International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218481

The Security of a Blockchain-Based File System in a Software Defined Network Framework

Anusha M*[1], Prof. Thyagaraja Murthy A*[2]

*[1]PG Scholar, MTech (NIE), Department of Electronics and Communication Engineering, JSS Science and Technology University Mysore, India

[2]Associate Professor, Department of Electronics and Communication Engineering, JSS Science and Technology University Mysore, India

Article Info
Volume 8, Issue 5
Page Number : 22-29

Publication Issue :
September-October-2021

Article History
Accepted : 01 Sep 2021
Published: 05 Sep 2021

ABSTRACT

Developing distributed form of file security systems using Blockchain technology. Based on the idea of cloud storage as it is a leading storage technology for huge data storage. Blockchain is one of the trending technology for decentralized data storage systems that ensures privacy, confidentiality, data security, authentication, and integrity. As SDN network provides support to have various nodes in the network for the secure transaction of data from source to destination. Blockchain helps in keeping track of block data by constructing the gateway to make it immutable. BCFS refers to Blockchain-Based File System Security in SDN. In the designed system, a Web-Based Interface is developed an authorized entity can upload file data the user's file is projected to encryption process and the block data is shared among the various nodes in the network. Along with Unique Document ID, encrypted random key, and hash data. This hash data value holds the file path and preserves in the blockchain into their corresponding block data folders. Detection of node failure across the network an automatic short path is chosen by the network and detection of an attack based on entropy value.

Keywords : Blockchain, Data Security, Encryption, Web Based Interface, authenticated user, Node failure, attack.

I. INTRODUCTION

Blockchain provides a universal state layer as any user can trust each other. The new kind of distributed data storage and management avoids data accessibility from fraudulent users. It provides a trusted ledger of transactions, where data is rigid and replicas of encrypted data information are stored on every single node of the secure network. The unique Document ID is added to reduce the risk of attacks and to make the network secure, collision-resistance, and fault-tolerant.

As per the article [1], The Blockchain was first used in the cryptocurrency network i.e. Bitcoins. As cryptocurrency networks prepare a virtual currency that is not dependent on any bank to manage the transactions. This network can handle a huge number of transactions due to the key architecture of Blockchain. Data integrity plays a major role in Blockchain's leading edge as data information is unchangeable in the network. Blockchain technology incorporates a list of single linked data which are of the form of blocks called Blockchain. A miner is used to create a set of blocks. In the designed system, a Web-Based Interface helps to keep track of all owners and users data in a SQL database. To enhance the security, accessibility, and integrity of the data SDN network is used. Data accessibility is approved by the owner of the data in a prioritized way for the corresponding file request. Based on the cloud storage approach and to secure the data integrity the proposed system is implemented using a web-based interface to keep track of the data access by unauthorized users.

The major contribution of this paper is performance of a Web-Based User Interface to trace the data access by unauthorized users by using the ideal cloud standard methodology in SDN. This mechanism provides a service to enhance data protection, data security, privacy, authentication and confidentiality in the data transaction.

II. LITERATURE SURVEY

Somanath Tripathy [1], Peer-to-Peer technology helps to enhance the integrity, security, privacy, and confidentiality of the data in the network system. The proposed mechanism uses the method called respect score. It reduces the chance of attacks like RTI, Sybil score attacks. Also provides a new mechanism to the operating nodes in the network to enhance the respect score by providing transaction services. Yuke Liu [2], The centralized cloud services provide all kinds of online services for data storing, sharing, modifying, and deleting. The CP-ABE (Ciphertext-Policy Attribute-Based encryption) usage helps to enhance the security of the fine-grained network. Lee, Bih-Hwang [3], As data security is the major challenge the use of Blockchain is one of the security improving factors. Another is increasing security by encryption process by using AES 256bit, SHA 512bit, IDA. HEROKU is one of the kinds of the platform as a service. Which encourages the use of many coding languages like Node.js, PHP, Java, Python, etc. Chaitanya Rahalkar [4], As HyperText Transfer Protocol is limited. In current world data duplication, data loss is a major issue. To overcome these securities, integrity-related issues P2P file-sharing systems came into existence. As the storage of data by the IPSF protocol network is more secure. Data is of the form of petabytes. Naizheng SU [5], step up the problems that are related to centralized cloud storage and Blockchain is the best suggestion to solve the issues. The current trends of how sky drives. Google drives and dropbox are working in centralized cloud data storage. Characteristics that influence the usage are low cost, virtualization, high demand.

