iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VIII Month of publication: August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46528

Blockchain Based Secured Document Storage for Cloud

Rushyanthan R
Student, Department of Computer Science and Engineering, Mount Zion College of Engineering and Technology, Pudukkottai

Abstract: Internet is the most common way used to share data around the globe. This sharing is backed by various cloud providers that allow customers to store & share data on the internet. But when it comes to privacy, cloud providers have consistently failed to make data 100% secure. Many data breaches, data piracy, hacking attacks have threatened the security mechanism of cloud providers. Though data stored by the customers should be 100% secure as it may contain private data which must be only accessible to the owner itself and some intended audience. So, it is very important to make this system more secure, so that data privacy & trust onto cloud providers can be maintained. We introduce a system that leverages the security of cloud-based data onto the blockchain. It allows users to store data onto the cloud and provides a prominent access control mechanism that will ensure the privacy of data. Users will be able to share data with other people in a permissioned manner by sharing the link for document with the intended user. Logs of all the operations performed with the document will be available to the owner at any instance of time. This will ensure the actual ownership & privacy of the data. Any person or third-party will not be able to access document without valid permission. This will make existing cloud storage more secure & decrease the data breaches & several attacks.

Keywords: Cloud Blockchain, Encrypted Sharing, block chain, secured environment, sharingdocs, Data Protection, Secured Data.

I. INTRODUCTION

Most organizations around the world create huge amounts of data through their day-to-day work. This data needs to be stored somewhere and should be easily accessible. This storage & easy access to huge data itself becomes a big problem for such organizations. Cloud as an emerging technology provides a solution to this problem by allowing such organizations to store data on cloud storage and it can be easily accessed through the internet. This also resulted in a vast shift of organizations from on-premises to cloud. With the adoption of cloud storage, organizations don't need to manage their data locally and also make this data available anytime anywhere through the internet as per the requirement of the user (public access/private access). Though this seems to be very efficient from the organization's perspective, there are various risks associated with cloud storage. Maintaining the security, integrity & confidentiality of this data should have the highest priority while opting for cloud storage. Large cloud providers don't guarantee the security of data being stored.

A. Block Chain Technology

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger. 'Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can't corrupt it.

Blockchain is combination of three leading technologies:

1) Cryptographic keys
2) A peer-to-peer network containing a shared ledger
3) A means of computing, to store the transactions and records of the network

Cryptography keys consist of two keys – Private key and public key. These keys help in performing successful transactions between two parties. Everyone has these two keys, which they use to produce a secure digital identity reference.

B. Dapps

Decentralized application requires a DApps to be open source, that is the application operates autonomously without a centralized entity in control of most the application's associated tokens. These DApps should also have a public, decentralized block chain that is used by the application to keep a cryptographic record of data, including historical transactions.

Although traditional DApps are typically open-source, DApps that are fully closed source and partially closed-source have emerged as the cryptocurrency industry develops. As of 2019, only 15.7% of DApps are fully open source compared to 25% of DApps being completely closed source, that is there are a smaller proportion of DApps with the code of the application and its smart contracts all completely available compared to the proportion of DApps without any disclosure of their code. DApps that are open-source, with the code of their smart contracts publicly available, generally have higher transaction volumes, indicating greater popularity in open-source DApps over closed-source DApps.

C. Cloud Storage

Cloud storage is a model of computer data storage in which the digital data is stored in logical pools, said to be on "the cloud". The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment secured, protected, and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a collocated cloud computing service, a web service application programming interface (API) or by applications that use the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

II. RELATED WORK

A. Maximilian Wöhrer, Uwe Zdun, " Smart contracts: Security patterns in the ethereum ecosystem and solidity", International Workshop on Blockchain Oriented Software Engineering (IWBOSE) ,IEEE, 2018.

Proposed a system has Smart contracts that build up on blockchain technologies are receiving great attention in new business applications and the scientific community, because they allow untrusted parties to manifest contract terms in program code and thus eliminate the need for a trusted third party. The creation process of writing well performing and secure contracts in Ethereum, which is today's most prominent smart contract platform, is a difficult task. Research on this topic has only recently started in industry and science. Based on an analysis of collected data with Grounded Theory techniques, we have elaborated several common security patterns, which we describe in detail on the basis of Solidity, the dominating programming language for Ethereum. The presented patterns describe solutions to typical security issues and can be applied by Solidity developers to mitigate typical attack scenarios.

B. Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat,Laurent Njilla, "ChainFS: Blockchain-Secured Cloud Storage", IEEE 11th International Conference on Cloud Computing

Proposed a system ChainFS, a middleware system that secures cloud storage services using a minimally trusted Blockchain. ChainFS hardens the cloud-storage security against forking attacks. The ChainFS middleware exposes a file-system interface to end users. Internally, ChainFS stores data files in the cloud and exports minimal and necessary functionalities to the Blockchain for key distribution and file operation logging. They implement the ChainFS system on Ethereum and S3FS and closely integrate it with FUSE clients and Amazon S3 cloud storage. We measure the system performance and demonstrate low overhead.

C. Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,"A systematic literature review of blockchain-based applications:Current status,classification and open issues" , Elsevier, 2018

Proposed this work provides a systematic literature review of blockchain-based applications across multiple domains. The aim is to investigate the current state of blockchain technology and its applications and to highlight how specific characteristics of this disruptive technology can revolutionise "business-as-usual" practices.

To this end, the theoretical underpinnings of numerous research papers published in high ranked scientific journals during the last decade, along with several reports from grey literature as a means of streamlining our assessment and capturing the continuously expanding blockchain domain, are included in this review. Based on a structured, systematic review and thematic content analysis of the discovered literature, we present a comprehensive classification of blockchain-enabled applications across diverse sectors such as supply chain, business, healthcare, IoT, privacy, and data management, and we establish key themes, trends and emerging areas for research.

We also point to the shortcomings identified in the relevant literature, particularly limitations the blockchain technology presents and how these limitations spawn across different sectors and industries. Building on these findings, we identify various research gaps and future exploratory directions that are anticipated to be of significant value both for academics and practitioners.

D. *Gowtham Saranya, A.Kousalya,"A comparative analysis of security algorithms using cryptographic techniques in cloud computing" , IEEE, 2017.*

Proposed a system as cloud computing which is describe different computing concepts which contains huge number of computers attached through a real-time communication like internet. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time.Computing is an emerging technology in today's business era. It allows convenient on demand access to resources that involve large number of computers connected through Internet. Public clouds vendors offer many resources such as application, storage, hardware, software's etc. The security issues present in public cloud is more challenging. As everything is accessed publically; many users have the threat to store and retrieve it publically. As many organizations are moving data to the cloud there is a need to protect data against unauthorized access. Hence it is necessary to study the security issues in public cloud to secure data. The purpose of this paper is to provide an overview of pubic cloud computing and the security issues involved .This paper deals with the different algorithms or method used for securing data in public cloud.

E. *Ilya Sukhodolskiy, Sergey Zapechnikov, "A Blockchain Based Access Control System for Cloud Storage," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.*

Proposed a system as to present a prototype of multi-user system for access control to datasets stored in an untrusted cloud environment. Cloud storage like any other untrusted environment needs the ability to secure share information. Our approach provides an access control over the data stored in the cloud without the provider participation. The main tool of access control mechanism is ciphertext-policy attribute-based encryption scheme with dynamic attributes. Using a blockchain-based decentralized ledger, our system provides immutable log of all meaningful security events, such as key generation, access policy assignment, change or revocation, access request.We propose a set of cryptographic protocols ensuring privacy of cryptographic operations requiring secret or private keys. Only ciphertexts of hash codes are transferred through the blockchain ledger. The prototype of our system is implemented using smart contracts and tested on Ethereum blockchain platform.

F. *Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare "Blockchain Based Secure Data Storage and Access Control System using Cloud" IEEE - ICCUBEA 2019.*

Proposed a system as cloud storage today depends entirely on large storage providers. Such storage providers function as untrusted third parties that process data for storing, sending and receiving data from an entity. This style of system has many problems, such as high operating costs, software quality and data security. They present a model of a multi-user access control system for databases that use blockchain technology to provide stable, distributed data processing. The system allows the data owner to upload the data via a web portal. So, the user who has the secret key to the particular data that has been uploaded to Cloud in encrypted form can only access the folder. Eventually, the system promotes data privacy by maintaining the immutability of the blockchain by processing it in the cloud. We have proposed a secure, blockchainbased data storage and access control system to increase the security of cloud storage.

