International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3S, 2025
https://www.theaspd.com/ijes.php

A Secure Storage Management Technique for Cloud in Collaborative Environment

Ritu Mishra[1](Corresponding Author),**Dr.Sandip Kumar Goyal**[2] ,**Dr. Sanjeev Rana**[3]
[1]Research Scholar, Department of CSE,
Maharishi Markandeshwar Engg.
College(MMEC),Maharishi Markandeshwar (Deemed to beUniversity), MM(DU),Mullana, Ambala, Haryana, India. Email: ritu.mishra8168@gmail.com
[2]Department of CSE, Maharishi Markandeshwar Engg.
College(MMEC),Maharishi Markandeshwar(Deemed to be University), MM(DU), Mullana, Ambala,Haryana, India.
[3]Department of CSE, Maharishi Markandeshwar Engg.
College(MMEC),Maharishi Markandeshwar (Deemed to beUniversity), MM(DU), Mullana, Ambala, Haryana, India.

Abstract
Large capacity storage needed by any organization is now the only requirement for cloud storage suppliers. These storage organizations manage files data for sending, storing, and receiving it from a source, they are unreliable third-party entities. High operating costs, data security, and software quality are just a few of the many problems with this kind of system. This work illustrates Blockchain-enabled databases to offer consistent, dispersed Processing of data. The mechanism permits the possessor(owner) of the data to use an online interface to upload the data. And the user possessing the secret password for the specific info can only access info via the cloud in encrypted form. In due course, The system encourages the privacy of data by upholding the block chain's immutability through cloud computing. The Paper suggested a safe blockchain-based data retention system and a mechanism of controlling access to improve cloud storage security.

Keywords: smart contracts, blockchain,cloud storage,Cryptography, decryption.

1.INTRODUCTION

In the modern day, there has been a challenge of keeping enormous volumes of data for big businesses that operate worldwide. Consequently, numerous companies have shifted to cloud which offers exceptional storing ,uploading and distribution offerings. The principal issue that Utilizing cloud computing is protecting the privacy and data integrity in supporting data security. The majority of users favor storing their personal data on the cloud. But there aren't many data related security and copyright concerns. Cloud service suppliers do not guarantee the superior quality of protection necessary for proper information privacy and security. Currently limited resources and techniques accessible to protect cloud stored data. In order to address this issue, this study suggests the use of Blockchain as a reliable surroundings to improve Cloud-based storage security and to safeguard malicious assaults.
Blockchain is a decentralized, unchangeable system, an electronic ledger and each and every user of the blockchain network can only view certain kinds of transactions, which are acceptable to them.[1]
Blockchain technology allows all parties involved to compile all transaction data into a ledger, and to alter their ledgers to maintain validity in the event that a new transaction takes place. Ever with the development of the Web and thanks to cryptography technologies, everyone may now participants to verify the transaction's integrity and a one mistake caused by depending on an official third party is no longer in place.It is a type of decentralized ledger, utilized to build an unchangeable, long lasting database of transactional data. Every block consists of a header and a body. The header includes the value of hash both present and earlier blocks, along with the nonce.

The server retrieves the block information through the index procedure. The interconnected nature of each neighbor in the chain, which holds hash values shaped by the preceding blocks, makes it particularly difficult to alter or falsify the recorded information [2].

1.1 Benefits of Blockchain

The unchangeable nature of Blockchain is established when a transaction get associated with the Blockchain, altering or removing it, is not feasible. Additionally, it is dependent on the kind of system , if it is centralized, it can be changed or eliminated because just one person makes the decisions. However, in a distributed system such as Blockchain, each transaction is duplicated across every node within the network. Because of this benefit, Blockchain technology is unchangeable and unaffected. Through the transaction's copying step , the Block chain's transparency characteristic is achieved. Every transaction is reflected, as previously said, on one or more of the Blockchain network's devices.

1.2 Major Contribution

This paper's primary contributions are enumerated below:
a.) The location details of the file will exclusively be shown on the blockchain and will be saved in the cloud.
b.) Since the information on the blockchain is accessible to everyone, encrypted(Data) being transmitted to the cloud and retrieval is restricted. Users who are eager to view a file need to adhere to the retrieve policies to locate files stored in the cloud.
c.) To download a specific file from the document pool, its encryption must be broken using the hash key that was provided by the data holder.
d.)The efficiency of the suggested technique is increased by including the HASBE approach using fixed length ciphertext and key.

2.SMART CONTRACT

To establish, run and uphold the conditions of a Consent among parties with questionable reliability, smart contracts serve as executable code that operates on the blockchain.[2]Fundamentally, it functions autonomously. Upon the fulfillment of specified conditions, a primary goal of a smart contract is to automatically implement its stipulations. This results in lower transaction fees in contrast to traditional services that depend on a reliable third party to carry out the agreement. Ethereum stands out as the most widely used for smart contracts. [7]

3.RELATED WORKS

Jain, A. K., Jones, R., & Joshi, P. in the field of computing, unique values must constantly be created for a variety of uses. There are several approaches, the most popular of which depends on a specific moment in time. Cryptographic hashing functions Digital signatures, message authentication, checksum generation, digital fingerprinting, and password security in databases are just a few applications for cryptographic hashing algorithms. This work focuses on message authentication by reviewing and comparing several hashing algorithms using various criteria.
Alexopoulos et al. [2] survey Collaborative Intrusion Detection Systems (CIDSs) and blockchain technology. The authors argue that blockchain properties such as enhancing trust between monitors, providing accountability and consensus can be beneficial to CIDSs. They proposed a generic architecture for incorporating blockchain into the field of CIDSs.
In their thorough review of blockchain technology, Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang [3] first give an outline of blockchain Framework and then evaluate some common consensus algorithms utilized in various block chains. A brief description of current developments and technical difficulties is also provided. Jin Ho Park and Jong Hyuk Park [4] talk about blockchain technology and the current research trends surrounding it. Additionally, a detailed explanation of how blockchain security can be integrated with cloud computing and its secure solutions.

Blockchain technology is described and its benefits and drawbacks are examined by Julija Golosova and Andrejs Romanovs [5]. Numerous blockchain applications that had already been put into use were examined, along with the elements that contributed to implementation success or failure. Its goal is to examine the benefits and challenges associated with integrating and implementing blockchain technology across several modern industry domains.

To gather all of the knowledge that is pertinent to smart contracts from a technological standpoint, Maher Alharby and Aad van Moorsel [6] carry out a methodical mapping analysis. Finding current study topics and unresolved issues for next smart contract studies is the goal of this. 24 publications were taken from various scientific databases by the author. Codification, security, privacy, and performance issues are the four main concerns that are noted. Applications of smart contracts are the main topic of the remaining papers.

