Data Security using Blockchain Technology

P.Nivethini
Department of Information Technology, Velammal Engineering College.
Email: nivsps@gmail.com
S.Meena
Department of Information Technology, Velammal Engineering College.
Email: meena29111997@gmail.com
V.Krithikaa
Department of Information Technology, Velammal Engineering College.
Email: krithikaav19@gmail.com
G. Prethija
Department of Information Technology, Velammal Engineering College.
Email: prethija@velammal.edu.in

----------ABSTRACT----------

In recent years, blockchain technology has gained considerable attention. A blockchain is a public ledger of transactions or events recorded and stored in chronologically- and linearly-connected blocks. Later blocks maintain the hash code of previous blocks. It records cryptographic transactions in a public ledger or book that is difficult to alter and compromise because of the distributed consensus. As a result, blockchain is believed to resist fraud activities and hacking.

Although blockchain technology resists several types of malicious attacks and reduces many associated risks, it does not eliminate all attacks. Its preventative mechanisms (e.g., distributed consensus, cryptography, and anonymity) may impair its resistance to some types of frauds and maliciousness. In this project, we use blockchain technology in file transfer system. Since blockchain provides only the authentication, we intend to provide confidentiality to the data by encrypting it with the encryption algorithm, AES before hashing. Thereby, we can ensure the security of data and can make it trustworthy for the users.

Keywords **- Blockchain, AES, Hashing, Encryption, File transfer.**

I. INTRODUCTION

In recent times, the blockchain technology has been a growing technologies and it is in use in various applications like bitcoin transactions, file transfer, record keeping and in many other applications. Blockchain uses a hash function to get the hash codes which is used to link two blocks in the blockchain. In a large network, the hash codes are difficult to compromise but in smaller networks, the hacker always finds a way to hack the network. In such cases, the data can be secured by using the more popular and widely used encryption algorithm, AES before hashing a file.

1.1 AES

AES is one of the widely accepted encryption algorithm used for encryption. AES holds its own and unique structure for encryption and decryption.AES can deal with three different key sizes such as AES 128, 192 and 256 bit and each of these ciphers has 128 bit block size.The number of rounds is based on the key length. The size of the key decides the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

From Fig.1, we can infer that AES encryption algorithm is more mathematically efficient and elegant cryptographic algorithm and exponentially stronger than the DES encryption algorithm.

1.2 Blockchain technology

A blockchain, as in Fig.3 is a chain of blocks or is a growing list of data, called blocks, which are linked together with the help of cryptography. Each data block contains a cryptographic hash code of the block before it, a timestamp, and the data to be transmitted. Modification of data in the blockchain is not allowed. When a data in a block is changed, it affects the upcoming blocks and hence the whole blockchain changes.

1.3 SHA 256

SHA 256 is the cryptography encryption algorithm, which is the advancement of SHA-1 and it is one of the strongest hash function available. It is not compromised by others till date. It provides a unique 256 bit hash code, also knownas signature for a text or a data file. By comparing the calculated "hash value" to a known and expected hash value, data's integrity can be determined.

The hash value as in Fig.2 is a one way code generated from the sender's side and it cannot secure the file or data in the file. The hash code, generated from the hash function is used only for authentication purpose and not for the encryption or security purposes. The hash code can only guarantee the authenticity but not the confidentiality of the data or the file that is transferred.

II. RELATED WORKS

There are several applications that provide file transferring, but no applications can match the security provided by block chain technology. In [12], Sri Balaji, et al proposed a Secured and decentralized file transfer application using block chain which explains the file sharing application by using private blockchain network that can be used in smaller organizations. The data structures such as Merkle tree data structures and Round

robin mining are used. In [14] A Survey on File Storage & Retrieval using Blockchain Technology explains about the Ethereum platform and technologies like swarm and whisper that can make it possible to make a secured file storage and retrieval Decentralized Application (DApp). An enhanced mechanism for data storage and file transfer is created. Alex Kibet researched on "A Synopsis of Block chain Technology" and presented a brief overview of block chain technology by giving its history, explaining its architecture and the challenges faced in blockchain technology currently and consensus algorithms used in systems that are based on blockchain [4]. In current Research on Blockchain Technology the most of the research is focused on explaining and improving constraints of Blockchain from privacy and security aspects, but many of the proposed solutions lag concrete evaluation on their power. Reinforcing the links of the blockchain explains the motivations, features and applications of blockchain in [8].A Temporal Blockchain: A Formal Analysis conduct a complete analysis of work and gives a formal analysis of the blockchain by Richard Dennis, et al [10] compared the results to a traditional blockchain model. In [5] Cryptography: A Comparative Analysis for Modern Techniques, FaiqaMasqsood, et alevaluated the execution of different symmetric and asymmetric algorithms by taking multiple attributes such as encryption/decryption time, key generation time and file size. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data explains the features of AES algorithm and some future researches on this algorithm in [3].[6]Are blockchains immune to all malicious attacks? Explains the different types of frauds and attacks that blockchain technology might prevent and behaviors to which it is vulnerable. It also gives many anti-attack measures. In [9] design of modified AES algorithm for data security provides high speed as well as less data transmission over the channels that are not secured.

III. Proposed Work

In this paper, we have used block chain technology concept and the encryption algorithm to secure the data file while transferring files from a server to a client. Firstly, the data in the requested text file is encrypted using AES encryption algorithm.

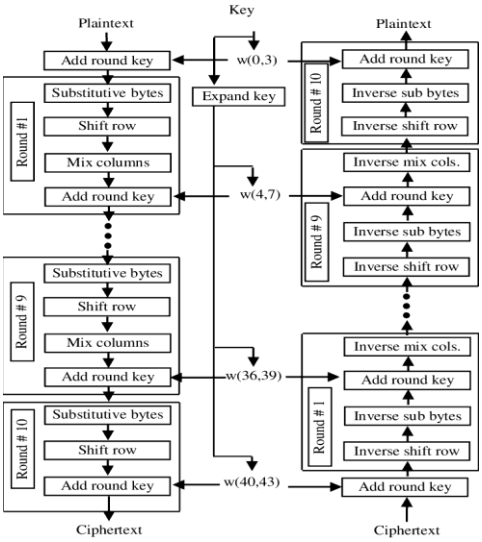

Fig.1:AES Encryption and Decryption.

Secondly, the encrypted data file is sent to the hash function which implements SHA 256 hashing algorithm and gives a hash code. The encrypted data file is then sent to the client.

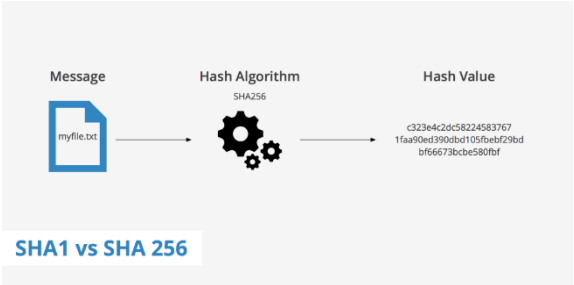

Fig.2: SHA-256

On the server side, the encrypted file is received and the server verifies the hash code to check the authenticity. If the hash code matches, then it is understood that the data file is not altered or accessed by any intruders or hackers. After the authentication verification, the client decrypts the data file using the same key that is used for encryption.

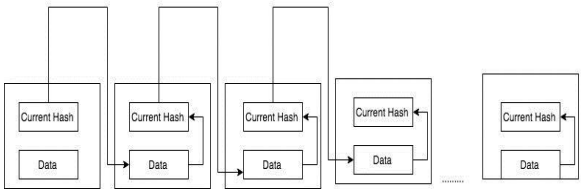

Fig.3: Blockchain Implementation.

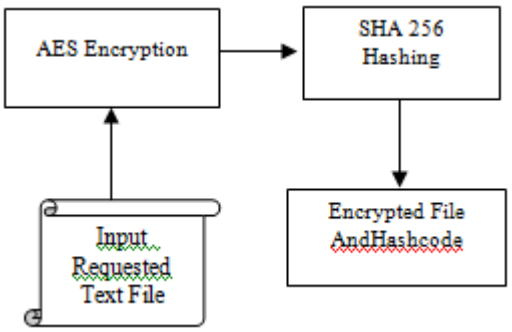

Fig.4: Block diagram of proposed work (server side)

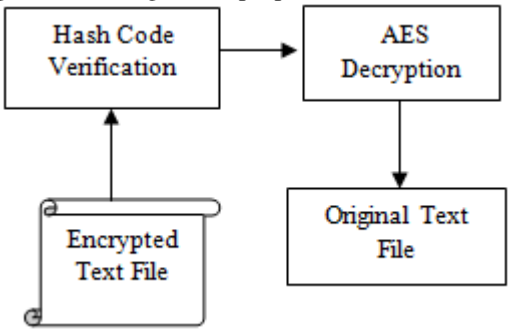

Fig.5: Block diagram of proposed work (client side)

Steps involved:

Step 1: The client requests for a text file to the server.

Step 2: The requested text files are given as input on the server side for encryption.

Step 3: The text files are encrypted using AES encryption using 'file processor' function in fileread.java.

Step 4: The hash code for the encrypted text file is calculated using 'applySha256' function in StringUtil.java

Step 5: The encrypted text file is sent to client from the server using Socket.

Step 6: The encrypted file is received by the client and the hash codes are verified.

Step 7: The hash code is calculated in the client side and is compared with the hash codes from the server side.

Step 8: If the hash codes match, then there is no problem with the file, the client can decrypt it using the secret symmetric key.

Step 9: If the hash codes do not match, then there is a change in the file and the hacker has changed the original data. In this case, the process is terminated.

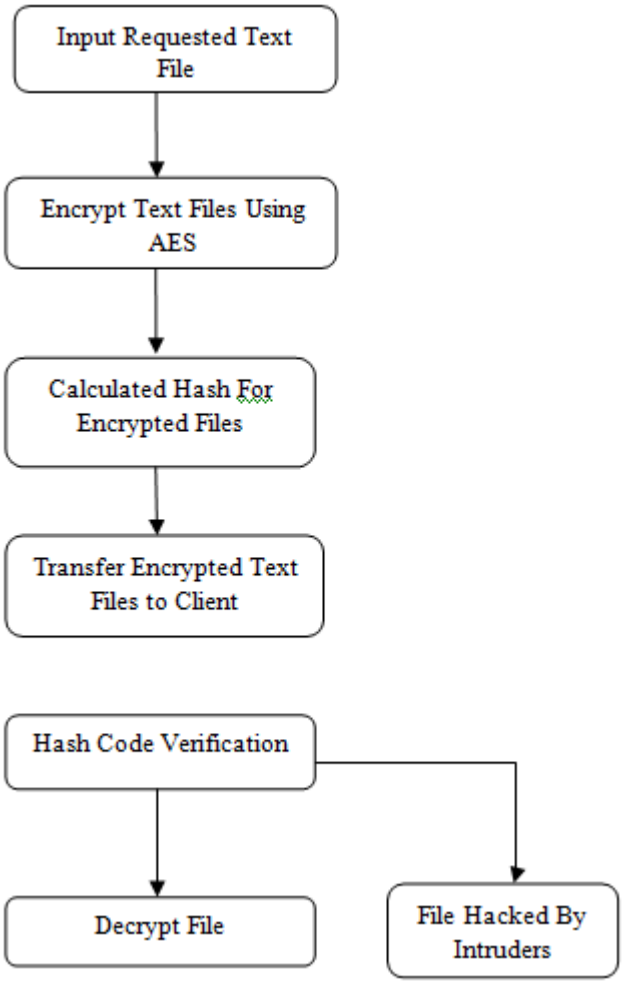

Fig.6: Implementation flow diagram.

IV. Results and Discussion

The implementation results for data security using block chain technology concept is as follows: Fig.7 and Fig.8 explains the java code implementation in eclipse IDE. In the server side implementation, the input text files are considered as blocks and the hash codes for the blocks are generated.

In client side implementation, the encrypted text files and their hash codes are received. The hash codes are calculated for the received files and are compared with the received hash codes. If the hash codes match, then the message, "Hash codes match" is displayed and the files are decrypted using AES decryption algorithm. If the hash codes don't match, then the message, "Hash codes do not match! File Hacked!" is displayed.

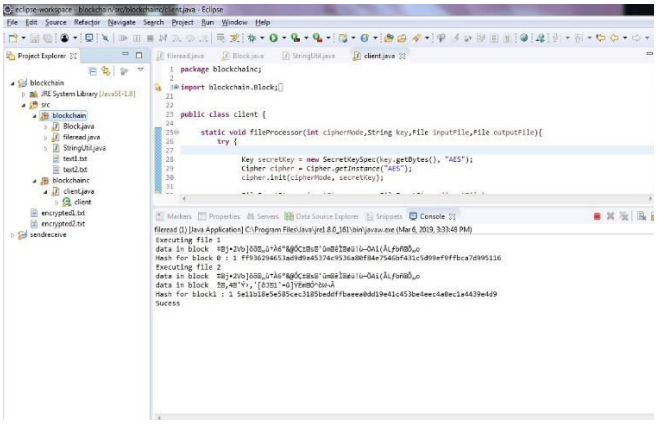

Fig.7: Server side implementation.

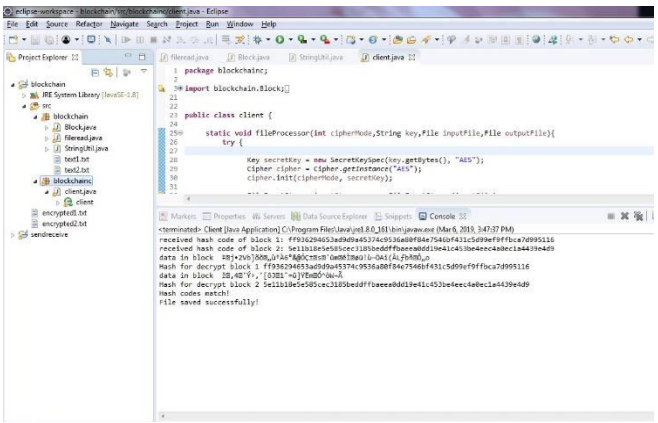

Fig.8: Client side implementation.

V. CONCLUSION

From this paper, we have ensured the safety of data files that is transferred over smaller networks and have used the blockchain technology concept for doing so. We hope that our work can provide security over transferring data files in a smaller network.

In future, this paper can be extended to larger networks with larger numbers of files transferring and can also use the blockchain technology concept more efficiently. In this way, we can provide better file transferring in a wide network with more security.

VI. REFERENCES

[1] Aitzhan, N. Z., &Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams.*IEEE Transactions on Dependable and Secure Computing,* 15(5), 840852.

[2] Ajay Kakkar, M.L. Singh, P.K. Bansal, *Efficient key mechanisms in multi node network for secured data transmission, Int. J. Eng. Sci. Technol*. 2 (5) (2010)787–795.

[3] AkoMuhamad Abdullah," Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", 2017.

[4] Alex Kibet, "A Synopsis of Blockchain Technology, December 2018, and *International Journal of Advanced Research in Computer Engineering & Technology" (IJARCET)* Volume 7, Issue 11, November 2018, ISSN: 2278 – 1323.

[5] FaiqaMaqsood, Muhammad Ahmed, Muhammad Mumtaz Ali, Munam Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques", *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 8, No. 6, 2017.

[6] Jennifer J. Xu, "Are blockchains immune to all malicious attacks?",Xu Financial Innovation (2016) 2:25 DOI 10.1186/s40854-016-0046-5.

[7] Jesse Yli-Huumo, DeokyoonKo, Sujin Choi, Sooyong Park, Kari Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review", DOI:10.1371/journal.pone.0163477 October 3, 2016.

[8] Morgen Peck, "reinforcing the links of the blockchain", *IEEE FUTURE DIRECTIONS BLOCKCHAIN INITIATIVE WHITE PAPER BLOCKCHAININCUBATOR.IEEE.ORG*.

[9] B.NageswaraRao, D.Tejaswi, K.AmruthaVarshini, K. Phani Shankar, B. Prasanth, "*design of modified aes algorithm for data security", International Journal For Technological Research In Engineering* Volume 4, Issue 8, April-2017.

[10] Richard Dennis, Gareth Owenson, Benjamin Aziz, "A Temporal Blockchain: A Formal Analysis".

[11] Shivani Sharma, Yash Gupta, "Study on Cryptography and Techniques",*International Journal of Scientific Research in Computer Science, Engineering and Information Technology* © 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307.

[12] SriBalaji, Vignesh Mohan, Soundarya, "*Secure and decentralized file transfer application using blockchain*", ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-4, 2017.

[13] Tien Tuan AnhDinh , Rui Liu, Meihui Zhang , Member, IEEE, Gang Chen, Member, IEEE, Beng Chin Ooi , Fellow, IEEE, and Ji Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems", *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING*, VOL. 30, NO. 7, JULY 2018.

[14] YashRanka, JainamBagrecha, Kavish Gandhi, BhargavSarvaria, Prof. P. M. Chawan, "A Survey on File Storage &Retrieval using Blockchain Technology", *International Research Journal of Engineering and Technology (IRJET)* e-ISSN: 2395-0056 Volume: 05 Issue: 10 | Oct 2018.

[15] ZibinZheng and ShaoanXie, Hong-Ning Dai, Xiangping Chen*,Huaimin Wang, "*Blockchain challenges and opportunities: a survey", Int. J. Web and Grid Services,* Vol. 14, No. 4, 2018.