III. EXISTING METHODOLOGIES

With the system proposed, we leverage the security of cloud-based data onto the blockchain. The results of the system promise to provide maximum security for the data stored on the cloud. The permission-based access control makes the system more reliable & trustable, in turn making the data more secure.

The results presented make it clear that the proposed system provides a better way to tackle above problems related to security of the data stored in the cloud. The logs accessible to the user ensure that every access operation to the data, let it be read or write or delete, are known to the actual owner of data. This preserves the integrity & intactness of the data. Also, it ensures that the permissioned user is only able to access the data.

The logs will be responsible to give this information to the owner of the data. The logs also detect the malicious access to data thereby informing the owner about the unauthorized access. In short, the system with its all features provides a solution to various problems associated with cloud data storage. Can fend against collusion attacks is an existing proposal.

Existing Systems	Proposed system
There are Many theories that have proposed the use of encrypted documents	There is no overhead of encryption and decryption
Cryptography is involved and it requires secure channel for sharing of various keys	There is no overhead of sharing keys as Cryptography is not Involved
There is no Involvement of Blockchain	The benefit of blockchain ledger, Consensus and its tamper proof nature is used for achieving more security
There are no logs generated and stored for every operation performed on each document	Here Logs are stored on Blockchain for every document and User can access these Logs stored on Blockchain
Cloud providers have sole right on document storage. He might perform unsecure operations on the document	As cloud database triggers are involved cloud provider has to take permission from user before doing any operation on document
The shared document links can be shared further to anyone, and User is unaware of who is using the link	If a document link is shared with anyone other than the trusted entity it will notify and request permission from the owner of the document
If User’s account is hacked, he will lose full control of his account	Here even if the account is hacked the owner of the document will be notified on his mobile before any unethical operation is performed on the document

A. Authentication And Login

User credentials are entered and verified in this module. As the first step of authentication, username of the user and passwords are collected via web forms and is validated via background process. Credentials are stored in safe place to avoid credentials leaks. Same credentials to be used for cloud login whenever required to view the data in the s3 bucket. Initially, the application requires users to be authenticated. The registration involves a simple form with email & password as login credentials.

On registering successfully, users can login with the credentials (email & password). If by chance a user forgets the password, then the application provides a facility to change the password, that is also in a secure manner by verifying email first. The password reset link can be accessed through registered mail only. Resetting of user credentials also to be enabled so that the user can reset whenever they forget his/her password.

B. Home Page

Once a user is logged in successfully, the initial page of our application is shown that has one button for uploading a new file, using which the user can upload the file to the cloud. Also, there is search box and view button available, with help of that user can access documents from other users by entering corresponding code of the file

C. Uploading Documents

As soon as the user selects a file, an alert is given and he has to confirm the notification whether he allows this operation or not. Also, he needs to confirm the transaction from meta mask. Meta mask is compulsory for this application as it accesses the blockchain. Once the transaction gets completed, the file is uploaded to the cloud. Finally, the log is stored on the blockchain for file creation.

D. Sharing Documents

By clicking on the view icon, the user can view/download the file, this also requires the same approval from the user which will also trigger meta mask transaction & the operation log details will be written to the blockchain. For sharing the document with other users or any other third-party, share button is available by clicking that it generates a code for file that can be shared with other users & file can be accessed using this code. Whereas, only allowed users can access the document as it will prompt for approval from the owner.