Prof. H. N., Prof. V. T. Gaikwad, and Mr. Anup R. Nimje. Datir [7] determined that HASBE emerged as the most effective access control mechanism following an analysis of seven distinct attribute-based encryption techniques. This strategy stands out for its effectiveness and flexibility, accompanied by a reduced calculation overhead compared to alternative methods. The HASBE scheme creates a structured hierarchy for application users through the CP-ASBE delegation technique. it facilitates efficient client revocation through its extensive value attributes and dynamic, dependable combinations of attribute sets.

Pooja More [8] proposed the implementation of the Key Aggregate Cryptosystem, which utilizes attributes, as a means to safeguard cloud data. This approach offers versatility through the use of two separate folders: one for the key and another for a collection of characteristics. Prior to undergoing processing and access control, anonymous data is subjected to encryption and subsequently stored on a blockchain. A client must be eligible for access and have the required key to unlock and decode a file before they may read it. The access control system's primary advantages are: The use of blockchain and smart contracts ensures that all transaction data is secure and private, that facts have access to files, that facts are rejected, that other stakeholders can change access policies without needing to take additional precautions to protect user keys, and that these data cannot be edited or modified.

A platform utilizing blockchain technology for user access to cloud storage was introduced by Sukhodolskiy and Zapechnikov [9]. This provides a model for retrieving data housed in unreliable circumstances, like cloud storage. The blockchain will provide access to the necessary information for file identification. Maximilian Wöhrer and Uwe Zdun [10] have identified six design patterns that address security concerns in the development of Solidity smart contract code.The sandbox execution environment of Ethereum addresses the challenge of maintaining control over execution upon contract deployment through these patterns. This special Ethereum feature has limitations even if it enables programs to operate autonomously on the blockchain. Unmanageable financial risks, unfavorable bounce-back scenarios, or unfavorable circumstances surrounding the handling of matters can all be examples of these disadvantages. These security flaws can be fixed by implementing the trends that have been noted, which may lessen the likelihood of traditional attack scenarios.

B. Thirumala Rao and Naresh Vurukonda [11], The study outlines problems with cloud data storage, including data theft, data breaches, and cloud data unavailability. Lastly, offering potential fixes for the corresponding cloud problems.

In order to construct HMAC utilizing SHA-2 hash algorithms, a novel system architecture is provided by H. Khali, MIEEE, R. Mehdi, and A. Araar [12]. This architecture uses a CODESIGN method to maximize speed, retaining the non-essential SHA-2 hash algorithm computations in software while implementing the important computations in hardware. Lastly, the suggested architecture is very adaptable and capable of effectively implementing keyed-hash message authentication codes and sophisticated digital signature algorithms. Aquino Commonly used encryption methods will be compared by Valentim Mota, Sami Azam, Bharanidharan Shanmugam, Kheng Cher Yeo, and Krishnan Kannoorpatti [13]. The time required for data encryption and decryption, security efficiency, memory utilization, power consumption, jitter, and latency will all be taken into consideration while making this comparison. It also concentrated on finding research on the various data

encryption methods and their widely utilized algorithms, comparing them based on similar factors. The best symmetric encryption algorithm in every category.

Abdelghani et al. [14] discussed the challenge of trust management in the Social Internet of Things (SIoT) paradigm. The author proposed a new trust model that can find and isolate suspected nodes for a reliable and resilient system. They introduced new characteristics to explain and evaluate the different conduct in the SIoT system.They provide experiments about the performance of their trust model.

Shen et al. [15] discussed the challenges of reliable and combined data sharing in multiple cloud platforms and proposed a collaboration model. The model uses blockchain technology and a smart contract to record data sharing and involves revenue distribution among the participants. The paper analyzes the topological relationships between the participants and developers. The proposed scheme is discussed in terms of its incentive effects and rationality of distribution rules.

Darwish et al. [16] presented a hybrid blockchain approach to address privacy and security challenges in cloud computing. By encrypting data and storing unique digital signatures on a decentralized blockchain, the algorithm enhances data integrity, reliability, and user privacy. Testing the framework in a virtual cloud environment demonstrates its effectiveness in preserving privacy, minimizing performance overhead, and ensuring the integrity of data. Despite the additional computational requirements, the given algorithm offers significant benefits in terms of privacy and data security for cloud storage systems.

Zhou et al. [17] proposed a blockchain-based approach called ALLSTAR to increase trust for equally merging Cloud with Edge resources to build a decentralized ecosystem.

Khashan et al. [18] proposed a hybrid architecture that combines centralized authentication provided by edge servers with decentralized authentication facilitated by a blockchain network. This approach aims to overcome the limitations of conventional authentication methods that may be resource- intensive or inapplicable for cross-domain authentication. Their architecture utilizes lightweight cryptographic techniques to achieve efficient authentication while ensuring the reliability and scalability of the given networks. The results demonstrate improvements measured by comparing computational expense, execution duration, and energy usage compared to blockchain-based and centralised authentication methods. The paper also provides a security analysis highlighting the architecture's ability to achieve requirements for IOT security.

Kumar, A. et al. [19] proposed a technique which is the combination of blockchain and cipher text, without the interference of third parties which is very useful in terms of cost and encryption-decryption time.

A prototype of distributed intrusion detection was proposed by the authors in [21] (DIDS). Their solution monitors a heterogeneous computer network by combining centralized analysis, distributed monitoring, and data reduction. A distributed intrusion detection system called DOMINO uses a design that encourages cooperation between heterogeneous nodes arranged in an overlay network. They employed active-sink nodes in their system to monitor and react to connections to unoccupied IP addresses. With the use of an active-sink node, attacks from spoofing IP sources may be detected more effectively, false positives can be decreased, attacks can be classified, and blacklists can be created quickly. Even though their system performed well, the integrity of the data that is stored could be jeopardized by hostile hackers who could corrupt the database used to oversee activities.

Message authentication code (MAC) was introduced by the authors in [20] as a way to identify any modifications made to stored data. This method can identify any changes in the data that is saved, but it is not suitable for big amounts of data because of the overwhelming and time-consuming nature of downloading and calculating the MAC of large files. By calculating the hash values of each piece of data in the cloud, another technique outlined in [20] protects the integrity of cloud data. Despite being simpler than the original approach in [20], this technique is impractical because of its higher computing power requirements, especially when handling huge volumes of data. The database's activities are managed by a third party, according to the designers of [22].

The author [23] provides thorough analysis of trust strategies in cloud systems. It highlights the unresolved issues and provides guidance for further study in this area.

