iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53696

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 11 Issue VI Jun 2023- Available at www.ijraset.com

Security Management for Transaction and KYC using Block Chain Technology

Prof. A.B. Bavane[1], Tushar Alhat[2], Saurabh Umbare[3], Pratik Shinde[4], Vishal Shinde[5]
[1]*Assistant Professor,* [2,3,4,5]*UG Students, Department Of Information technology Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Maharashtra, India Affiliated To Savitribai Phule Pune University*

Abstract: ***Blockchain technology promises to be hugely trending and empowering in financial domain computing applications. The digital economy is becoming an integral part of modern life. So as the use of the digital world increases there are more chances to decrease the security level. So more the use of digitization more the frauds and less the security.***
In some cases of personal data, leakage has brought back into the focus the security issues with the different identity sharing mechanisms. A customer is expected to provide his identity for authentication by different agencies. So the KYC process deals with the identification of the user. And in turn, provides the required security.
The KYC procedures which are used by the banks are completely dependent on the encryption which is slow and it can lead to the loss of customer details to other theirs party financial institutions. This system can be efficient by using Blockchain technology, which has the potential to automate a lot of manual processes and it is also resistant to hacks of any sort. The immutable blockchain block and its distributed ledger is the perfect complement to the process of KYC. With the addition of smart contacts, fraud detection can be automated.
For KYC identity details storage we can make use of any types of KYC. So, the banks can develop a shared private blockchain within the bank premise and the same can be used for verifying the documents. This allows the user to get control of their sensitive documents and also makes it easier for banks to obtain the documents they need for compliance.
Keywords: Blockchain, KYC verification, Security,Privacy

I. INTRODUCTION

A. Overview

A Blockchain-based security management system is for providing security to the bank transactions and to implement the KYC process in a more simpler and secured way. Blockchain technology is a new technology which is based on mathematical, cryptographic and economic principles for maintaining a database between various participants without the necessity of any third party or central authority. It is a secured distributed database, tamper evident, wherein the validity of a transaction can be verified by parties in the transaction.
Know Your Customer (KYC) processes performed by banks on their customers are unnecessary, unmanageable and costly. Therefore, a system is proposed to automate unskilled tasks and allow sharing of data related to KYC. Blockchain technology, with its concept of distributed database, time-stamped ledgers, can effectively help banks improve their KYC process.
One of the main tasks of the bank is to ensure information security of data of the customers, confidentiality and the state of their account to guarantee their safety and integrity, in the process of exchange and processing of information. Thus, by using the capabilities of innovative information technology i.e. the Blockchain technology information security can be achieved.

B. Motivation

KYC processes are generally repetitive, incompatible, tedious and duplicated, leading to high administrative overheads and costs. A blockchain-based solution, with its immutable ledger, ease of integration, and considerably lower operational and infrastructure costs, is undeniably a better option as compared to existing KYC processes.
Banking information has always raised the interest of intruders to it, so each bank needs to organize the security of the data it stores i.e. the state of their accounts, their transaction history, etc.
Blockchain is shared distributed ledger which stores transaction to a permanent chain which is unbreakable and can be viewed by the parties in a transaction.
The vulnerabilities in cyber-attacks in transaction can be over-come by this technology

II. RELATED WORK

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Block chain technology.

R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens present the concept between two arrangements of electric vehicles, which fundamentally diminish the effect of the charging procedureon the power framework amid business hours. This trading approach is also economically beneficial for all the users involved in the trading process. An activity-based approach is used to predict the daily agenda and trips of a synthetic population for Flanders (Belgium) [1].

Y. Xiao, D. Niyato, P. Wang, and Z. Han provide a study of the possible flow and functional factors that enable DET in communication networks. Various design issues on how to implement DET in practice are discussed. An ideal approach is created for delay-tolerant remote controlled correspondence organizes in which every remote powered device can masterminded its information transmission and energy exchanging activities as indicated by present and future vitality accessibility [2].