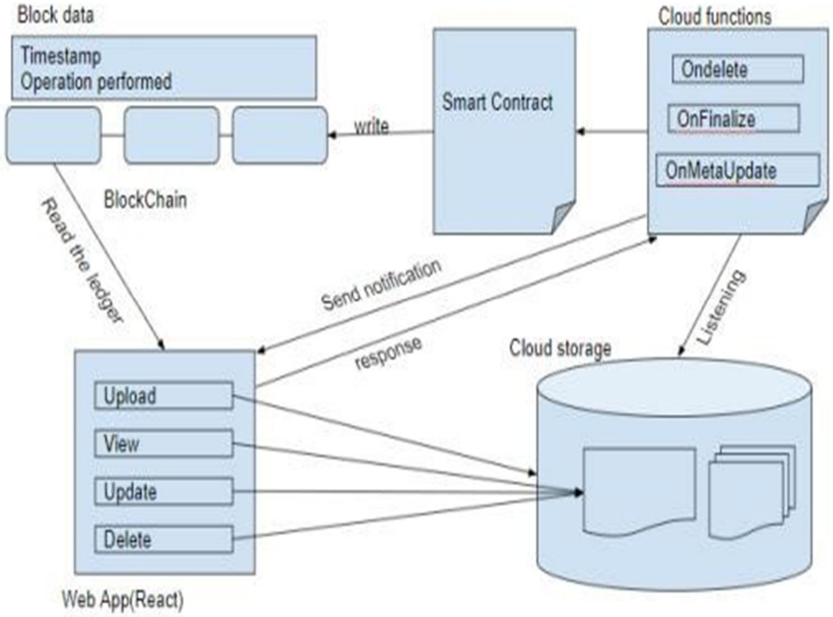


Fig 4.1: Architecture for Proposed Work

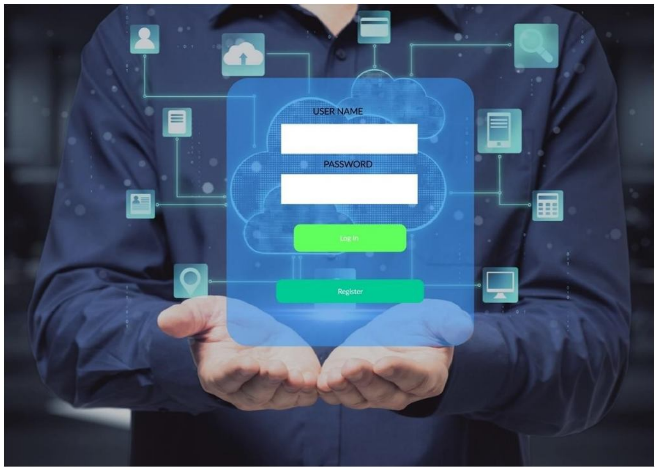
IV. EXPERIMENTAL RESULTS

We have implemented a functional prototype of the system & demonstrated its working concerning added security provided on top of cloud providers. In our System encryption, decryption, and generating the hash for uniquely identifying the documents in Blockchain is not necessary as documents are stored as it is with the mere addition of triggers and, we use User ID to uniquely identify the documents on the Blockchain.

Our system will save the time mentioned above for generating the links, encrypting, and decrypting the documents stored on the cloud. It will also save the memory space and energy required for encryption and decryption. It will allow users to refer to tamper-proof logs stored on Blockchain for all the operations and share the data securely using two-factor authentication in which the first step is sharing the link with the trusted entity.

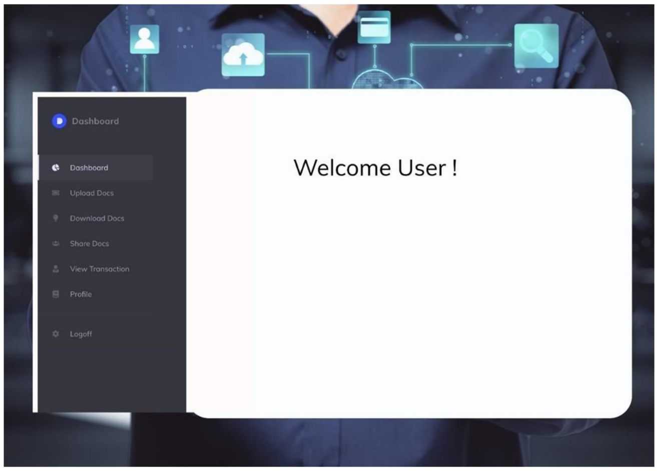
A. Storage Using Blockchain Explained

Login with authenticated user with valid credentials



B. User Login Success

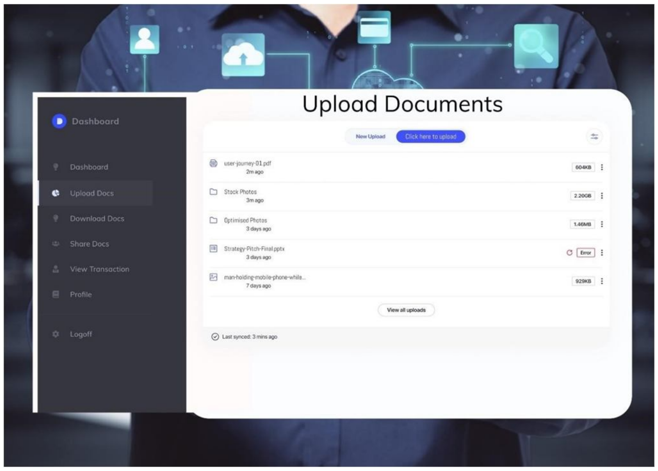
User success message is displayed in the screen with all the dashboard option available.