The author [24] suggests a brand-new blockchain-based secure access framework (BSAF) for private cloud-device service partnerships. Two smart contracts are created: one for behavior punishment to audit users' access

behaviors and another for request verification to confirm users' access permissions. Extensive tests conducted on the Ethereum blockchain network demonstrate that the suggested BSAF framework performs better than current schemes in terms of cost and delay reduction, and is better suited for low-profile IoT devices.

To preserve confidentiality and anonymity, data is frequently kept on cloud servers as cipher text. To access encrypted data, a data user needs a third-party access key and intervention. However, a dishonest third party will compromise the security of the system. To solve this problem, a blockchain-based improved secure cloud storage access solution was introduced in [25]. By combining ciphertext-policy attribute-based encryption with a shortened attribute string and Ethereum blockchain technology, we are able to develop a revolutionary approach. The author[26] investigates how Ethereum blockchain technology, namely its PoW consensus mechanism and smart contracts, might be used as instruments to improve access control in multi-SDN settings.

Author [27] enhances security, privacy, and trust in AI systems using blockchain in cyber security. It also looks at future research for the potential uses and ramifications of this technology in the field.

4.PROPOSED SYSTEM

An online storage option that uses several servers spread across various places to securely store the data has been made possible by cloud storage. The use of cloud storage has expanded over the last several years in several industries, directly challenging the use of local storage. In the present period, cloud computing has become a potential paradigm for a number of third-party service providers. Data holders can save their information in the cloud and grant permission to the organizations who require it [9]. Despite the many advantages of cloud computing, there are always significant security problems as well.

The following are some security concerns associated with cloud storage:

a. Data privacy: Until users provide permission, no one wants their information to be accessible. The capacity of an individual or organization to keep themselves apart or to disclose parts of themselves only when necessary, is called privacy. Additionally, it enables users to control how their information is handled and stored in the cloud, protecting it from loss, improper usage, and illegal resale. If you store your information locally, this seems manageable enough, but when personal information is stored at someplace, it is difficult to identify its level of accessibility. If no web servers are maintained where information is housed, how do we find out that no one will ever be able to access it? Take caution since moving personal data to the cloud could mean giving up crucial privacy protections.

b. Lack of control: Having a third party store your data relieves you of a great deal of responsibility. However, there are two sides to this. Although someone else will handle the data, in one sense, you won't have to. If something corrupts your data, including ransomware attacks or power outages, this will immediately impact your ability to access your data. You are totally dependent on your provider to handle these problems. Your data grows more dangerous the longer it is left unsecured.

c. Data exposure: A significant portion of cloud data storage makes sure that no one from outside the company tries to access documents. Ensuring that no one outside the organization receives the information is the goal.The vulnerability of private data to other party sources renders data leakage a grave concern.

d. Breach of data: It occurs when an employee is careless or makes a mistake, whether by assault or otherwise. The primary cause for concern with cloud systems is that Information breaches can also be caused by insufficient safety practices or implementation vulnerabilities.

Workers can use their own laptops or work computers to log into cloud systems, opening the system up to malicious assault. It includes all types of information not intended for public disclosure, such as private medical records, financial records, proprietary and sensitive data, and so forth.

e. Vulnerabilities in the system: Using Cloud computing devices can exhibit framework weaknesses, especially within complex network infrastructures and when interacting with various third-party applications. An easily exploitable vulnerability can pose significant risks to organizations, particularly if it has been identified in a commonly utilized third-party system.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3S, 2025
https://www.theaspd.com/ijes.php

4.1 Overview of System

" **A secure storage management technique for Cloud by using blockchain**. " is a technique in order to address the security concerns that were previously mentioned. In this technique, the security of the Cloud data is enhanced by utilizing Blockchain technology. The information holder will first upload the files in an encrypted format over the cloud. The aggregate key that the information holder has provided can be used to decrypt these documents.

