iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46810

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 IX Sep 2022- Available at www.ijraset.com

Decentralized Cloud Storage Using Blockchain

G. Richa Shalom[1], Ganesh Rohit Nirogi[2]
Department of Computer Science and Engineering, Mahatma Gandhi Institute Of Technology, Hyderabad, India

Abstract: ***Because of its accessibility and ease of use, cloud storage has become the most widely used type of storage on the market in recent years. However, the privacy and data security of cloud storage are at risk. The protection of data security and privacy is the main topic of this essay. We suggest a blockchain-based decentralised storage system. Since blockchain is a distributed peer-to-peer system, any processing node connected to the internet can join and build peers' networks, maximising resource usage. Blockchain protects data security. The user's file is encrypted and shared among a number of network peers in the proposed system utilising the IPFS (Interplanetary File System) protocol. Hashes are generated by IPFS. The path of the file is indicated by the hash value, which is kept on the blockchain. This project is focused on decentralised secure data storage, high data availability, and effective storage resource usage.***

Keywords: Cloud Computing; Security; Availability; Reliability; Integrity; Blockchain, Decentralized, Privacy

I. INTRODUCTION

Information has become the most important asset for anybody because to the expanding sectors of information technology, the Internet of Things, and the digitization of all businesses, organisational activity, and initiatives. The most powerful thing in the world today is data. Given the volume of data and its continual growth, it's crucial to arrange its storage to make it both secure and easily accessible. Databases are being employed as a data warehouse for this purpose.

Due to the value of data and the lack of available storage, databases are replicated, distributed, and backed up in various methods. Data is stored by individuals in the cloud services offered by various private businesses. To store their data, organisations build up their data centres all over the world. Data is dispersed and replicated to various servers located in various locations for security and bandwidth reasons. This appears to offer a practical answer for the handling of data that is accumulating quickly.

The rise in demand for storage, where the data can be easily accessible from anywhere and at any time, has led to the increasing popularity of Cloud Storage systems. The Cloud storage implementes a central repository. This storage is vulnerable to cyber attacks, once an attacker gains access to the system complete confidential information is under breach. If a file gets modified there is no way of getting hands on the original data. Further the cloud storage units are handled by third parties, the user must comply with the regulations. Few problems are

1) *Lack of Privacy of Data* - Organizations' scattered data centres and various cloud service providers guarantee the data's availability and security. However, the majority of them contain clauses that grant the business access to edit, change, view, remove, and analyse your content. This can be done in order to give the customer the best service possible, make advertisements, alter the data in some way to make money, or use the data for their own needs or analyses. Data housed in a privately owned database allows that corporation several access privileges, making it occasionally insecure.
2) *Data Loss* - Storing sensitive data only on local machines or drives can sometimes be very lamenting because once they are stolen, lost or destroyed by any other means, the user cannot make a recovery. Moreover, most of the personal accounts of Cloud Storage also do not cover the insurance of data, take responsibility in case of data loss due to catastrophic failure as well as ensure data availability all the time. This is well stated on Terms and Conditions of Dropbox, Box, RapidShare,Google Drive, Amazon Cloud Drive, MS Onedrive etc. So, completely relying on data storage on your local machine only or on the cloud storage is just not always safe and genuine.
3) *Financial and other losses due to Data hack* - Furthermore, despite the tremendous potential worth of that data, it is not recommended to store sensitive user data in the cloud. Here, "sensitive information" refers to user passwords, wallet encryption keys, secret and confidential documents, papers containing sensitive information, records of financial transactions, etc., the loss or hacking of which could spell catastrophic failure for any business or person.

All Things considered issues like privacy, vulnerability stand out requiring an alternate way of storing data. A solution to this is the use of a decentralized cloud storage with blockchain.