Welcome User !

C. Upload Documents

Uploading documents to be securely stored in the cloud.



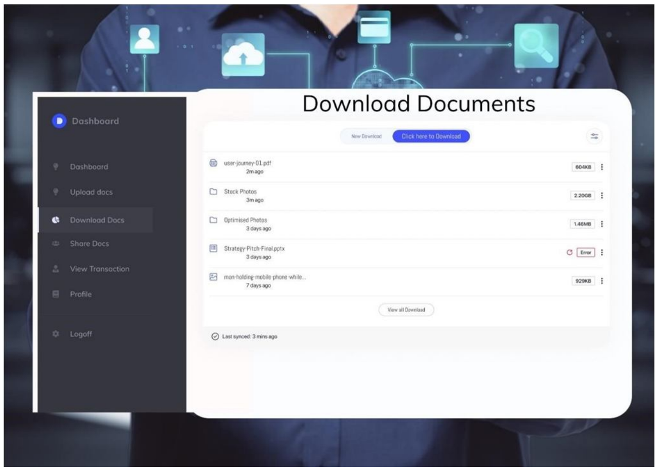
Upload Documents

user-journey-01.pdf 2m ago 604KB
Stock Photos 3m ago 2.20GB
Optimised Photos 3 days ago 1.46MB
Strategy-Pitch-Final.pptx 3 days ago Error
man-holding-mobile-phone-while... 7 days ago 929KB

Last synced: 3 mins ago

D. Download Documents

Downloading secured stored documents.



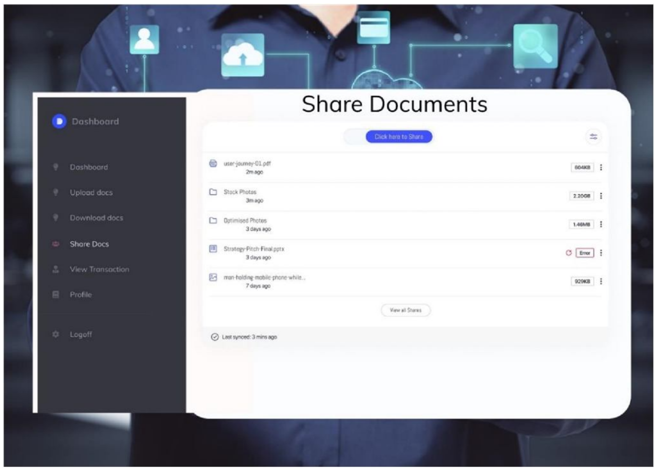
Download Documents

user-journey-01.pdf 2m ago 604KB
Stock Photos 3m ago 2.20GB
Optimised Photos 3 days ago 1.46MB
Strategy-Pitch-Final.pptx 3 days ago Error
man-holding-mobile-phone-while... 7 days ago 929KB

Last synced: 3 mins ago

E. Share Documents

Share documents across users to access



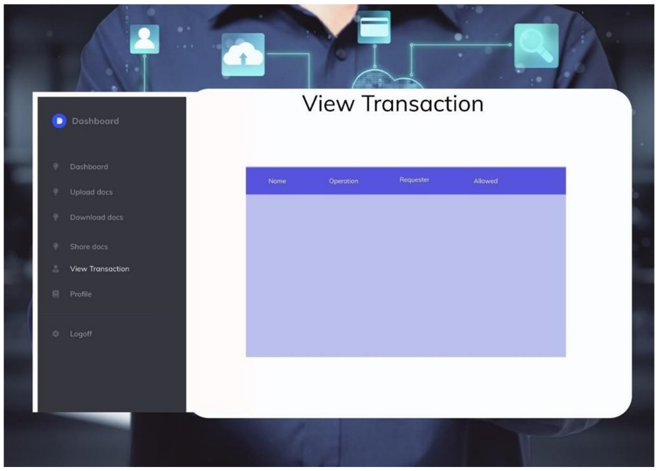
Share Documents

user-journey-01.pdf 2m ago	604KB	
Stock Photos 3m ago	2.20GB	
Optimised Photos 3 days ago	1.46MB	
Strategy-Pitch-Final.pptx 3 days ago	Error	
man-holding-mobile-phone-while... 7 days ago	929KB	