J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a work to accomplishes request reaction by giving motivating forces to releasing PHEVs to adjust nearby power request out of their own self-interests. Be that as it may, since exchange security and security insurance issues show genuine difficulties, they investigate a promising consortium block-chain innovation to enhance exchange security without dependence on a confided in outsider. A restricted P2P Electricity Trading framework with Consortium block- chain (PETCON) strategy is proposed to represent detailed activities of limited P2P power exchanging [3].

N. Z. Aitzhan and D. Svetinovic presents a work that address the issue of providing transaction security in decentralized smart grid energy trading without confidence on trusted third parties. We have developed a proof-of-concept for decentralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging flows, enabling peers to anonymously negotiate energy prices and securely perform trading transactions [4].

M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now presents a work that shows decentralized computerized cash, called NRG-coin. Prosumers in the smart grid framework exchange privately made sustainable power source utilizing NRG-coins, the estimation of which is indented on an open cash trade advertise. Like Bit-coins, this money proposes various favorable circumstances over fiat cash, however not at all like Bit-coins it is made by infusing vitality into the matrix, as opposed to giving vitality on computational influence. Likewise, they make a novel exchanging worldview for purchasing and offering environmentally friendly power vitality in the smart grid network [5].

S. Barber et al presents a work that Bit-coin is isolated computerized cash which has pulled in a significant number of clients. They play out a top to bottom examination to comprehend what made Bit-coin so effective, while many years of research on cryptographic e-money have not prompt a vast scale appropriation. They ask additionally how Bit-coin could turn into a decent contender for seemingly perpetual stable money [6].

Alqassem et al presents a work that Bit-coin is constantly improved by an open source network, and different Bit-coin libraries, APIs, and elective usage are being created. All things considered, there is no up and coming convention contrast or design portrayal since the authority whitepaper was distributed. The work demonstrates an a la mode convention detail and design investigation of the Bit-coin framework. We play out this examination as the initial move towards determination of the cryptographic currency reference design [7].

K. Croman et al presents a work that the expanding fame of block-chain-based digital forms of money has made versatility an essential and earnest obligation. The work ponders how essential and incidental bottlenecks in Bit-coin restrict the ability of its present distributed overlay system to help generously higher throughputs and lower latencies. These outcomes propose that re-parameterization of square size and interruption ought to be seen just as a first augmentation toward accomplishing people to come, high-stack block-chain conventions, and real advances will moreover require a fundamental reevaluating of specialized ways [8].

G. W. Peters and E. Panayi presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements [9].

L. Luu et al presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO scales exchange rates straightly with accessible estimation for mining: the more the calculation control in the system, the higher the quantity of exchange squares chosen per unittime. ELASTICO is productive in its system messages and permit complex foes of up to one-fourth of the aggregate computational power [10].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

III. PROPOSED SYSTEM

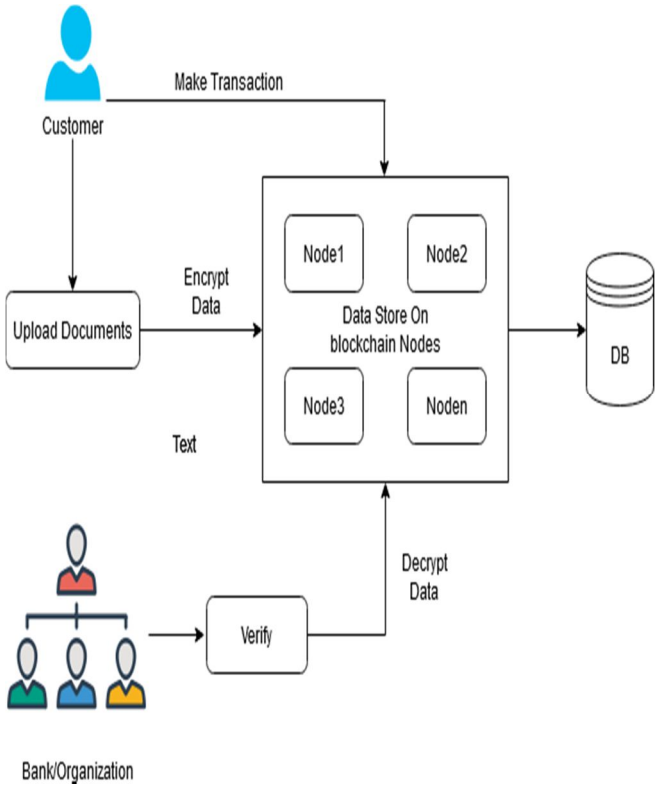


Fig. System Architecture

1) In proposed system, we implement a block chain Based KYC system, in which each customer upload a data files and encrypts these data with corresponding key.
2) To implement both security preservation and relevant searches, we propose an effective search scheme.
3) In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.

IV. ALGORITHMS USED

A. AES Algorithm for Encryption

AES (advanced encryption standard).It is a symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is a weakness in DES. The 56 bit key of des is no longer safe against attacks basedon exhaustive key searches and 64-bit block also consider as weak.AES was to be used128-bit block with128-bit keys. Rijendeal was the founder. In this drop we are using it to encrypt the data owner file. Input: ”128 bit /192 bit/256 bit input (0, 1)” Secret key ”(128 bit) +plain text (128 bit).” Process: 10/12/14-rounds for-128 bit /192 bit/256 bit input X or state block (i/p) Final round:10,12,14 Each round consists: sub byte, shift byte, mix columns, add round key. Output: Cipher text (128 bit)

B. MD5 Algorithm

MD5(Message-Digest Algorithm) The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. Steps: A message digest algorithm is a hash function that takes a bit sequence of any lengthand produces a bit sequence of a fixed small length. The output of a message digest is considered as a digital signature of the input data. MD5 is a message digest algorithm producing 128 bits of data. It uses constants derived to trigonometric Sine function. It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round. Most modern programming languages provides MD5 algorithm as built-in functions.

V. RESULTS

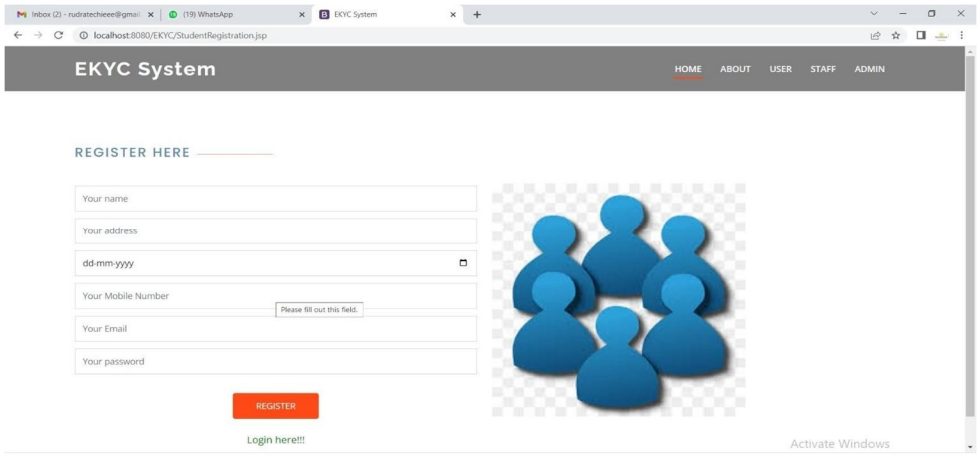


FIG.USER REGISTRATION

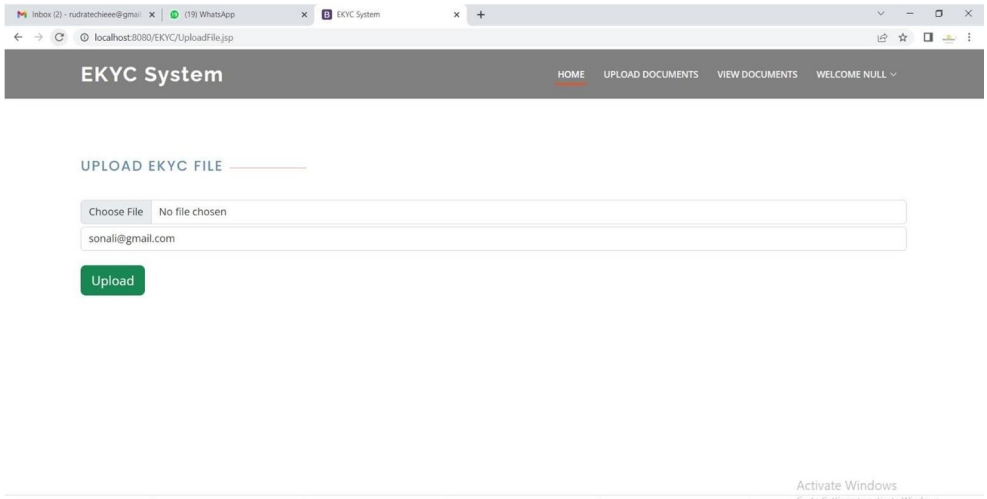


FIG.UPLOAD DOCUMENT

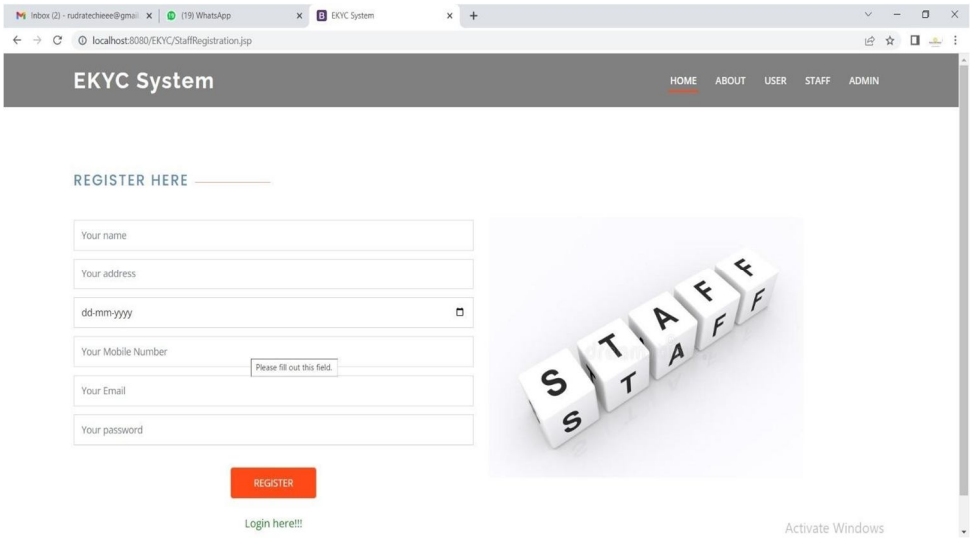


FIG.STAFF REGISTERED

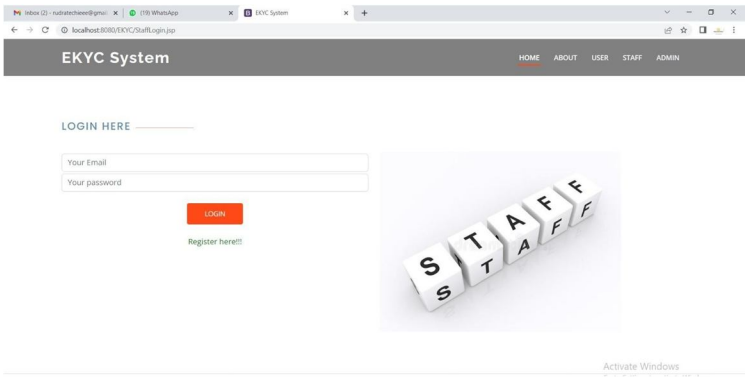


FIG.STAFF LOGIN

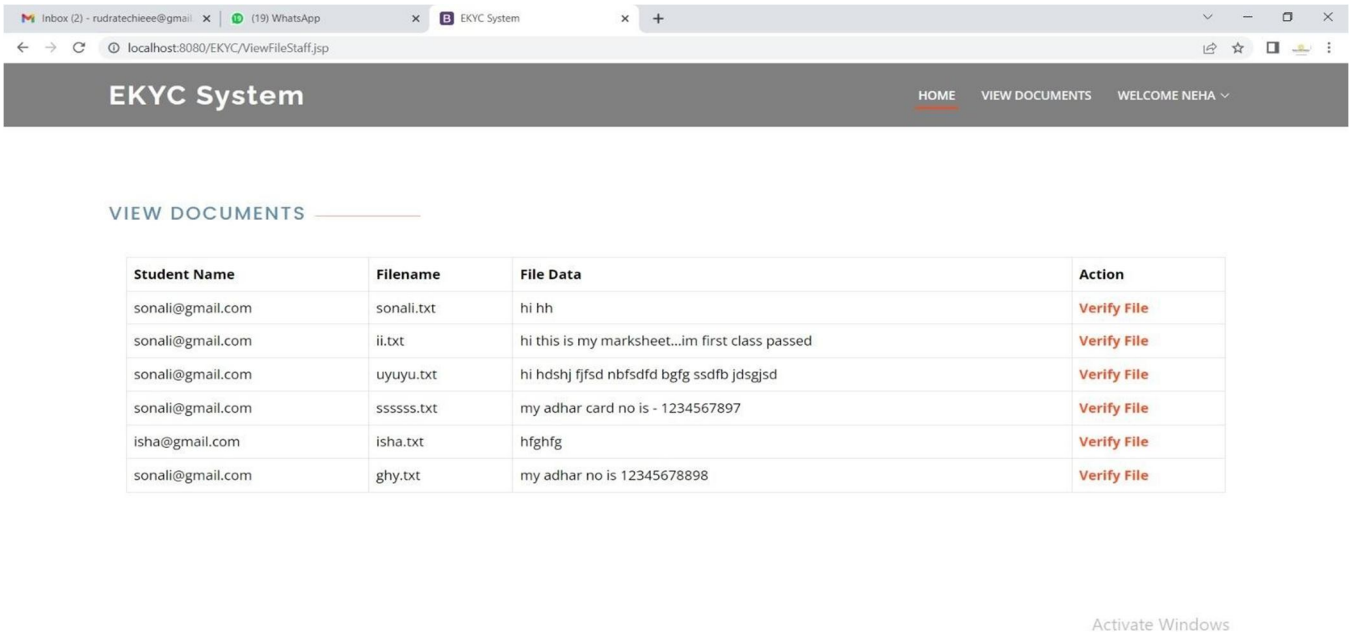


FIG.VIEW DOCUMENTS

VI. CONCLUSION

In many ways, Blockchain today is comparable to where the Internet was in early 20s. The development of information technology and electronic business every day has an increasingly significant impact on all spheres of the modern life. Blockchain technology is designed to change the traditional perception of how people interact through a network. The main advantage of the Blockchain technology is the complete synchronization of processes, integrity and uniqueness of all processed information, regardless of mining and tokens. Blockchain technology helps to improve distributed databases in terms of storage, synchronization, loss and integrity of data.

Its early days, but industry leaders are sponsoring a wide range of blockchain use cases supported by industry consortiums. Having seen the potential of this technology and the challenges, we think the opportunity is clear but the blue sky is too far off and companies need to validate use cases and business/technical viability before implementing blockchain.