©IJRASET: All Rights are Reserved

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was published in order to get into its hash. Blocks create a chain because each one has information about the block before it, hence strengthening the links in the chain. Because once recorded, the data in any given block cannot be changed retrospectively without changing all following blocks, blockchains are resistant to data manipulation. Consequently, ensuring that the data is secure and not exposed due to data distribution, which when viewed individually will not produce relevant information

The process we follow is like

a) To ensure a high level of data security, we encrypt the data and distribute it among numerous nodes.
b) Security is increased quickly with the AES encryption technique without impacting the system's performance.
c) The IPFS (InterPlanetary File System) protocol is used to encrypt and distribute the user's file among several network peers. Hashes are generated by IPFS. The blockchain stores the hash value, which identifies the file's path.
d) Proof-of-work is used by the peer-to-peer network to keep a public history of transactions.
e) Decentralizing the storage secures the data storage, provides high availability of data, and efficient utilization of storage resources.

II. RELATED WORKS

In 2020, "Decentralized Utility- and Locality-Aware Replication for Heterogeneous DHT-Based P2P Cloud Storage Systems," was published by Y. Hassanzadeh-Nazarabadi, A. Küpçü and O. Ozkasap.The advantages are there was higher availability of replica due to the use of Skip Graph Algorithm.[1]

In 2019, "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud," was published by M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri. The advantages are it addressed threats like on/off attack,Sybil attack and collusion attack.[2]

In 2019, Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications was published by Dong, Zhongli & Lee, Young-Choon & Zomaya, Albert. The advantages are we can develop and test our own Proof Of Useful Work(PoUW) consensus protocols.[3]

In 2018, "A Blockchain-Based Decentralized Data Storage and Access Framework for PingER," was published by S. Ali, G. Wang, B. White and R. L. Cottrell.The advantages are it used pingEr.[4]

III.RESEARCH METHODOLOGY

The objective of the project is to develop a decentralized storage system using blockchain. Initially the data owner first registers themselves. After registering successfully, the owner logs in and uploads a file using the file picker. The system checks the file size and ensures storage availability in the network. The file is uploaded when enough storage is available. Then the system performs steps. The uploaded file is encrypted using AES 256 bit algorithm. The encryption key is generated using the owner's wallet address and randomly generated salt value. This encryption key along with an IV is used to encrypt the owner's data. This maintains the confidentiality of the data. The encrypted file is then divided into blocks of 64KB and sent to different peers across the network with the help of the IPFS protocol. The proposed system uses a private IPFS network to allow registered peers to store the file in the network. This returns a hash value which indicates the path of the file. The hash value along with metadata is mapped with the user's wallet address and is stored in the blockchain using a smart contract. Smart contracts are utilised to do away with the necessity for a third party by acting as agreements. Under certain circumstances, they have control over the exchange of assets or transactions between nodes. These are lines of code that are stored on a blockchain network and are automatically run when certain criteria are satisfied. once it has been shared among peers. The only user who can combine all the small files into one large one is the one who possesses the hash values stored in the blockchain. Additionally, the data user must first register and log in. As long as the file's owner permits access, he can access the uploaded file. The user can look for the file and request access from the owner . If the owner gives permission to access the file, the user can view the file. The cloud storage has all the information about the data owner, the data user, the block data and they can also trace the data. The previous hash value and the current hash value needs to be given and the peer where the data has been stored can be tracked.

The internal operation of what takes place when data is edited is shown in figure below. Front end interactions that are submitted to a controller for information validation and forwarding result in data changes. Consensus algorithms run and examine each block as well as the newly added block. The P2P network's listings are updated if there are discrepancies, otherwise the block is accepted and adjustments are not made. The transaction list is then updated and the new block is inserted.