Last synced: 3 mins ago

F. View Transactions

To view all the transactions across data

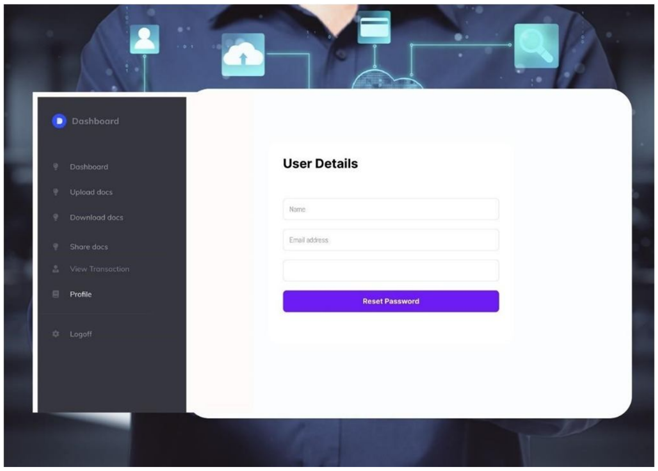


View Transaction

Name	Operation	Requester	Allowed

G. User Details

To have all the information about the users.



User Details

Name

Email address

V. CONCLUSION

Our system will save the time mentioned above for generating the links, encrypting, and decrypting the documents stored on the cloud. It will also save the memory space and energy required for encryption and decryption. It will allow users to refer to tamper-proof logs stored on Blockchain for all the operations and share the data securely using two-factor authentication in which the first step is sharing the link with the trusted entity.

And to prevent unauthorized access, the second is approving the notification for granting permission. This makes our system cheaper, secure and time efficient. In future, this policy can be applied to any organization which are using private or public cloud to store data more securely and to ensure security for the data. By assigning roles to users, data can be securely stored in the cloud without worrying about the data breach or security issues.

REFERENCES

[1] Maximilian Wöhrer, Uwe Zdun, “Smart contracts: Security patterns in the ethereum ecosystem and solidity”, International Workshop on Blockchain Oriented Software Engineering (IWBOSE) ,IEEE, 2018.

[2] Qiwu Zou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, “ChainFS: Blockchain-Secured Cloud Storage”, IEEE 11th International Conference on Cloud Computing (CLOUD), 2018.

[3] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,”A systematic literature review of blockchain-based applications:Current status,classification and open issues” , Elsevier, 2018

[4] R.Gowthami Saranya, A.Kousalya,”A comparative analysis of security algorithms using cryptographic techniques in cloud computing” ,IEEE,2017.

[5] Ilya Sukhodolskiy, Sergey Zapechnikov, “A Blockchain Based Access Control System for Cloud Storage,” IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.

[6] Shubham Desai, Rahul Shelke, Omkar Deshmukh, Harish Choudhary, Prof. S. S. Sambhare “Blockchain Based Secure Data Storage and Access Control System using Cloud” IEEE - ICCUBEA 2019.

[7] Gurudatt Kulkarni, Rani Waghmare, Rajnikant Palwe, Vidya Waykule, Hemant Bankar, Kundlik Koli, “Cloud Storage Architecture”, IEEE 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)Google Cloud Platform Documentation: https://cloud.google.com/docs AWS Documentation: https://docs.aws.amazon.com/

[8] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen,”A Survey on the Security of Blockchain Systems”,beijing university China, 2018.

[9] Rongzhi Wang, “Research on data security technology based on cloud storage”, 13th Global Congress on Manufacturing and Management, GCMM, 2016.

