International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

Collaborative Secured Data Management System Using Blockchain

[1]S. Ramamoorthy, [2]Vishal Rohila, [3]Kshitiz Sharma

Abstract*--The proposed system uses blockchain technology to provide data integrity to the user of the network. Blockchain enables security in which data integrity can be checked without revealing the information of the user or the actual data. The proposed architecture consists of a Data Owner, Data Auditor and users. The user is the person whose data is in the system, Owner is the person who owns the database and auditors are the technicians who check the data if any data is compromised and make sure the data integrity is intact. The entire data is in the form of blocks and the technology of ring signatures will be used to provide authentication. This will provide a way to check the data without unveiling the original under signer of the data block. Also the information of the members present in the ring signatures group are kept confidential. This provides total security both to the data and user of the database.*

Key words*--Blockchain, Auditing, Encryption, Data Management, etc*

I. INTRODUCTION

Blockchain as a technology involves distributing the entire data into several blocks of equal sizes. Each of such a block has three parts namely the head, the block and the root. The head contains the address of the block, the body contains the information and the foot has the pointer from the previous block. This is how a blockchain is maintained. Each block in a blockchain has it's unique credentials for its security. Any change made in any of the blocks is verified by each system in the blockchain and is recorded in the data maintenance ledger. This ledger shows all the changes made in the blockchain by the users.

In the proposed system various algorithms like Hashing, Message Digest 5 algorithms are used along with the blockchain to protect the database from any security breaches.

II. LITERATURE SURVEY

Public Data Auditing Mechanism and Dynamics (Cong Wang, Sherman S.-M. Chow, et. al.)

MAC is a sequence used to check the integrity of the information received.

Advantages

This allows the auditing of the data stored over the cloud which can easily be accessed on demand by the user. Data authentication of such data is provided by this auditing mechanism.

[1]*Assistant Professor, Dept. of CSE, SRMIST, Kattankulathur, India, ramamoos@srmist.edu.in*
[2]*Dept. of CSE, SRMIST, Kattankulathur, India, rohila.vishal1511@gmail.com*
[3]*Dept. of CSE, SRMIST, Kattankulathur, India, kshitiz1798@gmail.com*

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Disadvantages

Every piece of data retrieved from the cloud is checked by the authenticator. This makes the whole process very hectic and time consuming. This can be reduced for making the process less time consuming and efficient.

Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data authored by Y. Prasanna, et. al.

It provides security to the sensitive information before sending it over to the cloud.

Advantages

When data is uploaded over a cloud, the sensitive information should be protected so that any third party cannot breach the security. This paper provides information about how sensitive information could be protected over the cloud.

Disadvantages

The cost required for the operation of this is very high. Many folds of encryption are required both on the server and client side which makes it using for huge pieces of data very unfeasible.

Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud authored by Boyang Wang, Baochun Li, et. al.

This allows auditing of the data that is stored in some form of cloud storage like Dropbox, Drive, etc.

Advantages

Applications like GDrive and Dropbox are becoming increasingly popular. This mechanism will help in auditing the data which is shared between various users in the cloud environment and hence maintaining it's integrity by revoking the access of faluter over the shared cloud.

Disadvantages

The client which is once revoked can never have access to the data over the shared cloud ever.

Storing Shared Data on the Cloud via Security-Mediator authored by Boyang Wang, Sherman, et.al.

This uses mediators for authenticating the data present in the database.

Advantages

The data is checked by a third party security mediator. The SEM's task is to generate metadata in the form of signatures of the data owners in the data stored.

Disadvantages

The security mediators are a third party entity and have no accountability to the data users or the database owners.

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

Security Aspects of Blockchain authored by TEC, TS Division, Govt. of India.

Blockchain technology is being researched by the govt of India and soon different will be implemented in various fields.

Advantages

Blockchain provides anonymity and security to the various users of the block and the blockchain. This also allows processes such as mining where a huge network is accountable for any change is the data in the network.

Disadvantages

Blockchain computations require huge computing costs. Also mining is a very hefty, time and cost consuming task.

Cyber Security through Blockchain Technology by Alex R Mathew

Blockchain includes many technologies like data ledger and indexing which provides a superior level of security.

Advantages

Blockchain technology involves a network of computers which are connected to each other. Any change in any of the nodes will trigger a change in the entire network which will provide security and data integrity.

Disadvantages

Blockchain as a technology in it's implementation requires great computational and mining costs. This makes using the technology by everyone quite infeasible.

III. INFERENCE FROM THE SURVEY

Inference from the survey was that with the advent of cloud storages, the need for security of the private data stored over third party databases is very important. All the basic research done was based on cloud storage and blockchain separately. The researchers had many advantages but mostly all had the disadvantage that the computation costs were pretty high. This made the implementation of the various technologies quite difficult.

IV. OBJECTIVE OF THE PROJECT

The main objective of the system is to create a setup of ring signatures for performing homomorphic verification. The main goal is to create an open verifier who can verify the data in the database without getting the entire data from the database. This creates a method which provides total anonymity to the user and the verifier. Hence, here the verifier can check the entire data without getting complete access to the data. With the application of blockchain, the working of this method becomes easy and very proficient.

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

V. MODULES

The various modules used are as follows:

1. User Registration
2. Auditing
3. Data Sharing
4. Data Integrity Checking

A. User Registration

The user registration has a very straightforward task. All the new users which are to be registered in the database are done through this module. All users will have unique keys to access and amend the data in the given block. This key will be used for all the decryption process and verification of the data.

B. Auditing

The auditing part is the main part of the proposed system. Here the data is checked for it's integrity and the homomorphic authenticators are uniquely integrated by various masks. Individual blocks generate metadata in the form of homomorphic authenticators and the verifier uses it for the verification process. The verification process has two steps:

1. Setup phase
2. Audit phase.

In the setup phase, the verifiers are registered in the database. The various private keys are assigned to the verifiers whereas in the audit phase, the actual auditing takes phase.

C. Data Sharing

The data which is stored in the cloud is distributed over various blocks. Each block has its own private key and credentials which can only be accessed by the verifier having the correct private key. This module makes the usage of blockchain possible in the proposed system as data sharing sharing between various entities namely User, Data Owner and Auditor is done. These blocks are encrypted and decrypted using various encryption algorithms like Hashing, MD5 along with the various concepts of blockchain over the various blocks created.

D. Data Integrity Checking

Using the concepts of ring signatures here allows us to check the data for its integrity. Also all the changes made in the blockchain are stored and stored in the ledger which are only included in the actual block chain when all the users in thechain approve all the changes.

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

VI. ALGORITHMS USED

A. Advanced Encryption Standard (AES)

AES was an improvement over DES algorithm. The key size of DES was of less bit size, the drawback was that with increasing computing power it got easier to crack DES using brute force attacks. Also Advanced Encryption Standard was found out to be six time as strong as Triple DES.

The AES encryption standard has the following features:

- It uses Symmetric keys.
- It belongs to the class of Symmetric block cipher.
- The data is of 128-bits whereas the keys are of 128/192/256-bits.
- It is six times as stronger and faster than Triple-DES
- AES was implemented using technologies like Java and C.

B. Message Digest 5 and hashing Algorithm

MD5 algorithm is the improvement over MD4 and it was first invented by Ronald Rivest. It is a very widely used hashing function that generates a 128 bits hash key. It was firstly specified in the RFC1321 in 1992. MD5 is still very widely used in various institution,

VII. SCREENSHOT OF THE PROJECT

Fig 1

VIII. RESULTS AND DISCUSSIONS

The proposed system which had the above mentioned modules working together as a unit along with blockchain technology used for its security and authentication was successfully implemented.

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020

REFERENCES

1. P. Mell and T. Grance, "Draft NIST Working Definition of Blockchain Computing," Nat'l Inst. of Standards and Technology, 2019.
2. A. Mishra, R. Jain, and A. Durresi, "Blockchain Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2017.
3. R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, "Key Challenges in Blockchain to Enable the Future Internet of Services," IEEE Internet Computing,vol.17,no. 4,pp. 18-25)
4. K. Hwang and D. Li, "Trusted Block chain with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept.
5. Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data(Prasanna, Ramesh)
6. Security Aspects of Blockchain (TEC, TS Division, Govt. of India)
7. Storing Shared Data on the Cloud via Security-Mediato (BoyangWang, Sherman S. M.Chow, Ming Li, and Hui Li)
8. Short Group Signatures (Dan Boneh, Xavier Boyen,)
9. Remote Data Checking for Network Coding-based Distributed Storage Systems (Bo Chen, Reza Curtmola, Johns Hopkins University)
10. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud (Boyang Wang, Baochun Li and Hui Li)

DOI: 10.37200/IJPR/V24I8/PR280262
Received: 21 Jan 2020 | Revised: 08 Feb 2020 | Accepted: 14 Mar 2020