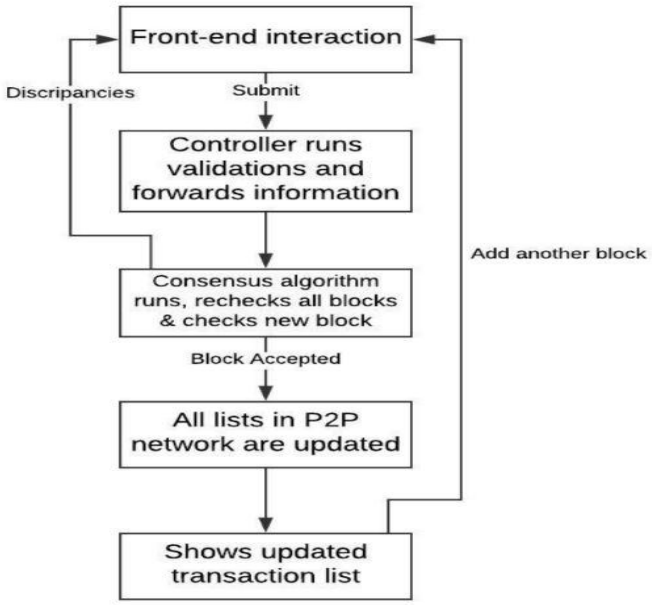


Fig 3.1:General work-flow of the program

A. IPFS Protocol

The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system. Each file in a global namespace connecting all computing devices is uniquely identified by IPFS via content-addressing. In contrast to a centralised server, IPFS is designed on a decentralised network of user-operators that each hold a piece of the total data, resulting in a robust system for sharing and storing files. Other peers in the network can locate and request that content from any node who has it using a distributed hash table, and any user in the network can serve a file by its content address (DHT).

B. Metamask

A browser add-on that serves as a bridge for the Ethereum network. A secure identity vault is a feature of MetaMask that offers a user interface for managing your online personas and signing blockchain transactions.

C. Ethereum

It is a distributed computing platform built on the open-source, public blockchain. Ethereum is a decentralised platform that supports Smart Contracts, which are programmes that execute exactly as intended with no chance of interruption, censorship, fraud, or outside interference. These apps are powered by a highly effective global shared infrastructure that can move value around and reflect the ownership of property. This infrastructure was created specifically for these apps. Without a mediator or counterparty risk, this enables developers to construct markets, hold registries of obligations or promises, move funds in line with instructions issued in the distant past (like a will or a futures contract), and many more things that have not yet been conceived.

D. Distributed Hash Table (DHT)

A hash table is a type of data structure that can store (key, value) pairs and look up values when a key is given. Given that they internally use arrays to store the data, the insertion and lookup of (key, value) pairs are extremely quick in the order of O(1). However, the array is always bigger than the entire number of (key, value) pairs, which slows down how quickly the hash table's entries are iterated over. A distributed service called Distributed Hash Table offers (key, value) pairs similar to Hash tables. In the distributed network, each node only keeps a predetermined number of (Key,Value) pairs. When a key is known, a technique or rule is created that enables the identification of the peer who might be in possession of the value. With one or more of these peers, the value is questioned. If the peer doesn't have the value, it makes inquiries with other peers until it does.

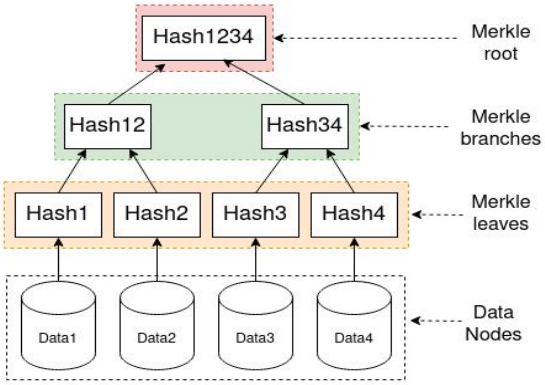


Fig.3.6 Working of Distributed Hash Table

IV. RESULTS AND DISCUSSION

Firstly, we enter eclipse and we run on server which initializes the Tomcat server at localhost. We get diverted into the homepage where the user and owner have to first register themselves and then they can login. The data owner can upload the files, view the uploaded files, view the requests for the files and also can send the key. The data user can search the file, send request to the owner to access the file and also view the file if the request gets approved. The cloud storage has all the information about the data owner, the data user, the block data and they can also trace the data. The cloud storage has login and the different methods like trace Data, block Data Info, data Owner Info and data User Info. The data owner has register and login and contains methods like upload File, view File, view Requests, send Key. The data user also has register and login and contains methods like search File and view Response. The database contains cloud storage, data owner and data user and the methods are trace data, upload File, data User info and view File. The database also can be accessed where the current and previous hash values can be seen. We can also trace the data by providing the current and previous hash value.