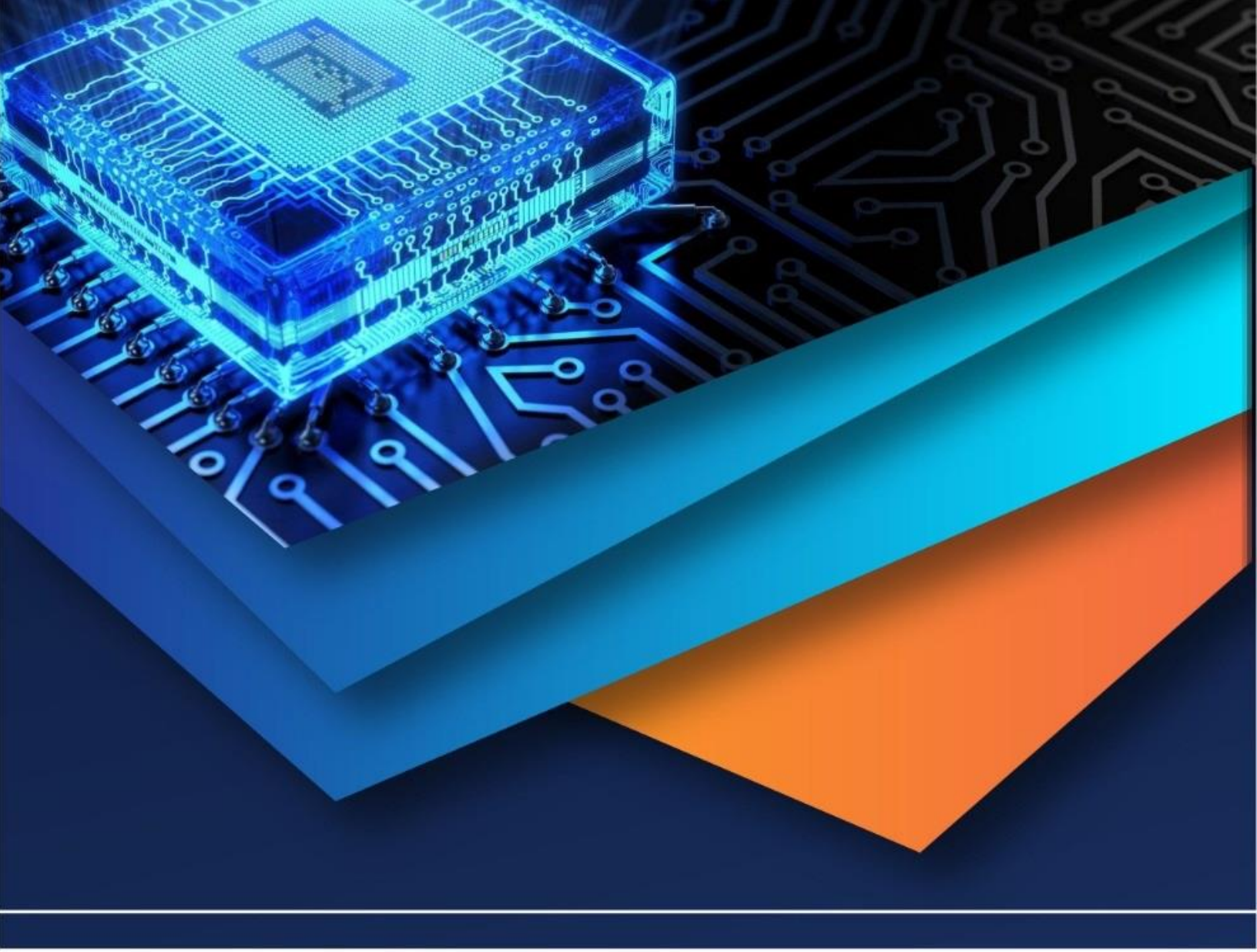
REFERENCES

[1] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, “Peer to peer energy trading with electric vehicles,” IEEE Intell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

[2] Y. Xiao, D. Niyato, P. Wang, and Z. Han, “Dynamic energy trading for wireless powered communication networks,” IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, “Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains,” IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[4] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Comput.
[5] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.
[6] S. Barber et al, "Bitter to better-how to make bitcoin a better currency," in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.
[7] I. Alqassem et al., "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in Proc. IEEE Internet Things, IEEE Int. Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.
[8] K. Croman et al., "On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.
[9] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.
[10] L. Luu et al., "A secure sharding protocol for open blockchains," Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY