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 9, Issue 6, June 2020 ||

File Storing and Sharing using Blockchain

Anjaly Renny [1], Anjana Santhosh[2] , Neeraja S, Teena Noyal[3]

UG Students, Department of Computer Engineering, College of Engineering, Chengannur, Kerala, India[1,2,3]

ABSTRACT: The paper deals with secure file sharing in an organization or enterprise by the application of certain modified encryption methods and a unique way of storing the file by adopting concepts used in blockchain technology**.** Normally the files are stored and shared in a centralized way. By using a centralized way of storing and sharing files, it becomes highly vulnerable to data breaches. It may even lead to denial of services and are usually prone to theft from the intruders who would possibly be capable of obtaining the encryption keys. So, in order to overcome this, we are introducing more efficient encryption standards. It focuses on modified AES encryption in the first stage and a technique called visual cryptography as part of re-encryption. This paper is explained by considering an organization into account where the input file or data which a project manager or any other employee in a particular organization needs to share with others in the organization is converted into fixed-sized blocks of data, which is apparently similar to the concept used in blockchain. Here the manager browses different files for each section of employees and merges into a single file with different access rights, so the employee with the respective access right could only view his part of the content that he is intended to view rather than reading the entire file.

KEYWORDS: Blockchain, Visual cryptography, MVC architecture, Access tree structure, Data breaches, dotnet, AES encryption.

I.INTRODUCTION

The growth in technological advancements has led to the abrupt rise in the improvement of digital belongings and transactions. Most people make use of a centralized storage system to share their legit documents or files. Centralized storage is where the files are stored in a single site. With centralized systems, it is very hard to keep personal or confidential files. The documents or files are more prone to information breaches and theft from the intruders who are successful in obtaining the encryption keys. This led to the advancement of adopting concepts from the blockchain. Blockchain is best known as data sharing technology with respect to its application in business transactions. It provides the ease of storing and getting access to data in a decentralized way. Taking into account the case of a company or an organization, the confidential files are first converted to fixed-sized blocks of data which are provided primary encryption using modified AES. Then we divide the file into fixed blocks and hash it, further converted to bytes and stored in a blockchain. We make use of the concept of access tree which forms the basis of automatic key generation. Visual cryptography is used as an additional encryption technique which comes into account if an employee or other user other than the project manager needs to share some confidential file to any other employee. We are using windows and dotnet platform and the code is written on the basis of MVC (Model View Controller) architecture. It is an architectural platform that separates an application into three main logical components: model ,view and controller. Each of these components are built to handle specific development aspects of an application. It is commonly used for developing modern user interfaces.

II.RELATED WORKS

Blockchain based system for secure data with a private keyword search by Hoang Giang Do et al. [1].In this paper, a system that leverages a blockchain technology to provide secure distributed data storage with keyword searches is introduced. The system allows the client to upload encrypted data and distribute to cloud nodes and ensure data availability using cryptographic techniques.

A blockchain-based decentralized data storage and access framework for pingER by Saqib Ali et al. [4] used the permissioned blockchain and Distributed Hash Tables(DHT) for this purpose. Here, metadata of files are stored on the blockchain and actual files are stored off-chain through DHT at multiple locations using the p2p network.

A dynamic tree-based data structure for access privacy in the cloud by Sabnna De Capitani di Vimercati et al.[3].It presents a novel approach for guaranteeing access privacy to data stored at an external cloud provider.

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

|| Volume 9, Issue 6, June 2020 ||

The concept of blockchain-based secure cloud files sharing scheme with fine-grained access control by Yuke Liu et al. [2], is to introduce cipher text policy-based attribute encryption as an effective tool to realize fine-grained data access control of the stored file. Meanwhile, the security analysis proves the confidentiality and integrity of the data stored in a cloud server.

III.METHODOLOGY

In this paper, we are proposing a secure file sharing method along with the concepts used in blockchain technology. The project is mainly divided into two systems: Proxy Server and the Application System. The user registration and login, file uploading, downloading of files etc takes place in the application system. The database stores the details of all users like username, designation, IP address etc. Whenever a user login to the system, it will be updated and get displayed in the proxy server.

A.MODIFIED AES ENCRYPTION

Before passing our data or file into the modified AES encryption algorithm we first convert the contents of the file into bytes. These bytes may be random numbers or letters that are in non-readable format. The password used for encryption is provided an additional security using 'salt'. The salt is a random data that is used as an additional input to a one-way function that hashes the password. A salt is basically some random constants or letters that is unique to each user. The key or password will also be converted into byte format by passing it into a class called 'crypto'. Now both the file and the key, in bytes form, is divided into an 8*8 matrix form. The salt is also converted to bytes. Then the salt and key in the bytes form get mixed up. They form a structure which will then be passed to a rigid management class. It forms an encoding structure which is further divided into 8*8matrix form. The modified key in bytes is converted into vector form. The key in vector form is again divided into blocks of eight. Finally, the file or data in blocks form and key is passed to the modified AES encryption. After performing the encryption, the file is divided into fixed-sized block based on the size of file. Then hashing will be performed on blocks of file, specifically SHA 256(Secure Hash Algorithm 256).The hashed blocks are converted into bytes and then stored in the blockchain.

B.HASHING TECHNIQUE

Hashing is a method of cryptography that converts any form of data into a unique string of text. Data having any arbitrary length can be hashed to a fixed sized length. In our proposed system we implement SHA-256 hashing algorithm.
SHA 256 is secure due to:

- Deterministic in nature
- Quick computation
- Infeasible to detect due to pre-image resistance

This concept of hashing makes the blockchain revolutionary. The file is divided into fixed size blocks and hash value is computed for each block. The file blocks are kept in the blockchain as a collection of records linked with a strongly connected hashing algorithm. Blockchain holds all the hash values using the hash pointers as reference so that duplicate blocks can be eliminated.
The security of blockchain relies in:

- Every file block has unique hash value
- No duplicate block can be added
- If tampering happens proof of work needed to be recalculated which is infeasible
- Blockchain is strongly connected via the P2P network.

C.AUTOMATIC KEY GENERATION

After encrypting the file with the secret key the file is uploaded and transferred to the blockchain. On the receiving side, the recipient downloads the file with the shared secret key and tries to decrypt. While decrypting the file an access tree is generated based on his user id. Access tree is a structure with hashed tree nodes containing the user information. This access tree is checked at the time of decryption to generate automatic random key. If an unintended user tries to decrypt the file his access tree will not match with the authorized access tree of user and fail to generate exact random key to decrypt the file. Thus the file uploaded can only be read by an intended user with proper access rights. This technique provide high security and distinguishes our system from the existing one.

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

|| Volume 9, Issue 6, June 2020 ||

*D.**VISUAL CRYPTOGRAPHY***

A cryptographic technique which allows visual information to be encrypted in such a way that the decrypted information appears as a visual image. Here in our project we are using this method as a re-encryption technique to add more security to the data, if the user wishes to. The file is divided into 'n' shares where each share is secured with a password. Finally the shares are merged and a secret key is generated. The security of this encryption lies in the fact that even if 'k' out of 'n' shares are hacked this can't be superimposed to get the original data or file.

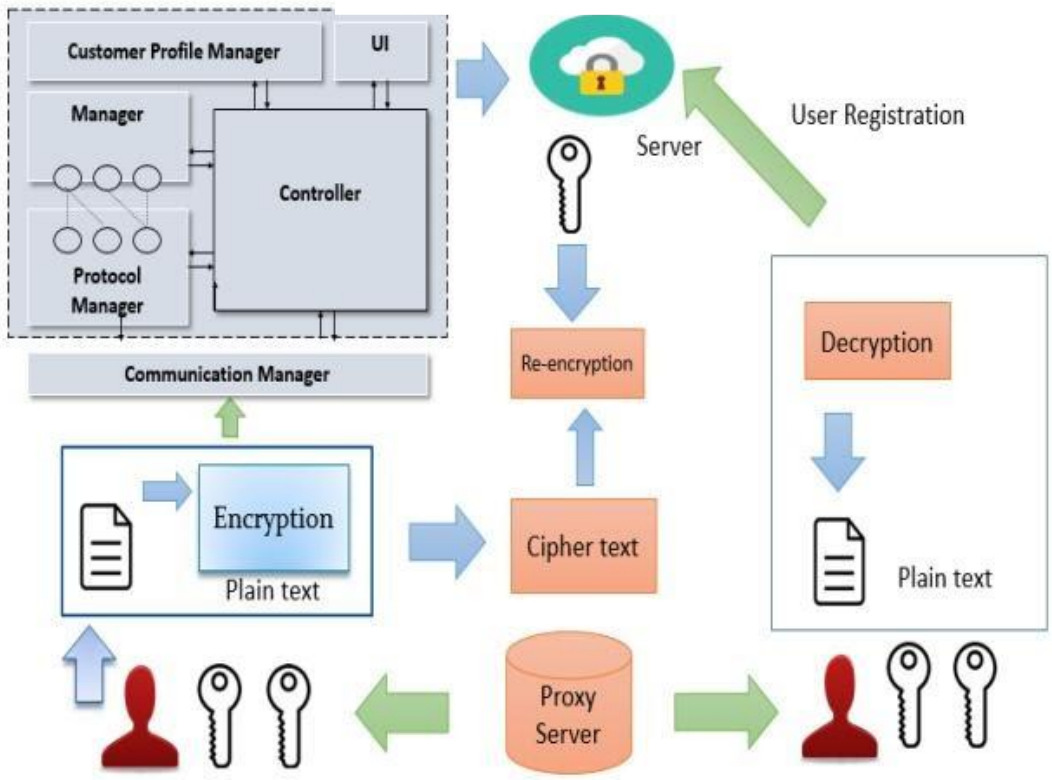

Figure 1:Block diagram for file storing and sharing using blockchain

IV.PERFORMANCE ANALYSIS

Comparison of Proposed system vs Existing system on the basis of node data parameters:

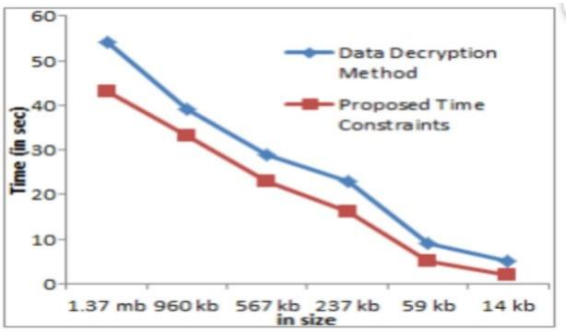

Figure 2: Data decryption vs time constraint plot

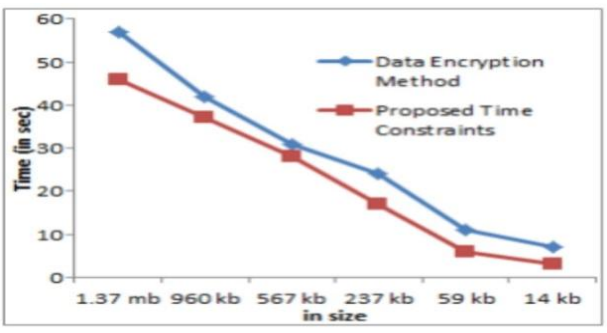

Figure 3:Data encryption vs time constraint plot

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

|| Volume 9, Issue 6, June 2020 ||

V.CONCLUSION

Blockchain is an emerging technology in many fields like machine learning, banking sector, military sector and many more. It also has certain limitations like immutability for certain applications in which information needs to be changed. Even with these limitations, we have to embrace and encourage its wide applications in various sectors. In this paper, we presented a much secure method of file sharing and storing it in a trusted platform like blockchain. This method can to an extent terminate all the limitations of using a centralized network for sharing confidential files in an organisation. The users also have an option to choose the additional re-encryption technique that this system is offering. Also the performance analysis graph shows the comparison of our system with the existing system which proves to be much secure, efficient and effective.

REFERENCES

[1] Hoang Giang Do, Wee Keong Ng, "Blockchain based System for Secure Data Storage with Private Keyword Search," in IEEE World Congress on Services (SERVICES) , 2017

[2] Saqib Ali, Guojun Wang, Bebo White, Roger Leslie Cottrell, " A Blockchain based Decentralized Data Storage and Access Framework for PingER," in 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Bigdata Science and Engineering (TrustCom/BigdataSE).

[3] Sabnna De Capitani di Vimercati, Sara Foresti, Riccardo Moretti, Stefano Paraboschi, Gerardo Pelosi, Pieran, "A Dynamic Tree based Data Structure for Access Privacy in the Cloud," in 2016 IEEE International Conference on Cloud Computing Technology and Sciences (CloudCom).

[4] Yuke Liu, Junwei Zhang, Qi Gao, "A Blockchain based Secure Cloud Files Sharing Scheme with Fine-Grained Access Control," in 2018 International Conference on Networking and Network Applications (NaNA).

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA,2006, pp.89-98.

[6] Zheng Yan, Senior Member, IEEE, Lifang Zhang, Wenxiu Ding, and Qinghua Zheng, Member, IEEE, "Heterogeneous Data Storage Management with Deduplication in Cloud Computing",2019