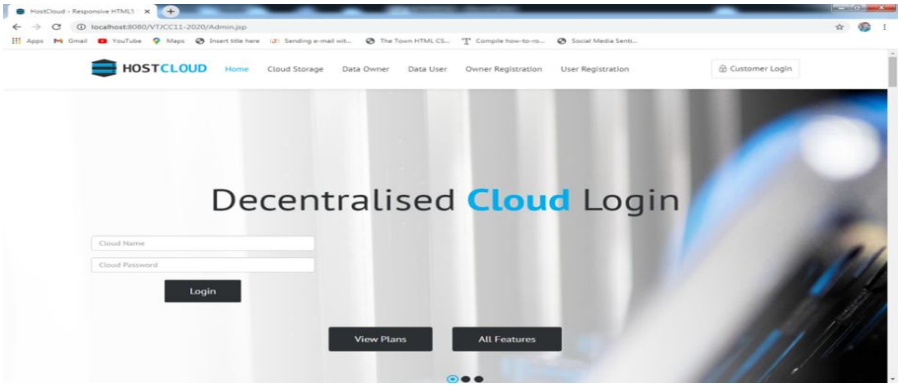


Fig.4.1.Cloud login page

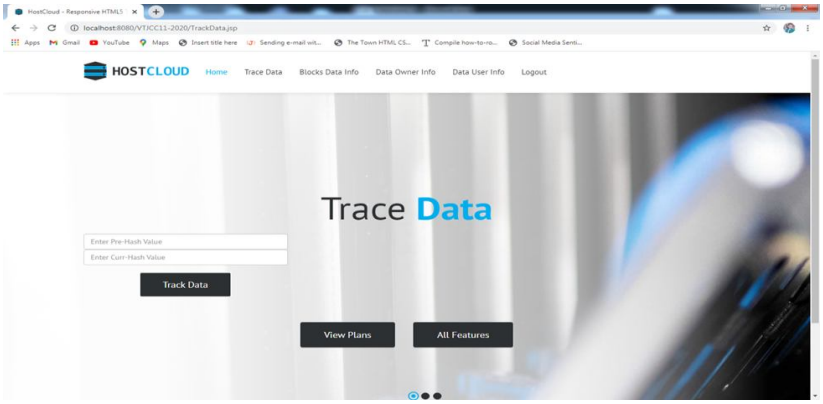


Fig.4.2.Page to trace the data

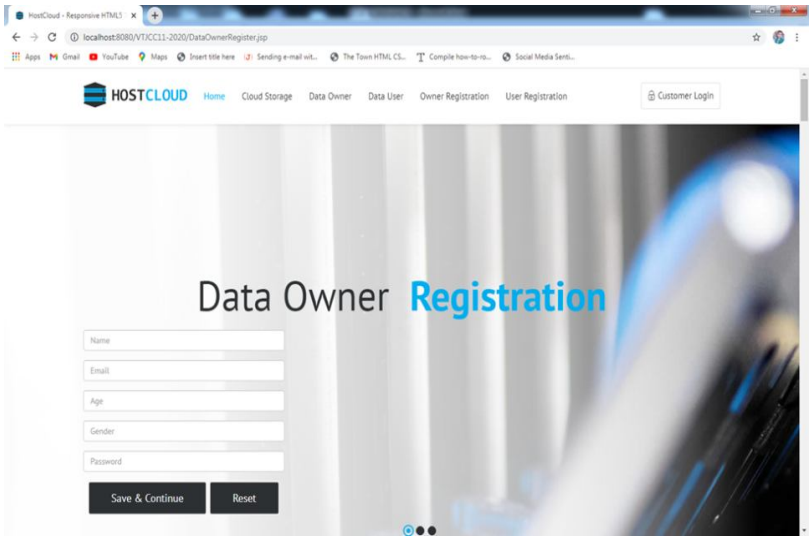


Fig.4.3.Data Owner Registration

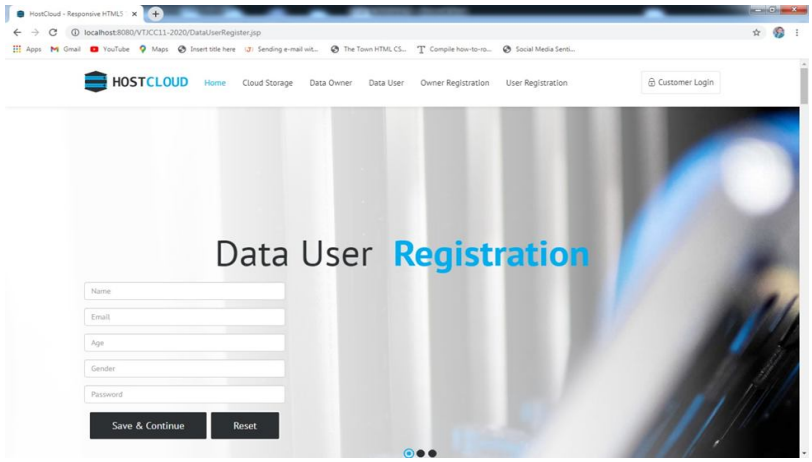


Fig.4.4.Data user registration page

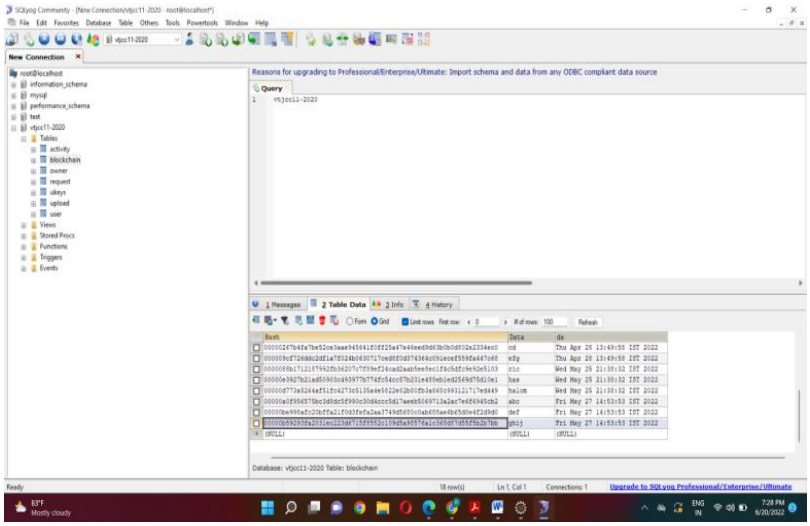


Fig.4.5.The stored hash values in the database

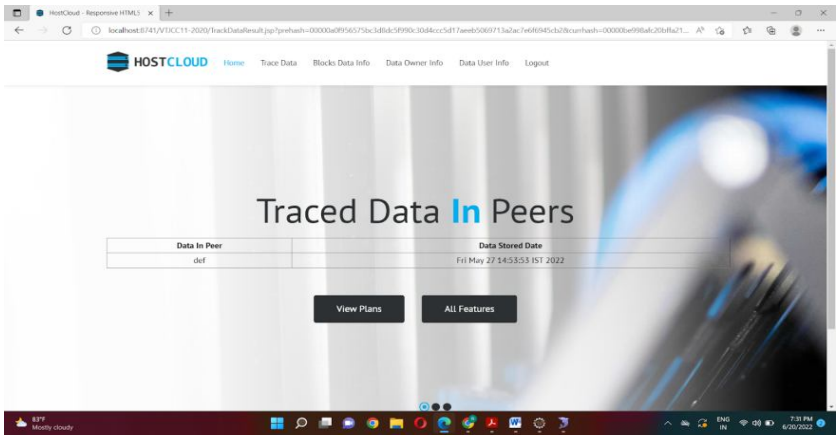


Fig.4.6.Traced data in peers

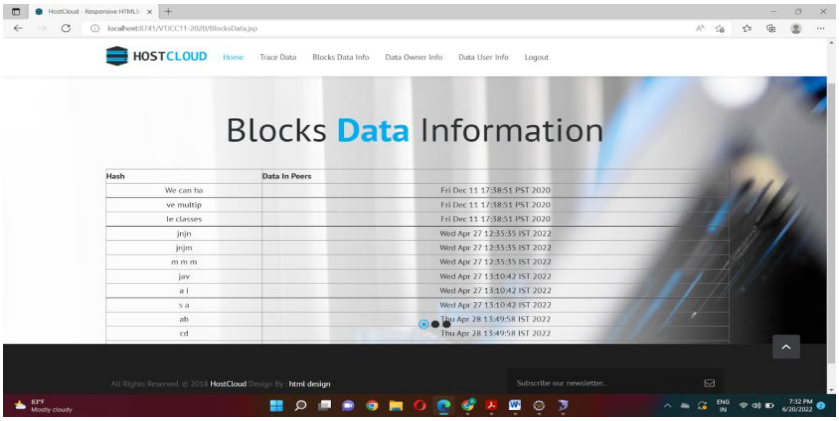


Fig.4.7.Blocks data information

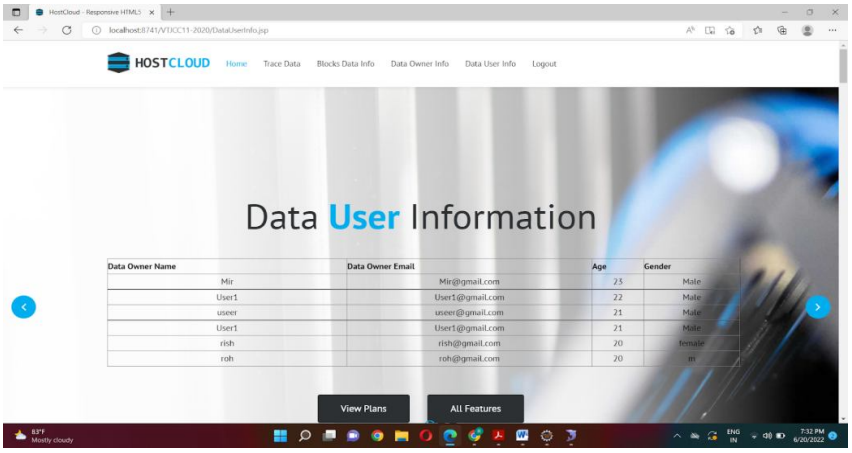


Fig.4.8.Data user information

V. CONCLUSIONS

By encrypting and sharing the data among several peers in the system, the suggested solution improves data security. The implemented system encrypts data using the AES 256 bit encryption technique to guarantee the privacy of the user's data. The network's peers then share and store the encrypted data. Our technology not only addresses the privacy and security issues associated with decentralised cloud storage, but it also offers a platform for peers to rent out their unused storage and earn cryptocurrency in return, maximising the use of available capacity. In the future, an adaptive scheduling mechanism can be included, allowing users to access files more frequently than those that are only used seldom.

This will make it easier for the user to access frequently used files whenever needed. Additionally, the addition of a credit system is possible. Under this system, each peer would receive a default 100 credits based on their system uptime, and for each successful file access request, their credits will either be added or subtracted. Higher priority for data storage will be given to peers with more credits.

REFERENCES

[1] Y. Hassanzadeh-Nazarabadi, A. Küpçü and O. Ozkasap, "Decentralized Utility- and Locality-Aware Replication for Heterogeneous DHT-Based P2P Cloud Storage Systems," in IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 5, pp. 1183-1193, 1 May 2020, doi: 10.1109/TPDS.2019.2960018.

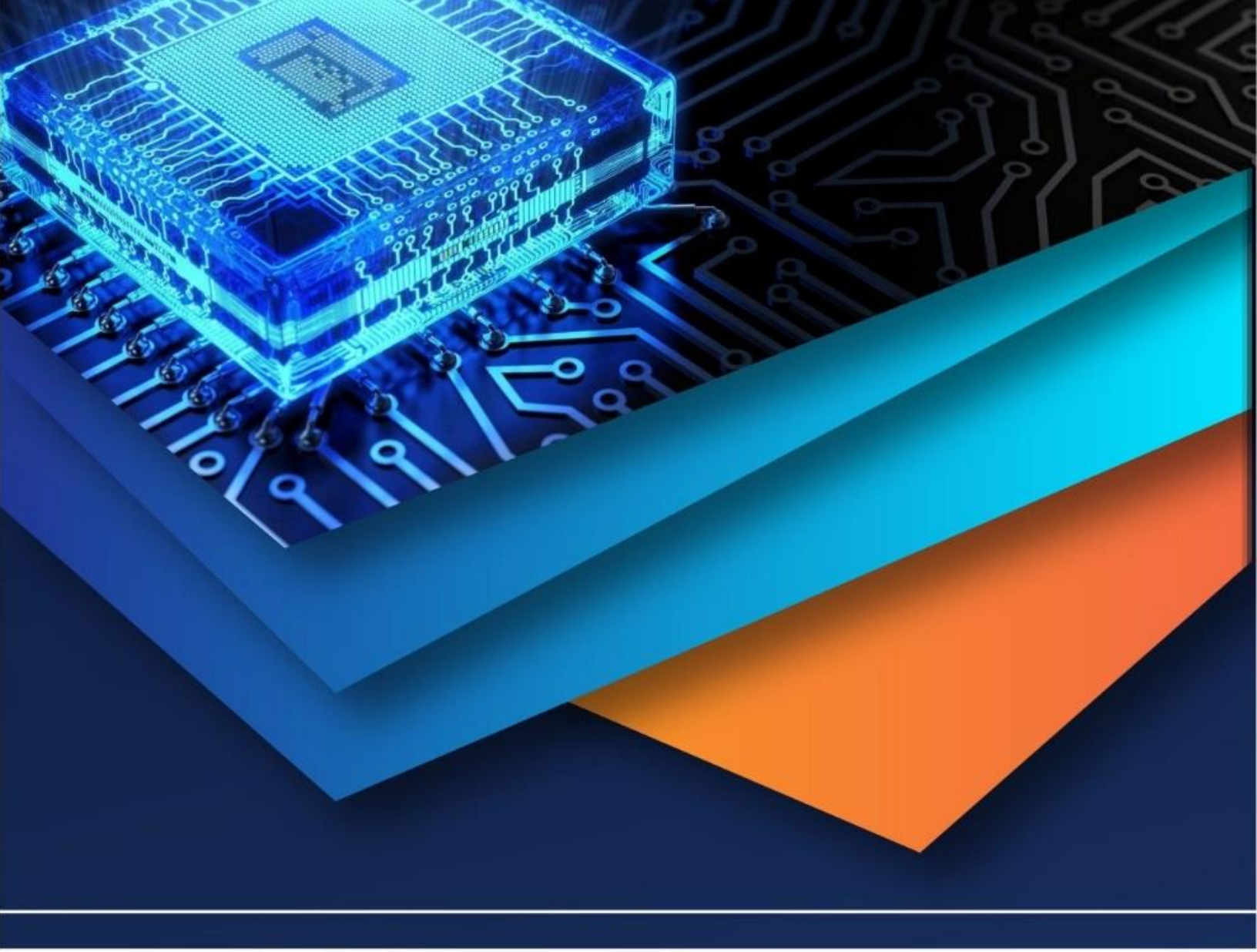
[2] M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri, "A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 4, pp. 778-788, 1 April 2019, doi: 10.1109/TPDS.2018.2870652.

[3] S. Ali, G. Wang, B. White and R. L. Cottrell, "A Blockchain-Based Decentralized Data Storage and Access Framework for PingER," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1303-1308, doi:10.1109/TrustCom/BigDataSE.2018.00179.

[4] Dong, Zhongli & Lee, Young-Choon & Zomaya, Albert. (2019). Proofware: Proof of Useful Work Blockchain Consensus Protocol for Decentralized Applications.

[5] Babitha M.P. and K. R. R. Babu, "Secure cloud storage using AES encryption," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 859-864, doi: 10.1109/ICACDOT.2016.7877709.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)