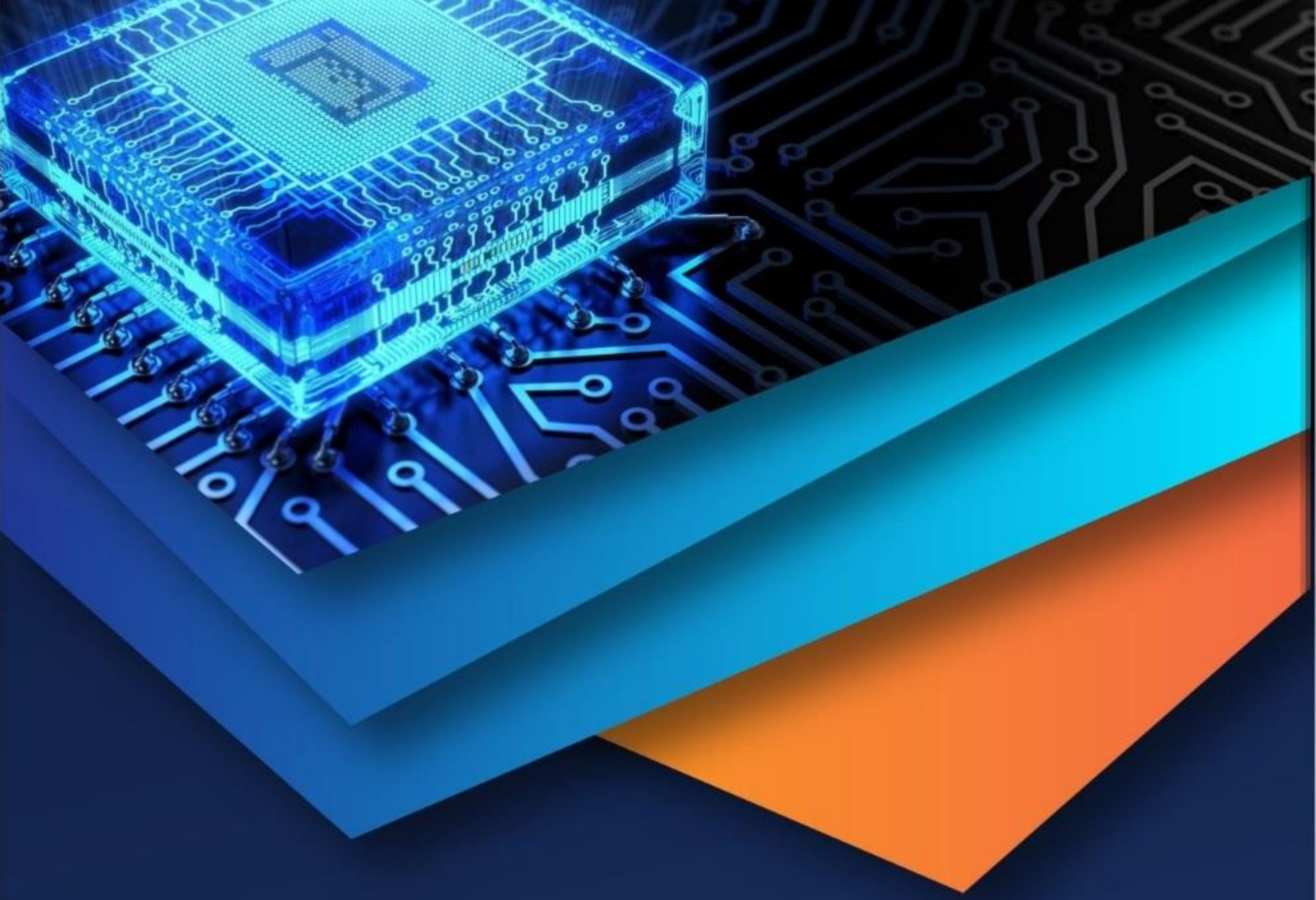
[10] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.

[11] Julija Golosova et.al. “The Advantages and Disadvantages of BlockchainTechnology”, IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.

[12] Mr Anup R. Nimje et.al. “Blockchain Attribute Based Encryption Techniques in Cloud Computing Security : An Overview ” IJCTT Volume 4 ,Issue 3-2013

[13] Sangsuree Vasupongayya -“Blockchain-Based AccessControl Model to Preserve Privacy for Personal Health Record Systems” , Research Article, 2019

[14] Naresh vurukonda, B.Thirumala Rao, -“A Study on Data Storage Security Issues in Cloud Computing”, 2nd International Conference on Intelligent Computing, Communication & Convergence , (ICCC-2016), 2018. [17] Guang Chen, Bing Xu1, Manli Lu1 and Nian-Shing Chen, -”Exploring blockchain technology and its potential applications”, [Elsevier] 2018



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY