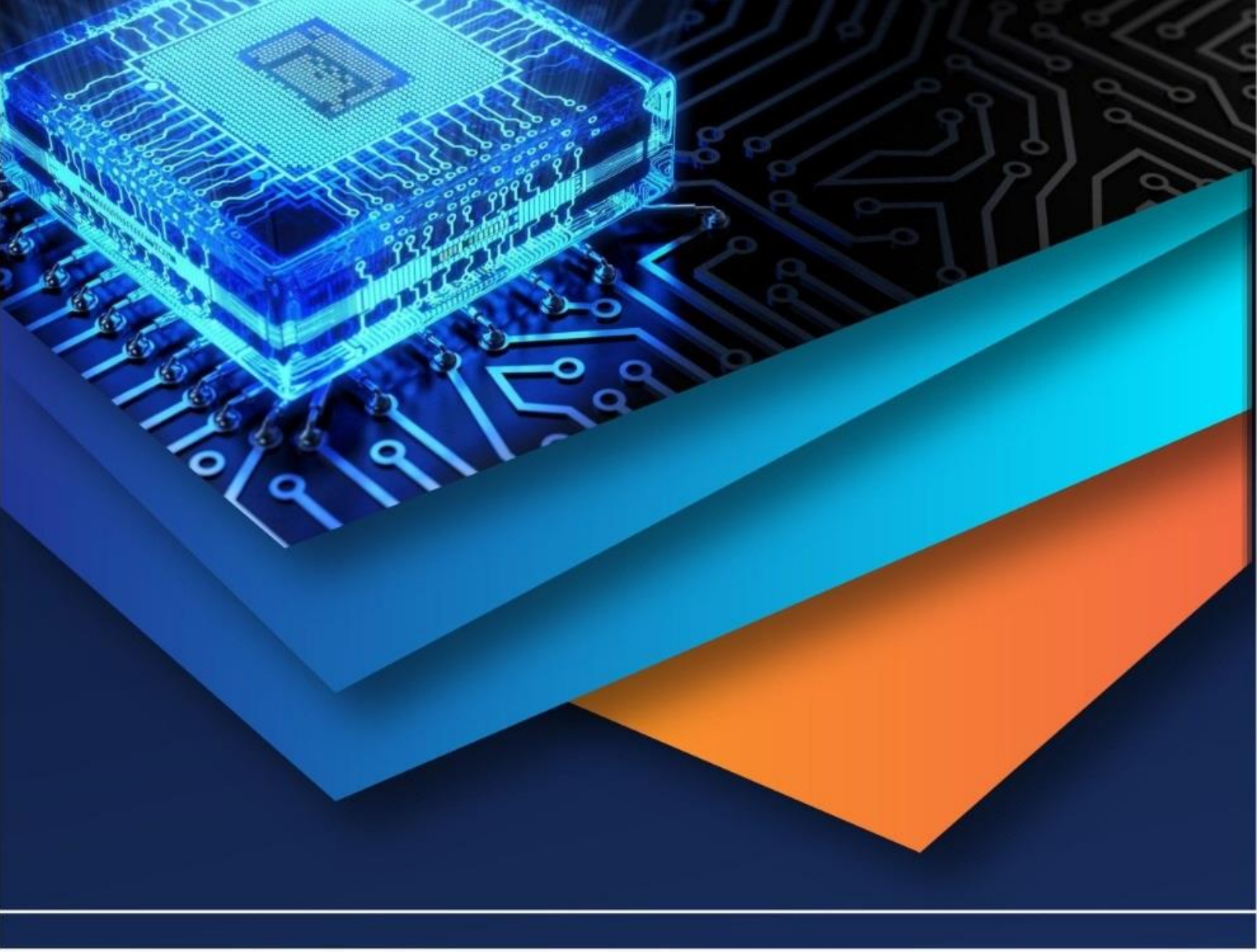
V. FUTURE WORK

We want to develop an ontology-based blockchain security reference model as a security risk management tool for systematically evaluating the security requirements of blockchain systems in the future. As a proof of concept, we built a Corda-based security ontology (CordaSecOnt) based on an ontological analysis that incorporates blockchain-based Corda platform in our earlier work. The CordaSecOnt project builds a semantic knowledge base using the Web ontology language (OWL) to eliminate conceptual ambiguity and a semantic gap in the financial industry's information security. The SRM domain model is used by CordaSecOnt to classify assets, threats, vulnerabilities, risk treatments, security needs, and countermeasures.