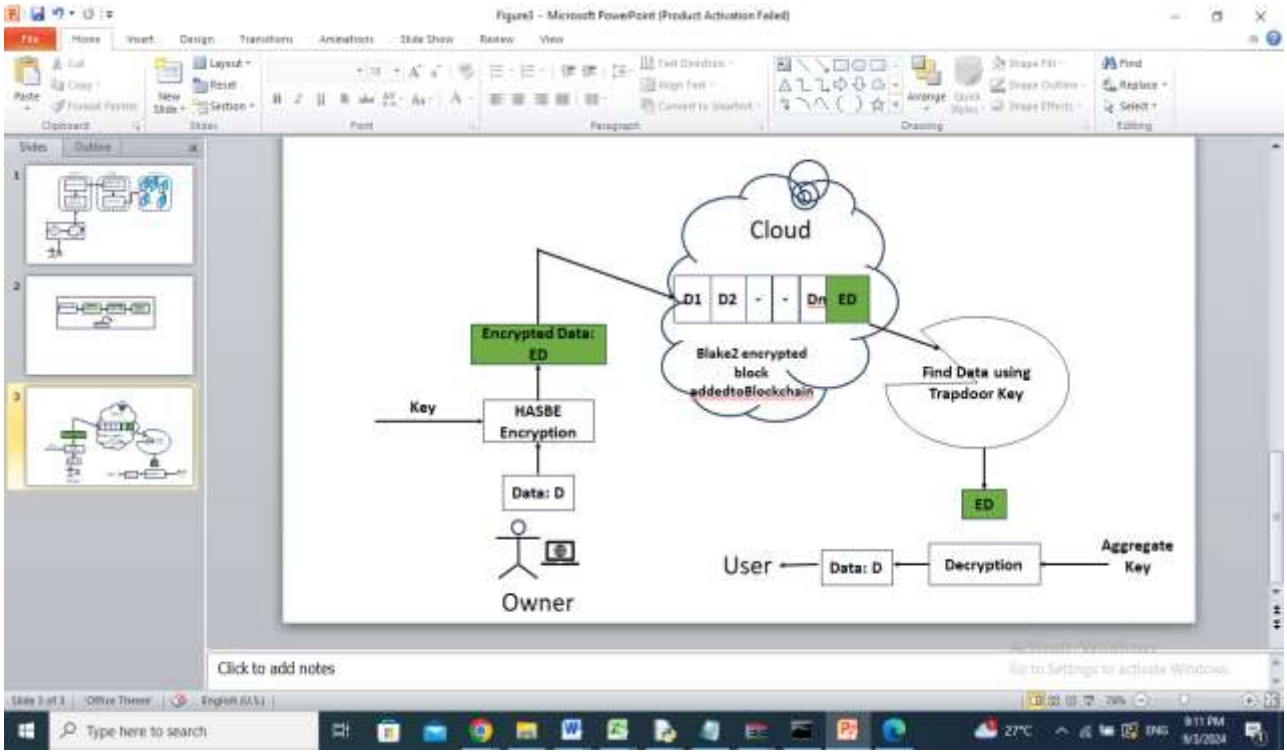


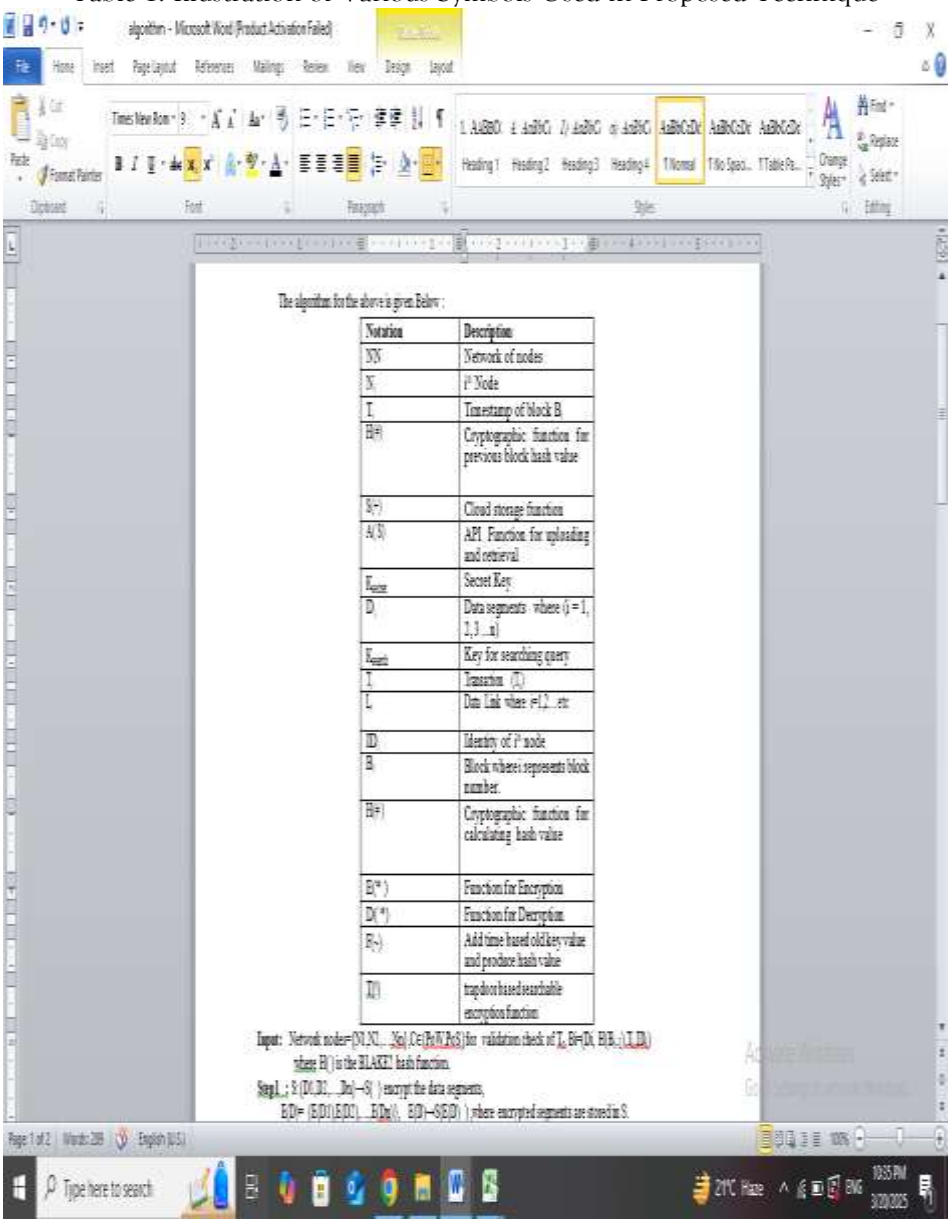
Figure 1. Data Storage and Retrieval Using Blockchain Technology

The user must first authenticate them in order to access files that are stored on the cloud. After verification, the user does a keyword search on the necessary file to find any number of documents. Only users who have been given permission by the data owner may access the public trapdoor key for each file, according to the information owner.

The user will seek access to the cloud stored data from the information owner if they are able to locate the desired file on the cloud. Upon receiving a request, the information owner provides the user requesting access to the data with the hashed keys. Now that the user has
access to the block chain's connection, the aggregate key used to decode the encrypted cloud data. You can download the specified file as a result. The offered system are illustrated in Table 1.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3S, 2025
https://www.theaspd.com/ijes.php

Table 1. Illustration of Various Symbols Used in Proposed Technique



The algorithm for the above is given Below :

Notation	Description
NN	Network of nodes
N_i	i^{th} Node
T_i	Timestamp of block B
H(#)	Cryptographic function for previous block hash value
S(+)	Cloud storage function
A(S)	API Function for uploading and retrieval
E_{secret}	Secret Key
D_i	Data segments where (i = 1, 2, 3 ...n)
K_{search}	Key for searching query
T_r	Transaction (T_r)
L	Data Link where e=1,2...etc
ID	Identity of i^{th} node
B	Block where: represents block number.
H(#)	Cryptographic function for calculating hash value
E(*)	Function for Encryption
D(*)	Function for Decryption
H(-)	Add time based old key value and produce hash value
T(.)	trapdoor based searchable encryption function

Input: Network nodes={N1,N2,... Nn} C∈{PoW,PoS} for validation check of T_r Bi=(Di, H(Bi-1),Ti, IDi)
where H( ) is the BLAKE2 hash function.

Step1 : S:{D1,D2,...,Dn}→S(+)
encrypt the data segments.
E(D)={E(D1),E(D2),...,E(Dn)},
E(D)→S(E(D)) ,where encrypted segments are stored in S.

The algorithm for the above is given Below :

Input: Network nodes NN= $\{N_1,N_2,...,N_n\}$, C∈{PoW,PoS}for validation check of T_r ,
Bi=(Di, $H(B_{i-1})$,T_i, ID_i)
where H(#) is the BLAKE2 hash function.

Step1 : S:$\{D_1,D_2,...,D_n\}\rightarrow S(+)$
encrypt the data segments.
$E(D)=\{E(D_1),E(D_2),...,E(D_n)\}$,
$E(D)\rightarrow S(E(D))$,where encrypted segments are stored in S. A(S) uploaded the data segments after verifying S.