Shubham Desai [6], Blockchain enables all the users to create a ledger to hold all the transaction details. All modified, new, or delete transactions are then updates into the ledger of the user. Uses SHA and md5 algorithms for security purposes. It also uses the HASBE mechanism to enhance the efficiency and security of the system. Cachin Christian [7], this paper discusses Blockchain data transaction is pemissioned or permissionless. As hyperledger allows permissioned transactions. Hyperledger is an open-source platform which permits block data transaction between trusted entities. Subarna Shakya [8], The major discussion in today's software-defined network (SDN) is to increase the data security level. As Blockchain is a distributed ledger data structure element similar to linked list but these blocks stores the hash value of previous blocks for further transactions. Openstack helps in the logical grouping of resources from the cloud storage. It uses SHA, Digital Signature algorithms for encryption purposes. Blockchain Security over SDN (BSS) is proposed which protects data privacy and availability of data resources against fraudulent users. Jiasi Weng [9], Blockchain-based secure monolithic technique is used for SDN. As SDN, provides a network for both control plane and data plane With these features, several pitfalls of the traditional network architectures such as maintenance cost, resource utilization, network management, integrity & consistency of information and controller utilization can be effectively avoided as an exposed mode between both control and the data planes is present. Ruj, Sushmita [10], This paper, Includes Blockchain data transactions from source to destination in the form of blocks. As Block Store uses Blockchain technology which guarantees the transaction between host and renters. Whether these entities are available for the public. As renters can create, search, modify, delete the data.

BhavinKumar Kothari [11], The Internet of Things is an interconnected network for all computing elements. As Blockchain provides a wide area for IoT gadgets and applications. Describes how the communication and transaction of data take place between various IoT devices and how data is stored on decentralized Blockchain systems by using new technologies of Bluetooth, 4G, etc. Manisha Nehe [12], Data reliability is the major problem in the current network world. Blockchain plays a major role in security, identity, data transparency, security of data during a data transaction. As many of us have less information about how Blockchain works its awareness and adoption. As Digital signature generates information of data integrity and data integrity of the signer is discussed. David Janos Feher [13], the paper discusses how authentication will play a role in the blockchain. Nowadays authentication is a major issue in the network system. As high-end companies make use of Security information event management. Log Collection and log analysis are major characteristics to monitor few standards like SOX, DSS, etc. In [14], a well-known factor that Blockchain technology maintains confidentiality, certainty, and availability of information. The paper explores about , the block data is subjected to the crypto hashing process. A hash function stores the variable-length data along with hash values in it. It also uses Digital Signatures for encryption purposes and generates the private key to fetch the original data and the comparison between Blockchain with digital signature and Blockchain without a digital signature is done for performance analysis. Meet Shah [15], As Blockchain is one of the decentralized storage systems. The paper, explains the metamask browser extensions how the data is divided into blocks, and data transmission to multiple peers in the form of blocks. Uses AES encryption standards for encryption purposes.

Indrajeet Bharadwaj [16], By making use of Blockchain technology for security purposes of all single users' data. To prevent data access from unauthorized users due to huge loss of data, privacy, confidentiality and, security. Sarra Boukria[17], Software Defined Networking (SDN) technology enhances the network certainty, integrity, and reliability of data. The paper talks about, the communication between various elements of the SDN network and forwarding devices plays a major role. The false rules forwarded from the attacker to the Software-Defined Network constituents of the data layer are detected.

III. METHODS AND MATERIAL

The designed interface mechanism includes five sections as shown in below fig 1. The user first creates an account or register on the Web-Based Interface. The user details are stored in a database and the user can access the data only through registered details also the data are fetched in the application through a register. aspx from the Web-Based Interface.

