IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Framework for Secure Banking Data Storage and Retrieval in Decentralized Cloud Environment Using Blockchain

Mr. Shriram Bhanudasrao Khadke [1]

Student

Department of Computer Science &Engineering

Deogiri Institute of Engineering &Management Studies, Aurangabad

E-mail: ramkhadke@yahoo.com

Prof. Pravin B. Mahadik.[2]

Project Guide

Department of Computer Science &Engineering

Deogiri Institute of Engineering &Management Studies, Aurangabad

E-mail: pravinmahadik@dietms.org

Abstract: **Nowadays, large amount of data is stored on cloud storage which is required to be protected from the unauthorized users. To maintain the privacy of data various algorithms are used to protect data so that data can be providing confidentiality, integrity, accessibility. However, the existing of centralized cloud storage lacks to provide these properties. So, to enhance the framework for data storing technique decentralized cloud storage is used and with the help of blockchain technology it is effectively helps to protect data from tampering or deleting a part of data. For any kind of data blockchain stores it in number of blocks which are linked in continuous order through hash value in order to reduce the chances of data altering. For this purpose, SHA-256 algorithm is use for secure banking framework to implement the blockchain technology, because it works on hashing function when data is given to its input. Hashing algorithm used in many aspects where security of data is required such as message digest, and consensus and mining algorithm is use for even in custom blockchain. By the combination of these methods makes data more secure and reliable to user who access data which is store on cloud storage. However, with the help of various algorithms we enhance the security of data by encryption. In this paper (AES) Advance Encryption Standard is used to encrypt and decrypt the data due to significant features of this algorithm.**

Keywords: Distributed System, user data privacy, SHA-256 Algorithm, Hashing Functions, Consensus Algorithm, Custom Blockchain, etc.

I. INTRODUCTION

A blockchain system may be considered as a simply incorruptible cryptographic database where vital and confidential user's information will be recorded. The system is maintained by a network of computers, which is accessible to anyone running the software.

Blockchain operates as a pseudo-anonymous system that has nonetheless privacy problem in view that all transactions are exposed to the general public, even though it is tamper-proof inside the sense of data-integrity. The access control to manage heterogeneous user's confidential records across a couple of MNC establishments and devices had to be cautiously designed. Blockchain itself isn't designed as a massive-scale storage system. Within the context of framework for secure banking, a decentralized storage solution would significantly complement the weak point of blockchain within the perspective. The blockchain network as a decentralized system is extra resilient in that there is no single-point assault or failure compared to centralized systems. However, because all the bitcoin transactions are public and everyone has got right of entry to, there already exists analytics equipment that picks out the members within the community based totally on the transaction records [2].

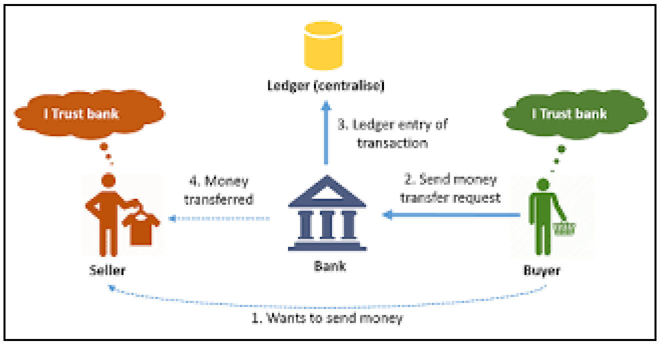

Fig.1: System Overview

In this research work fig.1 shows the system overview, and the most important module is blockchain implementation comprises two kinds of records: blocks and transactions. In every block contains a timestamp and a link to a preceding block is supplied via the secure hash algorithm. During the storage, the transaction information into the blockchain system executes various algorithms like SHA for hash generation, mining for generating a valid hash, smart contract for system policy, and consensus for validating current blockchain on all Peer to Peer nodes. Therefore, banking application is more secure. Second thing is that data storage and accessibility. For this point use the Secret Shamir hashing technique and keyword as well as content-based cryptography techniques.

II. RELATED WORK

In traditional storage where all data is store in only one place called centralized storage, the chances of data security are less as compared to decentralized storage due to the owner of centralized storage could monitor the data and it can be altered or theft. With the quick requirement to access data, each individual wants to retrieve their data instantly and more securely for this reason decentralized storage is developed. In decentralized storage data is stored in more than one data block; this itself reduces the chances of data reaching the data stealers. Because data stealers unaware of where the rest of the data is stored, due to this reason decentralized storage is popular and used widely.

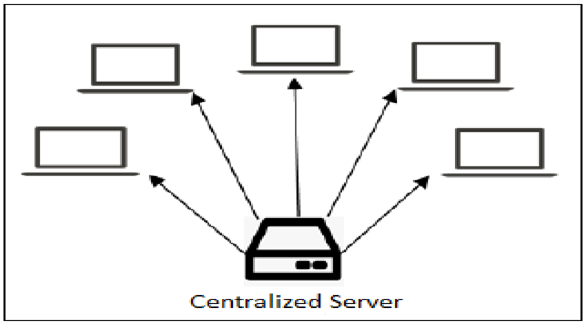

Fig.2: Traditional Centralized Storage

As shown in Fig.2 all data user who wants to access their data is dependent on only one server. Due to this bottleneck can arises and results in a longer time needed to access data because of high load on single point server.

There is also limited numbers of the user who can connect the server at the same time, the application where many numbers of user's needs to connects and access server are not possible, and if this server caught by some hardware failure or by some fault in setup, the data stored on the server will be inaccessible. If this kind of situation occurs and data may unexpectedly lose then it is very difficult to retrieve data back. The maintenance of this server is also high. Another issue with this data storing technique is that they charge the highest possible price to their customer to use their services. Due to overcome all the situations faced in centralized storage, decentralized storage is used to remove all the difficulty which is faced in a centralized structure.

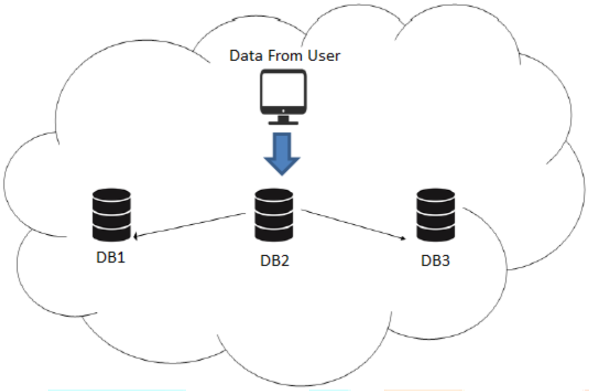

Fig.3: Decentralized Storage

The structure of decentralized storage is shown in Fig.3. Data from the user is being stored on multiple databases assign by a server to make a replica of data, while storing data on a different server it is broken into a piece of chunks. This means, there is huge storage space to store data, and the cost of storing data on a server is less. There is no single party to own the data and control it. This method of storing data is helpful when hackers want to steal data stored on cloud storage. Because of this, they won't able to retrieve complete data. As data stored data at a different location is itself secure in the senses of data loss but to protect data from hackers, we need an encryption method to make data more secure. Even a single data file is stored at multiple locations with small data blocks, but what if that small block of the file contains sensitive information. For this reason, we need an encryption method to encrypt data. All these storage uses some sort of algorithm to make data more secure for their customers. Even a hacker able to access a piece of data, due to an encryption mechanism used by the service provider's hackers is unable to decrypt the information within the data block. That's why decentralized storage is preferred as compared to a centralized storage structure. [1]

III. ALGORITHMS & METHODOLOGY

A. AES Algorithm (Advanced Encryption Standard):

Now a day's cloud storage is used to store and retrieve data that is based on the internet, instead of local storage devices for more reliable, secure, and availability of data. But data is very important and should not be revealed to any unauthorized person, for this purpose encryption method is used to convert this plain data into ciphertext, and a decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm plays the most important role to make data more secure. To achieve these operations some mathematical calculations are made and it is also possible to explain them practically. To encrypt and decrypt, data will be divided into a chunk of the block while performing this operation, there are various algorithms also available which are categorized into two different types. The first one is the symmetric encryption method, in which data can be encrypted and decrypt with the same key. After performing the encryption method data is converted into an unreadable form, to get the original message back intended user must have the key which is used while the encryption process. Then this method reverses its process and data will available in an understandable form. The second one is the asymmetric encryption method, where two keys are generated, one for encryption and the second for decryption [5].

Advanced Encryption Standard (AES) is also known as the Rijndael algorithm which works up to 128 bits of the block length. This algorithm allows the key length of three different bits which are 128, 192, 256 bits. To convert plain text into cipher, this encryption is dependent on key length where this algorithm repeats its method several times called rounds to enhance the security of data. For 128 bits it uses 10 rounds, for 192 bits it uses 12 rounds, and for 256 bits it uses 14 rounds. Excepting the last round in every case, the rest of the rounds are equal to each other. After performing this operation on data encrypted data block is obtained, this is in an unreadable form. To get the original data back the reverse procedure of the AES algorithm is required to perform on encrypted data [6].

To implement such a secure system, we are using Advance Encryption Standard to make data more secure and keep data out of reach from the attackers.

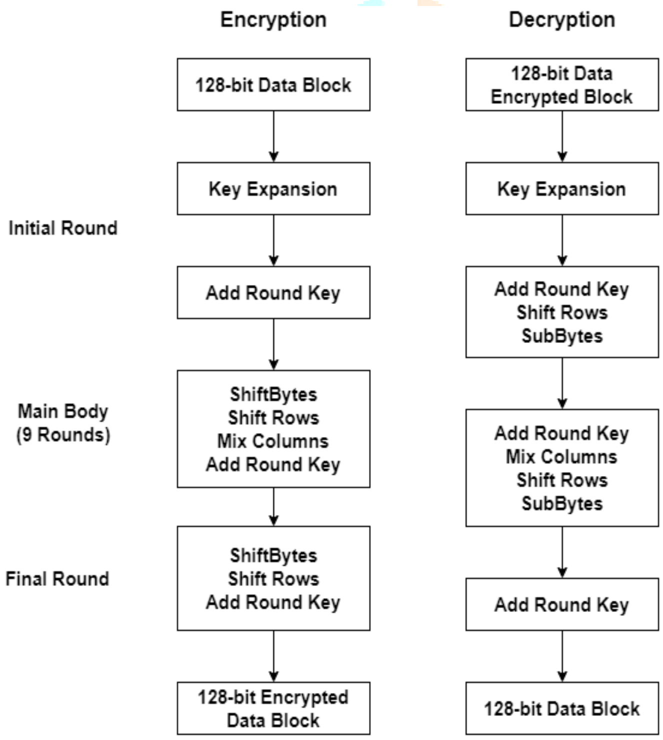
Encryption
Decryption
128-bit Data Block
128-bit Data Encrypted Block
Key Expansion
Key Expansion
Initial Round
Add Round Key
Add Round Key Shift Rows SubBytes
Main Body (9 Rounds)
ShiftBytes Shift Rows Mix Columns Add Round Key
Add Round Key Mix Columns Shift Rows SubBytes
Final Round
ShiftBytes Shift Rows Add Round Key
Add Round Key
128-bit Encrypted Data Block
128-bit Data Block

Fig.4: AES Algorithm Structure

Above fig.4 shows the AES algorithm overall structure:

a) **Data Block:** In this first stage, data is divided into separate blocks. As shown in figure 3 data is divided into columns of four by four in sixteen bytes.

b) **Key Expansion:** This process involves in taking the words as initial key and create array of 44 words, then use with series of keys for every next round for encryption process.

c) **Add Round Key:** Key expansion is done to make 10 keys by method called key schedule. This is done with XORing with resulted data to make input for the next round.

d) **Substitute bytes:** Here, whole words are coded in such a way that one letter after of current word in alphabet. For example, hello changes to ifmmp.

e) **Shift Rows:** As name give idea for this concept, each next row is moved one row back means second row is shift in space of first row; third row is shift in space of second row and so on.

f) **Mix Columns:** Each column has some value which is given by the previous stages of algorithm. Likewise, this mixing of column is performed.

g) **Add Round Key (again):** This block takes input from previous block and add round key which are derived at the beginning of encryption.

At the end of this step, we get encrypted data. To get the original data back reverse operation of encryption is performed on encrypted data and resultant data would be our original data [8].

Now while uploading encrypted data on the cloud server to keep track of the sequence of uploaded data blockchain technology is used. Blockchain technology is a technique that records the information in such a way that it is impossible to interchange the system transaction of data. It works on the hash function. Each block of data is linked with the next block of data by the hash value which is shown in fig.5.

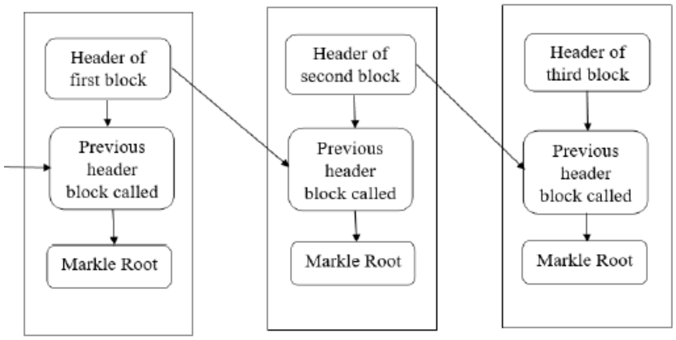

Fig.5: Structure of Blockchain.

For this purpose, blockchain technology is used and considered the most trustworthy, appended only, and efficient for applications where logs of data are more important. Such application including banking, online music, Internet of things (IoT) [3]

B. SHA-256:

The SHA-256 algorithm is a hashing algorithm that performs on data in one-way and it is developed by Ron Rivist. It is an evolution of previous algorithms such as SHA 0, SHA 1, SHA 256, SHA 384. Hashing is also known as compression or message summary function which takes the entire variable length and changes it into a binary sequence of fixed length. The concept of the hashing algorithm is shown in Fig.6.

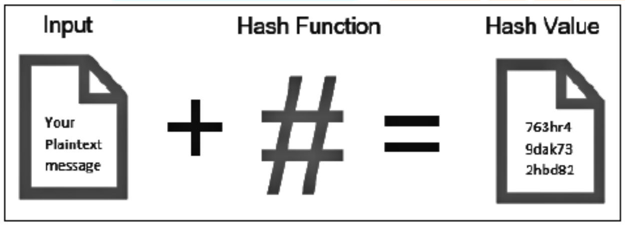

Fig.6: Working of hashing algorithm.

Working of SHA-256 algorithm is given as follows:

The first step is to add a bit as per algorithms rules. It is the first step in all the algorithms. Then SHA-256 algorithm process the block of a message in a block of 512 sizes. The next step is to add bits again with an original message; the addition of bits in the message is 128-bits. SHA-256 is a construction where data is absorbed into the sponge and then the output is derived as a squeezed from the input. In the absorbing stage, data is XORed and in the squeezing, stage data is altered with state transformation. Below fig.7 shown the actual structure of SHA-256 bit algorithm.

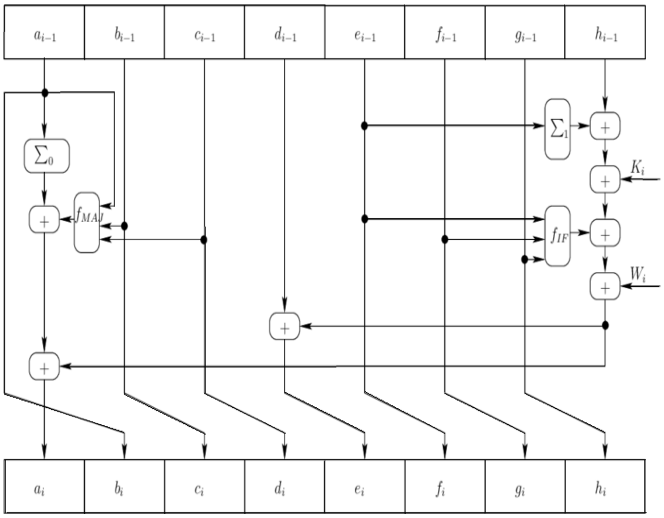

Fig.7: Structure of SHA-256

With the help of AES and Hashing algorithm, we have designed an architecture where users upload data to the cloud server, and with the help of a private key, the receiver can retrieve that data. [4]

C. Consensus Algorithms in Blockchain:

We recognize that Blockchain is a dispenseddecentralized network that offers immutability, privateness, protection, and transparency. There is no significant authority present to validate and affirmthe transactions, but every transaction within the Blockchain is taken intoconsiderationto be completely secured and established. This is feasibleonly because of the presence of the consensus protocol that is a core part of any blockchain community.

A consensus algorithm is a procedure through which all the peers of the blockchain community attain a not unusual settlementabout the prevailing nation of thedistributed ledger. In this way, consensus algorithms acquirereliability inside the blockchain communityand establish considerbetween unknown peers in a distributed computing environment. Basically, the consensus protocol makes certainthat every new block that is brought to the blockchain is the only version of the factthis is agreed upon by way of all the nodes within the blockchain.

IV. PROPOSED SYSTEM

Now a day's security is an important issue 99% of data process online and stored in a trusted server. But when the user stores their data in the authorized server they must be a data transmit and receive through the secure communication channel and at that time security issues have occurred. Recently, maximum data are processed in the following applications or fields such as Healthcare, E-Commerce, Internet Baking, Education and Business application, etc. These all are services are used over the internet and number of chances for various attacks in online services. To address these issues we implementation of a trusted framework for online banking in the public cloud using multi-factor authentication using blockchain framework service as security from various attacks which is shown in fig.8.

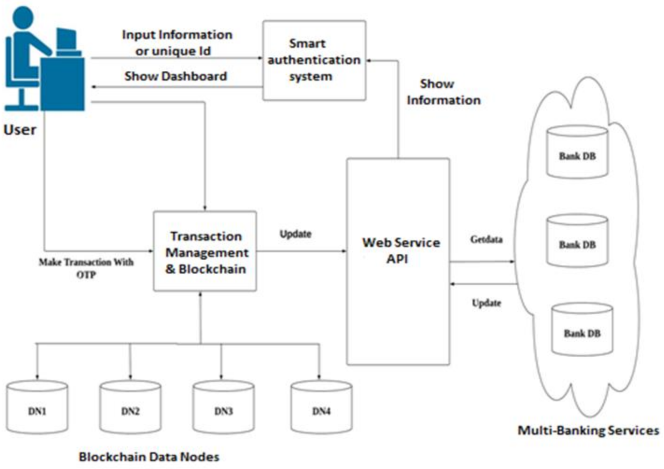

Fig. 8: System Architecture

As shown in Fig.8 here these all techniques are based on designing and develop an own (custom) blockchain to store all transaction records insecure manner. Deploy a dynamic smart contract with a consensus algorithm to enhance the transaction clarity to the end-user only for using a software-based system can achieve security of data records [7].

V. RESULT ANALYSIS

This research work is to implement a web-based application for the healthcare community to prevent various attacks of patients as well as user's confidential data records storage and transmission time. The result analysis is done based on the following parameters is as follows:

- Time consumption
- Response Time
- Computation Cost
- Performance accuracy

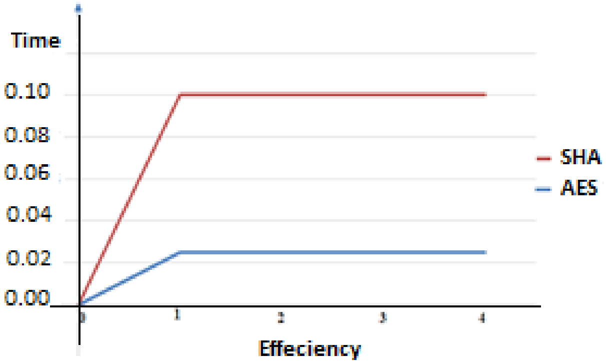

Fig.8: Time and Efficiency Chart

Here, Whole System took more attributes for the input purpose but here mainly concentrates on the Time and Performance of the system. In existing system required more time, space and security issues so we first focus on those things. Supported a couple of attributes we'll get the subsequent analytical result for our proposed system.

Parameter	Existing	Proposed
A	10	4
B	10	5
C	8	8
D	10	3
E	8	2

Table 1: Result Table

Where,

A = Time Consumption.

B = Response Time.

C = Computation Cost.

D = Performance accuracy

E = Scalable & User Friendly.

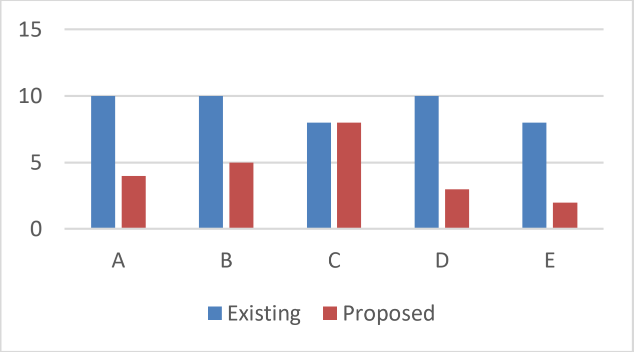

Fig.9: Time line chart of Result Analysis

VI. CONCLUSION

This paper suggests a secure and efficient way to store data on the cloud. Blockchain-based cloud storage with data encryption gives data security in a decentralized structure. The proposed framework for security model is suitable for measures initially used in banking transactions included blockchain technology [10]. The algorithms used to implement the system model are efficient and required less time and give high security for the data which is being stored on the cloud. This kind of architecture makes the system more robust and resistant to different security attacks which are performed by unauthorized users who try to steal and disclose the information in the data files of the user for their benefit. Finally, we conclude that the security level of banking transactions has considerably increased, thus making the overall process of banking much more convenient. [9]

VII. REFERENCES

[1] SaboutNagaraju and LathaParthiban, “Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway,” Open Access Journal of Cloud Computing: Advances, Systemsand Applications (2015)

[2] Dorri, S. S. Kanhere and R. Jurdak, “Blockchainin internet of things: Challenges and Solutions,” arXiv: 1608.05187 [cs], 2019. [Online].

[3] Sukhodolskiy,Ilya, and Sergey Zapechnikov. “A blockchain-based access control system for cloud storage.” Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2018 IEEE Conference of Russian IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. “A Blockchain-based Approach to the Secure Sharing of Healthcare Data.”Proceedings of the Norwegian Information Security Conference. 2020.

[5] Goyal, Vipul, et al. “Attribute-based encryption for fine-grained access control of encrypted data.” Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Wang, Hao, and Yujiao Song. ”Secure cloud-based EHR system using attribute-based crypto-system and blockchain.” Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. “Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy”.

[8] Wu, Axin, et al. “Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing.” Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. “Multiple authorities’ attribute-based verification mechanism for Blockchain micro-grid transactions”. Energies. 2018 May;11(5):1154.

[10] Guo, Rui, et al. “Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems.” IEEE Access 776.99 (2018): 1-12.