IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006427 |

An Approach for Secure Data Sharing in Cloud Using Blockchain

Ms Nikita Shimpi [1], Prof. Sushma Ghose [2]

P.G. Student, Department of Computer Engineering, SCOE, Pune, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, SCOE, Pune, Maharashtra, India[2]

ABSTRACT: Nowadays, secure information sharing access control has ended up being one of the genuine stresses in distributed storage framework. Progressively advanced innovation in the present helped various people lives. Block chain is an innovation that enables moving computerized coins or assets from one individual to other person. Block chain thought can be comprehend with connected rundown in DS, since its next key location are secured in past key and they are connected with each other. In this paper, we propose the Secure Data Sharing in Clouds approach that gives: 1) information uprightness and privacy; 2) get to control; 3) information sending (sharing); and 4) insider danger security. The Secure Data Sharing procedure uses Block-chain Technology to access, move and offer information archives safely. The Secure Data Sharing framework is material to conventional and adaptable appropriated processing circumstances. We realize a working model of the Secure Data Sharing method by utilizing Block chain innovation and survey its execution subject to the time consumed during various assignments. The results wound up being empowering and exhibit that Secure Data Sharing can be satisfactorily used for secure information partaking in the cloud.

KEYWORDS: Block-chain technology, Cloud Computing, Cryptography, Security.

I. INTRODUCTION

The structure of another network architecture including a reasonable security mechanism means to decrease the storage, transmission, and cost of computation however much as could be expected while ensuring the confidentiality, integrity, authenticity of the message [1]. The Financial Times (2016) characterizes Block-chain as a "network of computers, all of which must favor a transaction has occurred before it is recorded, in a 'chain' of computer code". The subtleties of the exchange are recorded on an open ledger that anybody on the network can see [2]. It can possibly alter the computerized world by empowering a circulated agreement where every single online transaction, over a wide span of time, including advanced resources can be confirmed whenever later on. It does this without bargaining the security of the advanced resources and gatherings included. The conveyed accord and namelessness are two critical attributes of blockchain innovation [3]. Decentralized framework is one of the principal attributes of coalition k chain innovation because of its premise is the peer-to-peer network. The principle favorable circumstances of decentralized frameworks incorporate fault tolerance and extensible. With regards to financial establishments, the block-chain innovation has the huge effect to the computerized world from a conveyed agreement where the confirmation of each online transaction is conceivable whenever without trading off the security of the advanced resources and gatherings included [4]. So as to play out a dispersed accord, the blockchain innovation utilizes a communicate mechanism as message transmission. Anyway the communicate mechanism can acquaint pointless messages and information with the framework, which impacts high message overhead. This issue has propelled an idea to apply scourge protocols to perform disseminated agreement to blockchain. Pestilence protocols are bio-motivated correspondence and computation protocols dependent on unicast mechanism plan to circulate data and register information conglomeration in large-scale networked frameworks [5, 6].

A block-chain framework can be considered as a basically ethical cryptographic DB where basic medicinal data could be recorded. The framework is kept up by a network of computers that is available to anybody running the software. Block-chain works as a pseudo-mysterious framework that has still security issue since all transactions are presented to people in general, despite the fact that it is carefully designed in the feeling of information integrity [7, 8]. The entrance control of heterogeneous patients' social insurance records over numerous wellbeing foundations and gadgets should have been cautiously structured. Blockchain itself isn't planned as the vast scale storage framework. In the setting medicinal services, a decentralized storage arrangement would significantly supplement the shortcoming of blockchain in the point of view [8]. The target of this paper is to investigate how to safeguard the protected record

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006427 |

share framework in a Cloud storage server for the more drawn out timeframe utilizing Blockchain methods. The paper features significance of information document safeguarding and what the advantages are of cloud investigation and Blockchain. Further area examine the upside of Blockchain and how it is utilized in the proposed architecture pursued by general exchange and end.