Step2 : Encrypt the data using secret key

$E(D, K_{secret})=E_{HASBE}(D, S_{ecret})$

where K_{Secret} is the secret key and apply T(!) trapdoor based searchable encryption function T(Query, K_{search})

Step3 : Compute $H(L_i)$ for B_i(BLAKE2(L_i))

And store

$B_i=(E(D_i),H(L_i),H(Bi-1),T_i, ID_i)$

Step4 : Apply $T(Query,K_{search})\Rightarrow L_i \in S$

to retrieve encrypted data.

Step5 : Check $D_i=E^{-}1(E(D_i),Ksecret)$;

//Decryption and re-encryption

If ($H(D_i)=?H(B_i)$) **Then**

" integrity verified" ; **Else**

"Integrity Not Varified";

Endif

Step6 : $K_{new}=F(K_{old},t)$

where t is the regular time interval for rotation of encryption keys.

where F(˜) add time based value to old key and hashed it .so new key is created on regular t interval.

Step7 : apply Audit(Storage) → audits for security on storage system to detect vulnerabilities.

Apply Monitor(N) → Networking Monitoring for security breaches and anomalies.

Figure 2. Show the flowchart of proposed technique

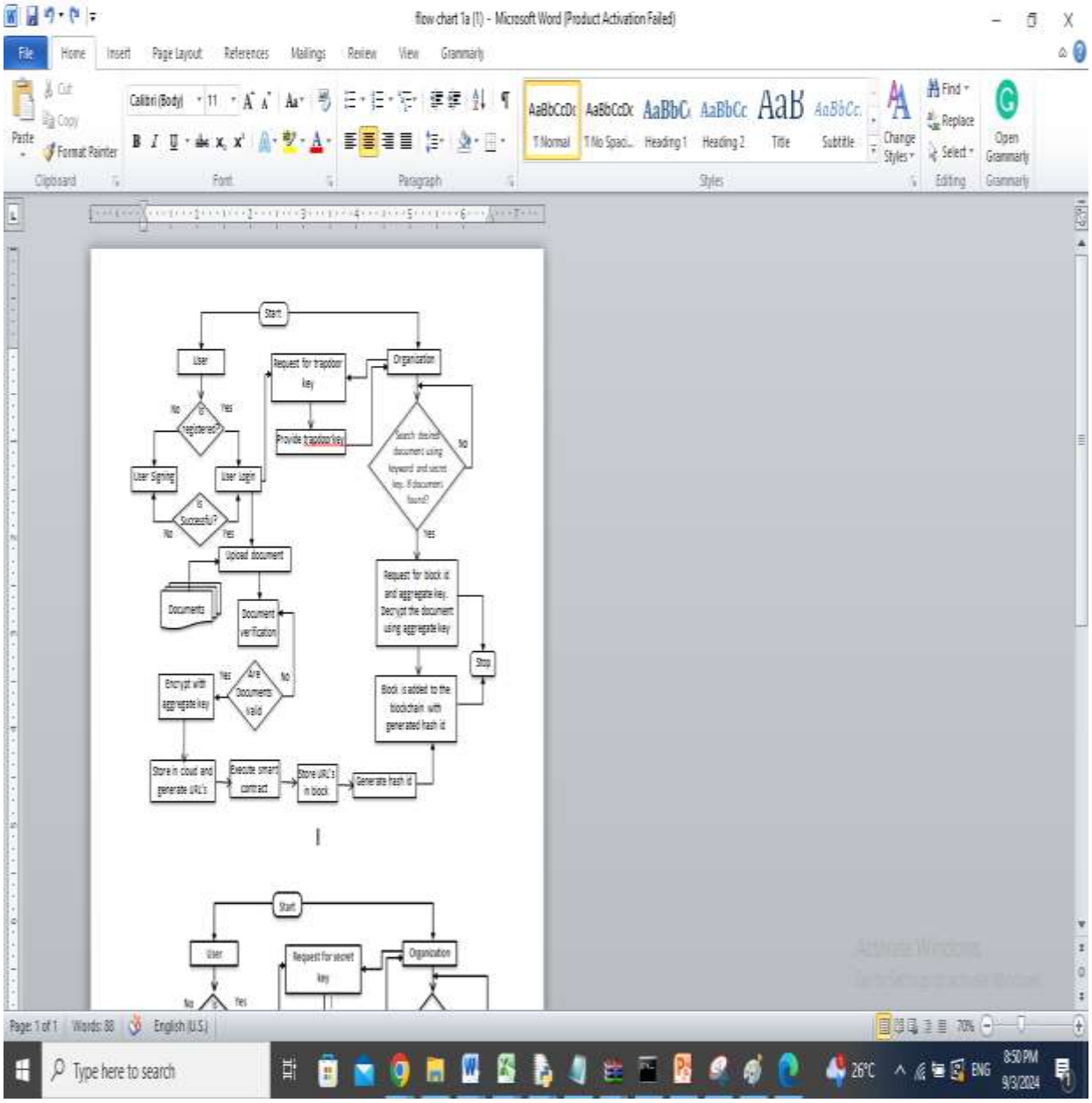


Figure 2. The proposed system's flow chart

5.Analysis

Any brief message may be converted into a tiny, static value using the hash function, which is often represented by the letter H. Represented as H(M), this serves as a verification code. Refer to Figure 3.The hash function is an one-way cryptosystem, password view, shows that it is only intended for encryption and makes decryption impracticable.

Since the H is a property of the message fragments, any changes to any of the bits will also affect the hash value, allowing for error detection capabilities. In the fields of data security and cryptography, the hash function is a vital instrument.