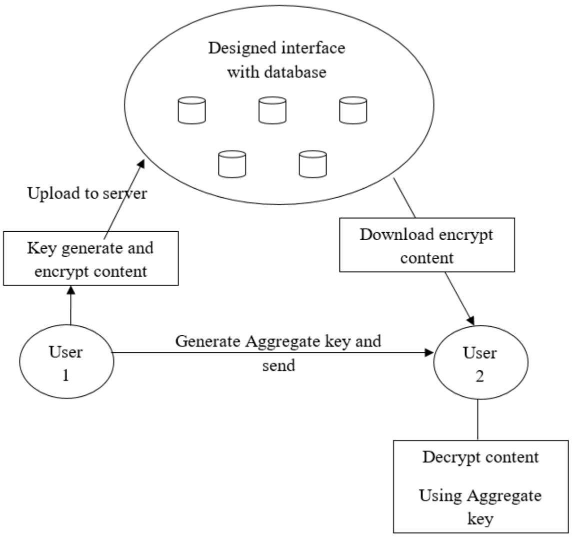

Designed interface with database
Upload to server
Key generate and encrypt content
Download encrypt content
User 1
Generate Aggregate key and send
User 2
Decrypt content
Using Aggregate key

Figure 1 : Block Diagram

Later users can log in with his/her credentials and each user can select any of the files to upload through the browser gateway. Forward to the Data Encryption Standard encryption algorithm uses the user's file data and encrypts the uploaded file subsequently divides the encrypted file data into blocks. An authorized user seeks the file data needed for work progress. Authorized users can wait for the data owner's confirmation. On confirming the data access for a particular authorized user, the user's file is maintained across available nodes using the MultiChain standard. MultiChain then retains a hash data value that comprises the file path. Then the file path is mapped to users unique document ID along with document name details by collecting Eupload data and reserved securely in the blockchain. For Pursuing high confidentiality, privacy, certainty, security, and accuracy of data.

The terminology briefs about the technology used are discussed below :

Web-Based User Interface: A Gateway that aims to link with the system.

Visual Studio: Visual Studio uses a database where one can add any number of databases to make an application platform as per the requirements. As Visual Studio is a open-source software.

Nodes: They are the users of the Interface who provides space to store user's file data and also play a major role in block data transactions.

MultiChain protocol: MultiChain is a protocol which is implemented for private network transactions .

DES: DES is a block cipher that encrypts the data of a length of 64 bits. As the key length is 56 bits.

1. File Upload

When a file is uploaded by Registered/Authorized Users. The user utilizes the file selector to upload the file. This Interface examines the space consumption by the file and ensures space accessibility in the system and pops up with the notification. The file is then uploaded when enough space is available.

2. Encrypting the file

When the file upload is done, the file is projected to the encryption process using DES 64 bit encryption standard. A random encrypted value is generated by manipulating the user's details along with a hash value. This value is used to encrypt the file block data. Which in turn enhances the privacy and integrity of data.

3. File data is stored across multiple nodes

The file which is projected to encryption is later divided into blocks of 1 KiloByte each. Then the block data is sent across the network to different nodes accompanying the support of the MultiChain standard. Designed interface makes use of intranet and only recorded list of users data storage is allowed. The data block is replicated into Eupload directory storage for the easy and high availability of the file data for lawful users. The hash value stores the file path. The file data is mapped with the hash value of the users file and the associated unique Document name and Document ID then stored in blockchain. SDN network is likely to provide support for privacy, security, and confidentiality of file data. Network controls the transaction between every single node in each scenario. Below are few lines of code executed in a blockchain network when predetermined conditions are true.

4. File request and file access for authorized users

The file request and providing file access are managed by the owner of file data. A lawful user can request the file data uploaded by the possessor of the file data. When an authorized user requests the file data the owner of file data will check the list of file requests he/she wants the access to download then the owner of file data tries to grant, revoke, reject requests based on the file request priorities and also based on the request made by legitimate users or not.

5. Transaction of the data, node failure detection by SDN, and attack detection.

The network is designed as shown in fig 2.Transaction of data packets along with encrypted blocks from source to destination. Node failure can be detected by SDN is based on several scenarios for node failure. Attack detection based on different scenarios.

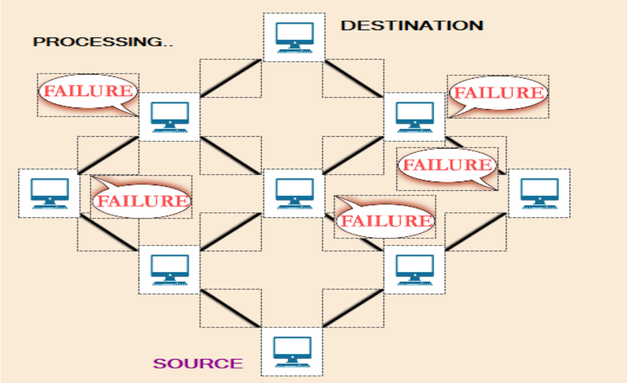


Figure 2. SDN network with multiple peers

IV. RESULTS AND DISCUSSION

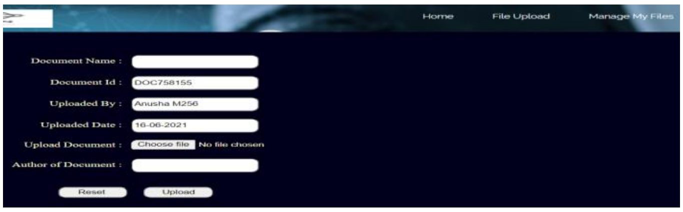
A. System Designed with Register and login page

As depicted in fig 3.To access the Web-Based Interface, GUI users have to first sign up on Web-Based Interface and log in with the relative registered username and passwords. The interface directs the users to the home page to select the file to upload when the login is successful.

Figure 3.Home page of Web-Based Interface

B. Designed System with File Upload Interface

The below fig 4 shows the page for a file upload by using the file browser. Which generates a random Document ID along with the Author of the Document, Unique Document Name can be added, and Uploaded by which user and Uploaded data are stored in the database.



Document Name :
Document Id : DOC758155
Uploaded By : Anusha M256
Uploaded Date : 16-06-2021
Upload Document : No file chosen
Author of Document :

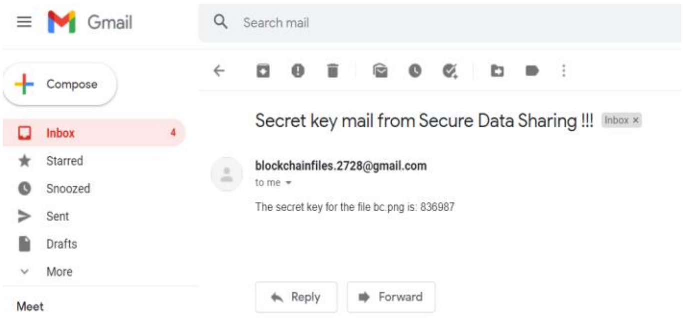
Figure 4. File Upload page of Web-Based Interface

C. Designed System with Multiple Nodes of Network

In which the network helps to find the nearest path for the data transactions from source to destination. Hence after each packet reaches the destination then the data packet is marked as sent.

D. Designed System with Secret Key Interface

Fig.5 shows the secret private key generated to the particular file access when the owner grants permission to the file request and he/she download the file data. This secret key is then validated and then he/she can download the file data.



Secret key mail from Secure Data Sharing !!!

blockchainfiles.2728@gmail.com
to me

The secret key for the file bc.png is: 836987

Figure 5. Secret private key generated to the particular file access

TABLE I

TEST CASE FOR ALL PHASE

Test ID	Test Cases	Expected Result	Actual Result	Result Status
TC - 01	Select file path to upload files to the cloud	File uploaded message should be displayed.	Message is successfully displayed.	**Pass**
TC - 02	Select file download option to download the file from the cloud.	Should show the list of files in the cloud to download.	Successfully shows the file list for download.	**Pass**
TC - 03	Select Key download option to download the encryption key file	Prompts to save the encryption file.	Successfully saved.	**Pass**
TC - 04	Decryption of file	Asks for downloaded cloud file and encryption key file and the key value sent to the mail	Successfully displays the fields as on expected result.	**Pass**
TC - 05	File forwarding	Select file to send with recipient mail ID	Successful	**Pass**
TC - 06	If User ID is not correct	Display message “Enter the correct user ID”.	“*” is displayed	**Fail**

User Acceptance Testing (UAT) is a vital step in any project that necessitates active engagement from the end user. It also guarantees that the system meets the functional specifications as described in the table 1.

V. CONCLUSION

The designed Interface strengthens data privacy and data security by the process of encryption. The encrypted file block data is distributed across the nodes of the network. On accomplishing the designed system as it makes use of the Data Encryption Standard DES 64bit cryptographic encryption algorithm for the process of encryption and to enhance the confidentiality of users' file data. Block data that is already encrypted is shared across several nodes of the network using the MultiChain protocol. The interface provides access for legitimate users to download the required file by the mechanism of a grant, revoke and reject by the owner of file data. On approval of the file request by the owner of the data the authorized user can access the requested file. The designed system tries to resolve the problems related to unauthorized access for file data, confidentiality, reliability, and dependability. As SDN network plays a major role in node failure detection for various scenarios and attack detection based on entropy values in several scenarios.

VI. FUTURE SCOPE

The future scope of the proposed system can be implemented, using a scheduling algorithm that can include data that could be accessed many times by multiple legitimate users. This helps to make sure the frequently accessed files to the owner of the data and files accessibility is made easier to the authorized users whenever needed. Centralized cloud storage can also be implemented with the backend SDN network for secured data transactions of the file data and to keep track of attacks to access the file data by unauthorized users.

VII.REFERENCES

[1]. Srikanta Pradhan, Sukumar Nandi, Somanath Tripathy, “Blockchain-based Security Framework for P2P File sharing system”. IEEE (ANTS) 2018

[2]. Yuke Liu,” A Blockchain-based secure cloud files sharing scheme with fine-grained access control” IEEE, International conference on networking and network applications IEEE,2018

[3]. Lee, Bih-Hwang, Ervin Kusuma Dewi, Muhammad Farid Wajdi,”Data security in cloud computing using AES under HEROKU cloud.” 2018 27th wireless and optical communication , IEEE.

[4]. Chaitanya Rahalkar, Dhaval Gujar, “Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data IntegrityIEEE 2019 International Conference on Advances in Computing, Communication and Control (ICAC3).

[5]. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, “Study on Data Security Policy Based On Cloud Storage IEEE 2017 3rd International Conference on Big Data Security on Cloud

[6]. Shubham Desai, Onkar Deshmukh, Harish Choudhary, Rahul Shelke ” Blockchain-based secure data storage and access control system using cloud”, IEEE 2019 , ICCUBEA .

[7]. Cachin Christian,” Architecture of the hyperledger blockchain fabric”, 2016.

[8]. Subarna Shakya, Sadhu Ram Basnet ” Blockchain Security Over Software Defined Network”. IEEE, 2017

[9]. Yue Zhang, Weng Jian , ” Secure Software-Defined Networking based on Blockchain”, 2019

[10]. Ruj, Sushmita, Anirban Basu , Mohammad Shahriar Rahman , Shinsaku Kiyomoto “A Secure Decentralized Storage Framework on Blockchain” 2018 IEEE International Conference on Advanced Information Networking and Applications (AINA).IEEE,2018

[11]. BhavinKumar Kothari, Shakthi Mudaliar and Sabestin Nadar, “Securing IoT with Blockchain”, Proceedings of the Fifth International Conference on Inventive Computation Technologies (ICICT-2020), IEEE 2020.

[12]. Manisha Nehe, “A survey on Data Security using Blockchain: Merits, Demerits, and Applications”.IEEE, 2019 International Conference on Recent Advances in Energy-Efficient Computing and Communication (ICRAECC)

[13]. Barnabas Sandor, David Janos Feher, Log File Authentication and Storage on Blockchain

Network. IEEE 16th International Symposium on Intelligent Systems and Informatics, 2018.

[14]. Dr. V. Suma," Security and Privacy Mechanism using Blockchain", Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019) Vol.01/ No. 01

[15]. Meet Shah, Mohammedhasan Shaikh, Grinal Tuscano, " Decentralized Cloud Storage using Blockchain", Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020)(48184), IEEE 2020

[16]. Saifull ah Khan, Akanksha Jadhav, Indrajeet Bharadwaj, "Blockchain and the Identity based Encryption Scheme for High Data Security". Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020).

[17]. Sarra Boukria, Mohamed Guerroumi, Imed Romdhani " Blockchain-Based Controller Against False Flow Rule Injection In SDN ." Performance Evaluation of Communications in Distributed Systems and Web-based Service Architectures.IEEE,2019 Symposium on computers and communications (ISCC).

Cite this article as :

Anusha M, Prof. Thyagaraja Murthy A, "The Security of a Blockchain-Based File System in a Software Defined Network Framework", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 5, pp. 22-29, September-October 2021. Available at doi : https://doi.org/10.32628/IJSRSET218481
Journal URL : https://ijsrset.com/IJSRSET218481