II. RELATED WORK

Lou, Junjun, et al. Proposes, a key management model on NDN test-bed for check of the Data packet to be invulnerable to dispersing harmed content. In any case, by and by, this model postures two difficulties for confirming phony substance: (1) the incorporated architecture effectively prompts a solitary purpose of disappointment, particularly when the root key falls flat, its hard to check the keys crosswise over destinations because of the absence of trust among them, and (2) exorbitant overhead of authentication chain traversal while confirming mark. This paper initially proposes a blockchain based key management conspire in NDN to address the issue of absence of shared trust between locales without trust grapples. In particular, all site hubs shape a permissioned blockchain for storing open key hashes to guarantee the authenticity, and the intermediary door takes an interest in confirming to decrease unnecessarily visit correspondence between the switch and the blockchain. Furthermore, the NDN open key substance object and the plan of their storage, confirmation, and denial are overhauled. The aftereffect of our investigation and assessment demonstrates that the proposed plan is fit for supporting less confirmation numbers and higher check proficiency [1].

Ahram, Tareq, et al. Shows, a push to break the ground for exhibiting and exhibiting the utilization of Blockchain innovation in numerous mechanical applications. A human services industry application, Healthchain, is formalized and created on the establishment of Blockchain utilizing IBM Blockchain activity. The ideas are transferable to a wide scope of ventures as fund, government and assembling where security, adaptability and effectiveness must meet [2].

Underwood, Sarah. Proposes, that the blockchain builds up an arrangement of making an appropriated accord I n the advanced online world. This enables taking an interest elements to know for sure that an advanced occasion occurred by making an obvious record in an open ledger. I t opens the entryway for building up an equitable open and adaptable advanced economy from an incorporated one. There are huge open doors in this troublesome innovation and insurgency in this space has quite recently started. This white paper portrays blockchain innovation and some convincing explicit applications in both financial and non financial sector. We then take a gander at the difficulties ahead and business openings in this major innovation that is good to go to change our computerized world [3].

Kumar, Manish, Ashish Kumar Singh, and TV Suresh Kumar.Portrays, a protected log storage utilizing Blockchain on Cloud stage. We are living in the period of data innovation. Our everyday life is intensely reliant on it and subsequently it's sheltered and secure working turn out to be extremely significant and imperative. Consistently, there are a huge number of digital assaults occurring the world over. Assailants are persistently developing refined and stealthy systems to focus on the person in question. They takes all the careful steps to evacuate assault follows, for example, framework logs and related data on the injured individual frameworks with the goal that they can't be followed back. Assailants purposefully spread their exercises over longer timeframe to sidestep recognition. To comprehend and recognize such complex assault, it is required to keep up a safe log records over broadened timespan. In any case, safeguarding the log records for longer time is testing issue. The framework ought to likewise guarantee the integrity of log records and logging process. So as to conquer these issues, in this paper we are proposing a protected log storage utilizing Blockchain on Cloud stage. Blockchain innovation will make sealed review logs. It gives proof of log control and nonrepudiation. Cloud stage makes the general framework adaptable and bolster for profound investigation [4].

Poonpakdee, Pasu, et al. Shows, Smart contract frameworks through improvements of mechanical advancements are progressively observed as elective advances to affect transactional forms fundamentally. Blockchain is a savvy contract protocol with trust offering the potential for making new transaction stages and in this manner demonstrates an extreme difference in the present basic belief creation in outsiders. These outcomes in gigantic cost and time investment funds and the diminished hazard for the gatherings. This examination proposed a strategy to enhance the proficiency of dispersed accord in blockchains utilizing scourge calculation. The outcomes demonstrated that plague protocols can appropriate the data like blockchain [5].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006427 |

III. PROPOSED ALGORITHM

A. *System Architecture*

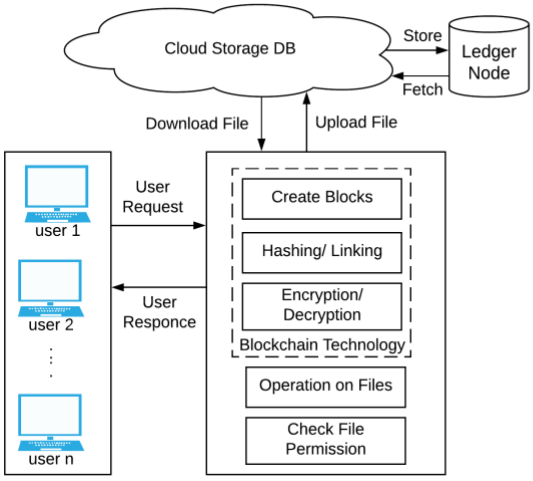

Fig 1 : Proposed System Architecture

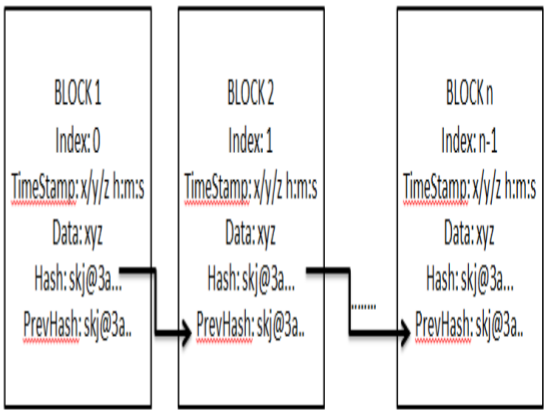

Fig 2 : Structure of Block chain

B. *Description of the Proposed Algorithm:*

The overall architecture of the cloud based Multi User Secure File Sharing System using Block-chain is shown in Fig. 1. There are three major functional components in the system.

1. User Data Operation Module

In this Module there are various operations are covered which consist of File upload, File Download, File Share, File Access, File Prevent Access, Update and Delete File. This module responsible for actual application processing on which user interaction is happens.

2. Block-chain Data Security Module

This is a Module used by application internally as a function. In this module mainly Block-chain technology covered. Which consist of Block Generation, Cryptography like encryption and decryption, hashing and linking, etc. It is the main module for proposed approach for security purpose. Figure 2 shows the structure of Blocks and show their linking methodology.

3. Cloud Data Storage and ledger Log Module

This Module is responsible for data storage in cloud and creation of ledger for info of data storage and their metadata. In our case we are using Mysql for database to store files and data.

IV. PSEUDO CODE

Algorithm 1: SHA-512 hashing Algorithm.

Input: a pointer to the hash string (8 * 64bit long words), a pointer to the message whose byte length is a multiple of 128.

Output: The hash string holding the SHA-512 digest of the message.

Prototype:

void SHA-512_128byte_blocks(uint64_t hash[8], uint8_t msg[256], intbyte_length)

Flow:

SHA-512Init(hash)

last_block = zero_string

last_block[byte 0] = 0x80

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006427 |

```
last_block[qword 15] = big_endian(byte_length*8) append(msg, last_block)
for i=0 to byte_length/128
        SHA-512 Update(hash, msg)
        msg = msg+128
end for
```

Algorithm 2: Block-Chain Algorithm.

Input: User Uploaded Data File

Output: Chain of Blocks of original Data File

Flow:

Step 1: File splits into multiple data blocks of 512 bit

Step 2: GenerateChainBlock(index, timestamp, blockData, prevHash)

Step 3: is blockValid (newBlock, oldBlock)

Where, check whether "preHash" of current Block matches to "Hash" of previous block for validity purpose. Return false;

Step 4: if (CalculatedHash(newBlock) == newBlockHash)

Return true;

else

return false;

Step 5: GenerateChain(add NewBlock)

Step 6: Continues process step 2, 3, 4, 5 till last chained Block.

V. Simulation Results

Table 1 shows Current system evaluation outcome, In table there is a time analysis is there for different size files for uploading as well as downloading process. We create record and analysis for file size of 25KB, 50KB, 75KB, 100KB and 200KB.

Approach	No. of files with encrypted index(File Size in Kb)	Times in Seconds(File Upload Time)	Times in Seconds(File Download Time)
Proposed system with File Data Encrypted and decrypted store cloud	25	55	65
	50	95	115
	75	125	155
	100	170	200
	200	356	275

Table 1: Current system evaluation outcome

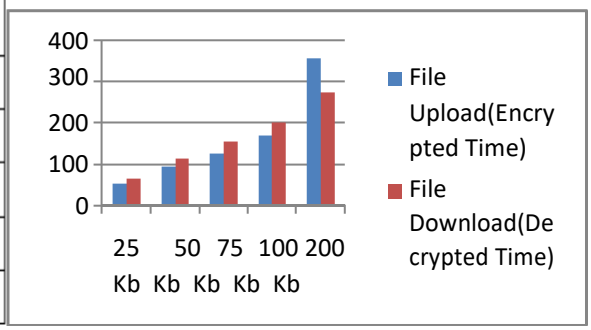

Fig.3. Current system evaluation outcome.

Figure 3 shows Current system evaluation outcome in graphical view, in below figure 3 there is a time analysis is there for different size files for uploading as well as downloading process. We create record and analysis for file size of 25KB, 50KB, 75KB, 100KB and 200KB as per table 1 values.

VI. Conclusion and Future Work

We implement a working prototype of the Secure Data Sharing methodology by using block-chain technology and evaluate its performance based on the time consumed during various operations. The results proved to be encouraging and show that Secure Data Sharing has the potential to be effectively used for secure data sharing in the cloud. It gives highest accuracy rate than other technology as well it promises the high security to share, upload, and access file data.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006427 |

We will combine explicit applications, (for example, video playback) to manufacture frameworks and direct deliberate audits, including computing, stockpiling overhead, proficiency of key conveyance, and so on to actualize our key administration plot. We will likewise investigate progressively proficient trust credential look-up mode and public key hash synchronization to accomplish quicker verification and key signing.

REFERENCES

1. Lou, Junjun, et al. "A Blockchain-based key Management Scheme for Named Data Networking." 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018.
2. Ahram, Tareq, et al. "Blockchain technology innovations." Technology & Engineering Management Conference (TEMSCON), 2017 IEEE. IEEE, 2017.
3. Underwood, Sarah. "Blockchain beyond bitcoin." Communications of the ACM 59.11 (2016): 15-17.
4. Kumar, Manish, Ashish Kumar Singh, and TV Suresh Kumar. "Secure Log Storage Using Blockchain and Cloud Infrastructure." 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2018.
5. Poonpakdee, Pasu, et al. "Applying Epidemic Algorithm for Financial Service Based on Blockchain Technology." 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST). IEEE, 2018
6. Gupta A, Patel J, Gupta M, Gupta H., (2017), Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, Vol. 7, No. 1
7. Navya A., Roopini R., SaiNiranjan A. S. et. Al, Electronic voting machine based on Blockchain technology and Aadhar verification, International Journal of Advance Research, Ideas and Innovations in Technology, (Volume 4, Issue 2)
8. Paul TakShing Liu. Medical record system using blockchain, big data and tokenization. In International Conference on Information and Communications Security, pages 254261. Springer, 2016.
9. Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, pages 110. IEEE, 2013.
10. Xu, Qian, et al. "Secure Multi-Authority Data Access Control Scheme in Cloud Storage System based on Attribute-Based Signcryption." IEEE Access (2018).
11. Vidya, K., and A. Abinaya. "Secure data access control for multi-authority Quantum based cloud storage." Computing and Communications Technologies (ICCCT), 2015 International Conference on. IEEE, 2015.
12. Riad, Khaled. "Revocation basis and proofs access control for cloud storage multi-authority systems." Artificial Intelligence and Pattern Recognition (AIPR), International Conference on. IEEE, 2016.
13. Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.
14. Seccombe A.., Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, 25 p.
15. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details