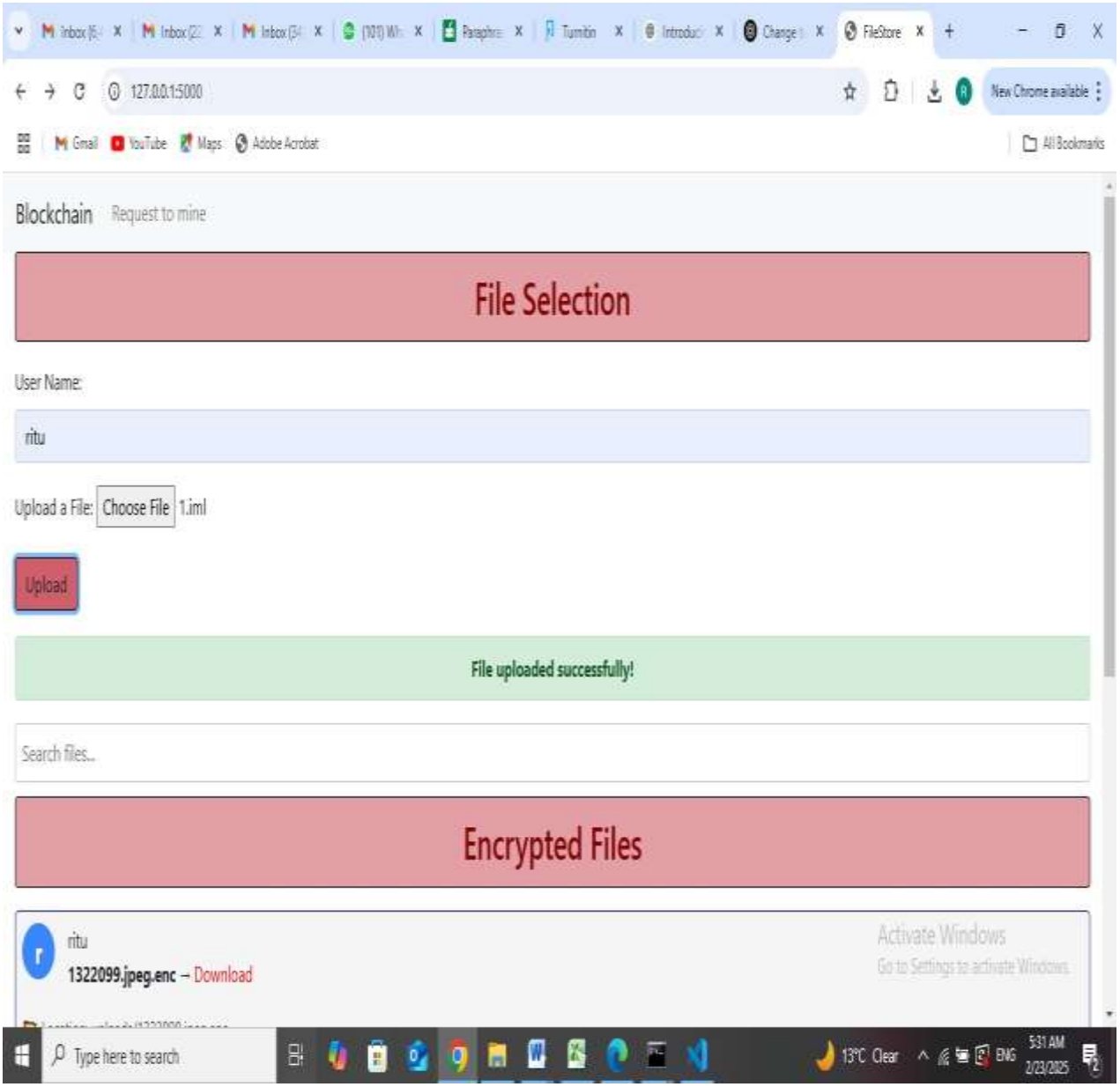


Figure 3. Selection of file

Fig. 4 represents the searching for retrieval of a file. When the user wants some specific file. The involvement of network members in saving and validating the blockchain imposes constraints that prevent unilateral exploitation. The blockchain functions as a sequentially organized form that maintains information same as in a communal ledger

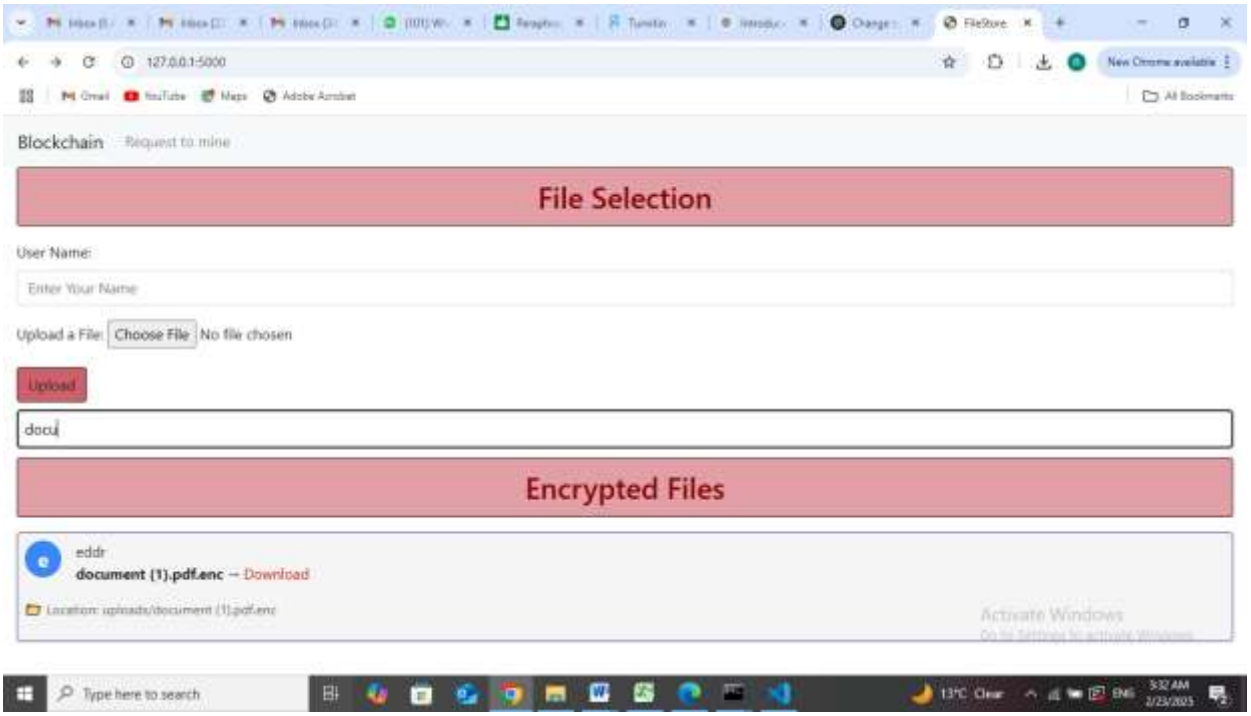


Fig 4. Shows the searching of file

The uploaded encrypted file is shown by Figure 5. Since all members have access to all transactions, all activity is visible to all other members of the Blockchain, making it transparent. [3]

Figure 5. Shows the encrypted uploaded file

The hash function that is most frequently employed can be categorized into the following :

The cryptographic hashing technique known as **BLAKE** was created by Raphael C.-W, Willi Meier, Luca Henzen, and Jean-Philippe Aumasson [1]. Phan .Even though BLAKE was not as SHA-3 , it is still a very strong

algorithm that has been enhanced, even further with BLAKE2 higher performance as a result of things like cutting the number of compression rounds from 16 to 12 for BLAKE2b and from 14 to 10 for BLAKE2s, as well as cutting the amount of initialization words from 24 to 8 are some enhancements of BLAKE2 over the original BLAKE. The random-access memory demand of the BLAKE2 method is as much as 33% less than that of the original BLAKE algorithm because of the fewer rounds. Tree hashing is implemented by BLAKE2 for incremental updates or file verification. In general, BLAKE2 is easier to build and computationally faster than BLAKE since it uses less padding for messages. Similar to the real BLAKE procedure, there are two primary variations of the BLAKE2 hashing algorithm based on alternate word sizes: the 32-bit variant, which yields 256-bit hashes, and the 64-bit variant, which yields 512-bit hashes. In contrast to BALKE2b, which is geared for 64-bit architectures, BLAKE2s is designed for tiny architectures. Additionally, by utilizing multiple cores and SMID, there BLAKE2sp and BLAKE2bp, which are up to eight and four times faster, respectively are versions of the BLAKE2 algorithms. While offering security similar to SHA-3, such as up to 256-bit collision resistance, immunity to length extension, in differentiability from a random oracle, etc. BLAKE2 is frequently much quicker than MD5 on 64-bit platforms.[1]

SHA-256: This cryptographic hash algorithm has applications in digital certificates and data integrity.it generates a 256-bit reference digest.SHA256 is utilized for password encryption since it eliminates the need for a hash key on the server side, only the hashed value corresponding to a specific user is necessary. This is advantageous since, in the situation when a server compromises, the hacker would only gain access to the H(M) rather than the actual password.

MD-5: It is capable of identifying any length value as input and generating a digest having fixed length that can be utilized to confirm the authenticity of the actual information. It produces a 128-bit "text digest" or "fingerprint" derived from the random-length message that acted as the source. It is generally accepted that generating two messages that yield the same message digest, or any other message that aligns with a specified target message digest, is computationally unfeasible. This system is meticulously crafted for application in digital signature frameworks, where substantial documents require secure "compression" prior to validation through public key cryptography and secret keys.

Comparing different hashing algorithms:[1][11]

Figure 6 demonstrates how the encryption times of MD5, SHA256, and Blake2 varies for different source sizes. When the source size is 10 MB, SHA256 encryption takes about five times as long as MD5 encryption and more time than Blake2 encryption.

a. **Time to Encrypt Data:**

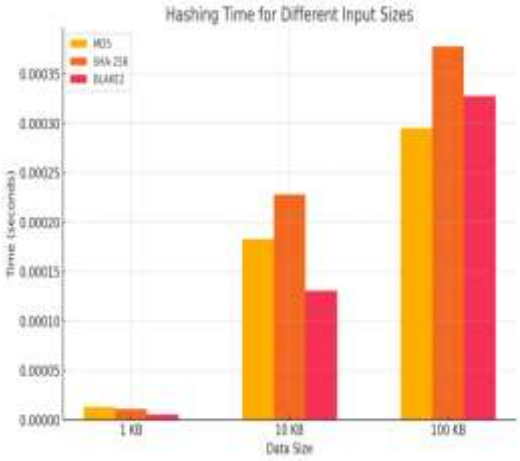


Figure 6. Time spent using a hashing technique to encrypt various input sizes

Figure.7. MD5, Blake2, and SHA256 latency comparison. It is clear that MD5 takes the longest, followed by Blake2 and SHA-256[1].

b. **Latency Comparison:**

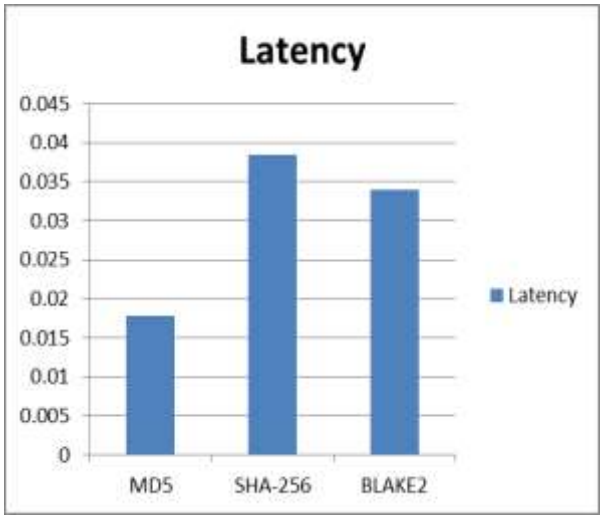
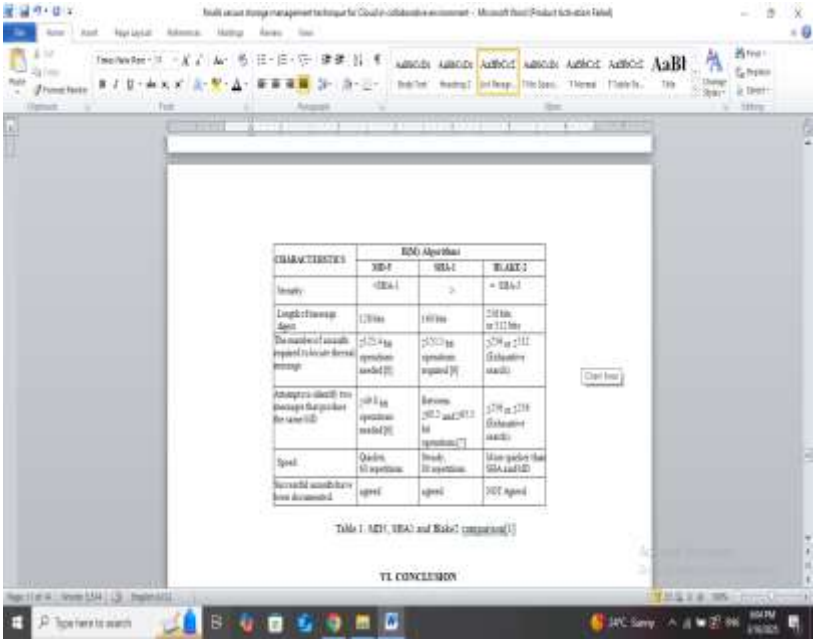


Figure 7. Latency comparison between MD5, Blake2 and SHA 256 .

5.1 Hashing Algorithms – Comparison

Table 2. provides a thorough analysis of the two most widely used hashing algorithms now in use (SHA-1 and MD-5) as well as a compelling alternative for hashing needs, BLAKE2. This will aid in understanding of these hashing algorithms and their characteristics.

Table 2. comparison between various hashing techniques



6.Conclusion

The recommended approach suggests a secure storage mechanism for cloud based on blockchain technology. A few security techniques with acceptable temporal Efficiency, usefulness, and complexity were selected in order to execute the system. The location will only be displayed on the blockchain and will be saved in the cloud. In order to find files stored in the cloud, users who are eager to examine a document must adhere to the retrieve regulations and have the required authorization key and search query. The aggregate key supplied by the information holder must be utilized to download the document when it has been decrypted from the document pool. As a result, it is observed that the recommended method provides a better approach than traditional cloud storage technologies.

REFERENCES

[1] Jain, A. K., Jones, R., & Joshi, P. Survey of cryptographic hashing algorithms for message signing. IJCST, Volume 8, Issue 2, 18-22,(2017).
[2] Alexopoulos, N., Vasilomanolakis, E., Ivánkó, N. R., & Mühlhäuser, M. (2018). Towards Blockchain-based collaborative intrusion detection Systems. In Critical Information Infrastructures Security: 12th International Conference, CRITIS 2017, Lucca, Italy, October 8-13, 2017, Revised Selected Papers 12 (pp. 107-118). Springer International Publishing,https://doi.org/ 10.1007/978-3-319-99843-5_10.
[3] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE International Conference on Big Data (Bigdata Congress), 2017,https://doi.org/10.1109/BigDataCongress.2017.85.
[4] Jin Ho Park and Jong Hyuk Park, Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) 01811, Korea, 18 August 2017. https://doi.org/10.3390/sym9080164
[5] Julija Golosova, Andrejs Romanovs, The Advantages and Disadvantages of the Blockchain Technology, IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018. https://doi.org/10.1109/AIEEE.2018.8592253
[6] Maher Alharby and Aad van Moorsel, Blockchain-Based Smart Contracts: A Systematic Mapping Study, Fourth International Conference on Computer Science and Information Technology (CSIT), 2017. https://doi.org/10.5121/csit.2017.71011
[7] Mr. Anup R. Nimje, Prof. V. T. Gaikwad, Prof. H. N. Datir, Blockchain Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview, International Journal of Computer Trends and Technology, Volume 4, Issue 3- 2013.
[8] Pooja More, Cloud data security using attribute-based key-aggregate cryptosystem, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, https://doi.org/10.1109/WiSPNET.2016.7566253
[9] 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,(pp 157-160), https://doi.org/10.1109/EIConRus.2018.8317400.
[10] Maximilian Wöhrer, Uwe Zdun, Smart Contracts: Security patterns in the ethereum ecosystem and solidity, International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018 pp(1-6)
[11] Naresh vurukonda, B.Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, 2nd International Conference on Intelligent Computing, Communication & Convergence, 2016 ,pp(128-135), https://doi.org/10.1016/j.procs.2016.07.347.
[12] H. Khali, MIEEE, R. Mehdi, A. Araar, A System-Level architecture For Hash Message Authentication Code, 12th IEEE International Conference on Electronics Circuits and Systems, 2005, pp.(1-4), https://doi.org/10.1109/ICECS.2005.4633372.
[13] Aquino Valentim Mota, Sami Azam, Bharanidharan Shanmugam, Kheng Cher Yeo, Krishnan Kannoorpatti, Comparative Analysis of Different Techniques of Encryption for Secured Data

Transmission, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017,pp.(1-6).

[14] W. Abdelghani, C. A. Zayani, I. Amous, F. S`edes, Trust evaluation model for attack detection in social internet of things, in: Risks and Security of Internet and Systems: 13th International Conference, CRiSIS 2018, Arcachon, France, October 16–18, 2018, Revised Selected Papers13, Springer, 2019, pp. 48–64,doi: https://doi.org/10.1007/978-3-030-12143-3_5.

[15] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, M. Guizani, Blockchain- based Incentives for secure and collaborative data sharing in Multiple Clouds, IEEE Journal on Selected Areas in Communications 38 (6)(2020)1229–1241,https://doi.org/10.1109/JSAC.2020.2986619.

[16] M. A. Darwish, E. Yafi, M. A. Al Ghamdi, A. Almasri , Decentralizing privacy implementation at cloud storage using blockchain-based hybrid Algorithm, Arabian Journal for Science and Engineering 45 (2020) 3369–3378,https://doi.org/10.1007/s13369-020-04394-w.

[17] H. Zhou, Z. Shi, X. Ouyang, Z. Zhao, Building a blockchain-based decentralized ecosystem for cloud and edge Computing: an all-star approach and empirical Study, Peer-to-Peer Networking and Applications 14(6)(2021)3578–3594,https://doi.org/10.1007/s12083-021-01198-z.

[18] O. A. Khashan, N. M. Khafajah, Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IOT Systems, Journal of King Saud University-Computer and Information Sciences 35 (2) (2023) 726–739 https://doi.org/10.1016/j.jksuci.2023.01.011.

[19] Kumar, A., & Verma, G. (2023, December). Secure cloud storage access framework using Blockchain Technology. In 2023 11th International Conference on Intelligent Systems and Embedded Design (ISED) (pp. 1-5). IEEE ,https://doi.org/10.1109/ISED59382.2023.10444539.

[20] Alkadi, O.,Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A Deep blockchain framework enabled collaborative intrusion detection for protecting IOT and Cloud Networks. IEEE Internet of Things Journal, 8(12), 9463-9472.

[21] Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An Integrated architecture for maintaining security in cloud computing based On Blockchain. IEEE Access, 9,pp. 69513-69526 , https://doi.org/10.1109/ACCESS.2021.3077838.

[22] Qu, G., Cui, N., Wu, H., Li, R., & Ding, Y. M. (2021). Chainfl: A Simulation Platform for joint federated learning and blockchain in edge/cloud computing Environments. IEEE Transactions on Industrial Informatics,pp.(1234-1245).

[23] Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain based trust management in Cloud Computing Systems: A taxonomy, review and future directions. Journal of Cloud Computing, 10(1), pp.(1-34),https://doi.org/10.1186/s13677-021-00247-5

[24] Duan, L., Xu, W., Ni, W., & Wang, W. (2023). BSAF: A Blockchain based secure access framework with privacy protection for cloud-device service Collaborations. Journal of Systems Architecture, 140, 102897, https://doi.org/10.1016/j.sysarc.2023.102897.

[25] Kumar, A., & Verma, G. (2023, December). Secure cloud storage access framework using blockchain technology. In 2023 11th International Conference on Intelligent Systems and Embedded Design (ISED) (pp. 1-5). IEEE,https://doi.org/10.1109/ISED59382.2023.10444539.

[26] Ohri, P., Daniel, A., Neogi, S. G., & Muttoo, S. K. (2024). Blockchain based security framework for mitigating network attacks in multi-SDN controller Environment. International Journal of Information Technology, 1-13,https://doi.org/10.1007/s41870-024-01933-8.

[27] Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in Cyber Security: A comprehensive Review. Blockchain: Research and Applications,10019 ,https://doi.org/10.1016/j.bcra.2024.100193.