This framework may be used as a decision support tool in the same way that the ontology-based security reference model can. Based on security risks and weaknesses, the tool would assist in determining security countermeasures. The SRM domain model will be used to guide the development of a decision support tool. It also allows for a dynamic and seamless method to adding new knowledge and analysing blockchain security issues. To explain the assets to protect, security risks, threats, vulnerabilities, and countermeasures of blockchain-based applications, for example.

REFERENCES

[1] T. Sato and Y. Himura, ‘‘Smart-contract based system operations for permissioned blockchain,’’ in Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Feb. 2018, pp. 1–6.
[2] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, ‘‘BlockChain technology beyond bitcoin,’’ Dept. Eng., Sutardja Center Entrepreneurship Technol., Berkeley, CA, USA, 2015, pp. 1–35.
[3] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, ‘‘ReGuard: Finding reentrancy bugs in smart contracts,’’ in Proc. 40th Int. Conf. Softw. Eng., Companion, May 2018, pp. 65–68.
[4] N. Atzei, M. Bartoletti, and T. Cimoli, ‘‘A survey of attacks on Ethereum smart contracts (SoK),’’ in Proc. Int. Conf. Princ. Secur. Trust, 2017, pp. 1–24.
[5] É. Dubois, N. Mayer, P. Heymans, and R. Matulevièius, ‘‘A systematic approach to define the domain of information system security risk management,’’ in Intentional Perspectives on Information Systems Engineer-ing. Berlin, Germany: Springer, 2010, pp. 289–306.
[6] R. Matulevicius, Fundamentals of Secure System Modelling. New York, NY, USA: Springer, 2017.
[7] J. R. Douceur, ‘‘The Sybil attack,’’ in Proc. Int. Workshop Peer Peer Syst.,2002, pp. 251–260.
[8] P. Otte, M. de Vos, and J. Pouwelse, ‘‘TrustChain: A Sybil-resistant scalable blockchain,’’ Future Gener. Comput. Syst., vol. 107, pp. 770–780,Jun. 2020.
[9] P. Swathi, C. Modi, and D. Patel, ‘‘Preventing Sybil attack in blockchain using distributed behavior monitoring of miners,’’ in Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2019, pp. 6–11.
[10] J. H. Mosakheil. (2018). Security Threats Classification in Blockchains. [Online]. Available: https://repository.stcloudstate.edu/msia_etds/48
[11] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, ‘‘A stealthier partitioning attack against bitcoin peer-to-peer network,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2020, pp. 894–909.
[12] S. Sayeed and H. Marco-Gisbert, ‘‘Assessing blockchain consensus and security mechanisms against the 51% attack,’’ Appl. Sci., vol. 9, no. 9, p. 1788, Apr. 2019.
[13] R. Pass and E. Shi, ‘‘FruitChains: A fair blockchain,’’ in Proc. ACM Symp. Princ. Distrib. Comput., Jul. 2017, pp. 315–324.
[14] S. Zhang and J.-H. Lee, ‘‘Double-spending with a Sybil attack in the bitcoin decentralized network,’’ IEEE Trans. Ind. Informat., vol. 15, no. 10, pp. 5715–5722, Oct. 2019.
[15] Y. Du, J. Liu, Z. Guan, and H. Feng, ‘‘A medical information service platform based on distributed cloud and blockchain,’’ in Proc. IEEE Int. Conf. Smart Cloud (SmartCloud), Sep. 2018, pp. 34–39.
[16] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ‘‘MedRec: Using blockchain for medical data access and permission management,’’ in Proc. 2nd Int. Conf. Open Big Data (OBD), Aug. 2016, pp. 25–30.
[17] L. Zhou, L. Wang, and Y. Sun, ‘‘MIStore: A blockchain-based medical insurance storage system,’’ J. Med. Syst., vol. 42, no. 8, pp. 148–165, Aug. 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY