International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

PUBLIC INTEGRITY VERIFICATION FOR CLOUD STORAGE USING BLOCKCHAIN

K. Sai Uday Kumar[1], R. Raghavendra Naik[2], K. Deekshith[3], Golda Dilip[4]

[1,2,3]B. Tech, Dept. of CSE, SRM Institute of Science and Technology, Tamil Nadu, India
[4]Associate Professor, Dept. of CSE, SRM Institute of Science and Technology, Tamil Nadu, India

---

Abstract - *With the introduction of cloud storage concept, managing information has become quite easier for the data users.. Here, in this paper, we tend to come up with a replacement conception with the employment of the blockchain technology i.e., certificate less public verification theme against procrastinating auditors. The auditor records each verification as a transaction and this is serves as the main ideology. So as soon as the auditor audits and upload the data, the verification result is time-stamped and the users can observe the auditors behaviour. Moreover, CPVPA (certificate less public verification theme against procrastinating auditors) is made on certificate less cryptography. So, one does not need to worry about managing the certificates from any third party certificate authority.*

Keywords - Blockchain, time sensitive, CPVPA, transactions, verifications.

1. INTRODUCTION

In the cloud storages, the user can store data over it and they can access their data wherever they are and whenever they want through the internet [1]. Because of this nature of cloud storage, users need not spend on local storages such as hard disks and this will be economical [3]. Though it proves to be advantageous to the user, there arises a vital problem with it i.e., the security issue [6]. One amongst those problems, foremost vital security considerations is data integrity. Once the data is stored in the cloud servers, the user would have no physical over it which is quite opposite to the old method of maintaining data which would prove costly. Hence, users are perpetually distressed regarding the data integrity, i.e., whether data stored in the cloud servers is well maintained on not. The integrity of information stored in this way is being placed in danger practically. For instance, the data may be corrupted and hidden to maintain its prestige or could be stolen and misused for other purposes for the sake of their profits . Moreover, an external individual could manipulate the stored information as his way to gain malicious advantages over the user who is the actual owner for benefits. Hence, the sporadic verification of the cloud stored data is very essential. The verification process can be carried out on their own by the users. Public verification schemes allows users to maintain data integrity through an avid third party auditor. This auditor thoroughly check the data integrity very often and informs about the file corruption to the users. But, current schemes think that auditor is capable and honest in doing his job. If their assumption is wrong all there are going to be useless. For instance, the auditor can construct false report about the verification and send it to the user. So, the auditor here is just about non-existent and works irresponsibly. Moreover, these false reports can be generated and used for the sake of profits [7]. Hence, the user has to observe the auditors behaviour sporadically so that nothing goes wrong [2]. So, in order to make this possible the auditor must save and upload each report of the verifications he perform such that the user can observe his behaviour.

1.1 Blockchain

Blockchain can be defined as a decentralized network where the data is stored in the form of block and are linked together. Blockchain technology is greatly used in cryptocurrency such as Bitcoin. Each block contains 4 elements : Previous Hash, Transaction details, Nonce and Hash address of the block. When a new block is introduced in the chain a nonce is randomly generated. With the help of this nonce the hash address of the current block is created using the hashing functions such as SHA - 256 (Secure Hashing Function) where 256 refers to as the digest length. It works independently without the involvement of any third party. For each and every block in the chain, the value of current blocks previous hash and previous block current hash will be the same. So, in this way one can find out whether anyone has tried to steal the data. So, it can be used as a proof against meddling.

2. EXISTING SYSTEM

In the existing systems, the user i.e., the data owner stores his information in the cloud storages. There exists a third party auditor who works for the user and sporadically audits the user files for data integrity. If the file is corrupted the auditor must inform about it to the user as early as possible to avoid any issues to be faced by the users. Here the Public Key Infrastructure scheme is used. So the auditor must attain a certificate from any of the third party certificate authorities. Here, based on the users' details the key generation center generates a private key for the user [2]. In this kind of systems the auditor may not work properly which makes way for may difficulties to the users. Additionally the certificate management would become an issue as it is time consuming and expensive.

3. CHALLENGES OF EXISTING SYSTEM

- Make the third party auditor to work punctually and perfectly without the aid of any other person. We cannot completely trust the third party auditor to perform his duty correctly as suggested. But many of the current systems leave this job completely on the auditor as they trust him. In the worst case scenario the auditor may not perform the verification of data integrity in time which may be a threat as the data may be corrupted and would be difficulty to retrieve the corrupted data by then. He may not perform the verification and generate false report to the user as if he checked the information which will be risky. It would be difficulty such carelessness with the current schemes.

- Eliminate the use of certificates from a third party authorities. Almost all of the current techniques which are available are using methods which require certificates from the third party authorities. This may be a difficult and time-consuming task to manage these certificates. Additionally, they might even be expensive.[5]. So, the alternative to these situations would be an auditor who is employed without the use of any certificates which will be of lesser cost and easier to manage when compared to the previous scheme. All this have to be achieved with consistency and security

4. PROPOSED SYSTEM

In the proposed system, we employ a new technique called as certificate less public integrity verification scheme (CPVPA) [2]. Here, there is no need to manage certificates from the third party certificate authorities. So, this will be economical when compared to the existing systems. Also that, the blockchain technique used here enables the user to observe the behaviour of the auditor after auditing as the auditor must embed each verification result as a transaction in the blockchain. Since it istimesensitive, the time stamp is present on each verification upload by the auditor.

5. COMPONENTS

5.1 Data Owner

The Data Owner is incharge of the data within a particular Domain. They are accountable to confirm that the data among their Domain is ruled across systems and features of the business. Data owners typically are a part of committee, either as voting or non-voting members.

5.2 Cloud Storage

A cloud storage is a kind of storage in contrast to the traditional, ancient storage methods such as hard disks, Pen Drives which exists virtually unlike the previously mentioned physically existing devices. The examples of cloud storages are Google Drive, One Drive, i Cloud, Mi Cloud etc. These cloud storages are under the control of the respective cloud service providers on their servers. Though these cloud server the user can access the data he required anytime or anywhere.

5.3 Key Generation Center

The key might be a string of random alphanumeric characters or simple a string of either of them. It is generate by the key generation center which is in control of the admin of the system. Here, we use Java Random Class to generate the key to send it to the user to upload his file to the mail he enters while requesting for the key. The key is sent using the Simple Mail Transfer Protocol (SMTP).

5.4 Third Party Auditor

A third party auditor is the one who check the data files uploaded by the data user for the data integrity sporadically. If there is any issue with the file or it is corrupted he informs to the data user as soon as possible to minimize the risks to the data user. He is employed when an organization or a company requires for the Quality Management Systems (QMS). He has to work perfectly, punctually and periodically.

5.5 Admin

Admin is the one who maintains the database. He responds to the request of the data users who wants to download any of the files which are uploaded in the database by the auditor after auditing the files. The data user requests for the key to download particular files in the database he responds to it by generating the key and sending it to the given mail ID by the data user.

5.6 Data User

Data users are the ones who wants to use the data which are uploaded by the third party auditor in the database by downloading the files. In order to download the files he requires a key which has to be given by the admin. After he request the admin for a key to download a particular file, the admin processes his request. He receives the key to the given mail ID he entered during the request.

6. MODULE DESCRIPTION

6.1 User Interface Design

The user i.e., the data owner must register as a data owner before logging in. So, this provides security to the data owners as others may intrude into his account. The user must provide details such as his name and email while registering. To log in, the user must enter his user name and

password. If it matches he can proceed to upload the file or else he will be rejected.

6.2 Data Owner Request for Key

Here, data owner will register, login and request for a key to upload the files. Data owner will request key center for the key

6.3 Key Center Generates the Key

In this module, key center checks the data owner list or profile. If the data owner is a valid person then the key center generates a key for uploading a file. Otherwise it can't generate a key.

6.4 Data Owner Upload the File

In this module, data owner will logs in and have to upload his files i.e. to a pdf or a text file. The uploaded file gets encrypted and stored in the database. While uploading a file, key also will be stored there.

6.5 Sends the File for Auditing

Uploaded file will be sent to the auditor for checking purpose. In this module separate auditing team will be present for checking and correcting the files. All uploaded files to be sent here for auditing.

6.6 Auditor Check the File

Auditor checks all files uploaded by all data owner with the file key. Auditor can block the file when there is an incorrect file or an incorrect user.

6.7 Data User Requests for the File

Here data user will register, login and request to download some files which are uploaded. Data user can view the all files uploaded in the database. They click on request button and a request will be sent to admin.

6.8 Admin Responds to the Request

Admin receives notification after getting log in.Here there will be the request sent by other data user. If they accept, the key will be sent to the data user to download the file. The key will be sent to the requested data user for downloading file with acceptance notification. Otherwise it will be rejected.

6.9 Admin Maintains the Data

Here the admin will login and he can view the files uploaded by data owner, and Admin manages all files uploaded by all data owners in the database

6.10 Data User Download the File

Here the response notification will be received with the key. The file key is sent by the admin in the back end for downloading the file. When he downloads the file it asks for the key. If it matches, the file will be downloaded.

7. SYSTEM ARCHITECTURE

The system architecture "Figure 1", is used to explain the working of the software or module according to its principles, concepts, and characteristics which are logically related and consistent with each other. The design of the approach has the attributes, properties, and functions that solve as many challenges as possible or the potential provided by the job method and the definition of the life cycle and applied by the technologies.

This is an abstract, conceptual-based, regional, and program-oriented word to attain the goal and work-life span of the method. System architecture also concentrates on the high-end structure in the system and system elements. One architecture can be used for representing the common structures, pattern and set of requirements for similar classes and families.

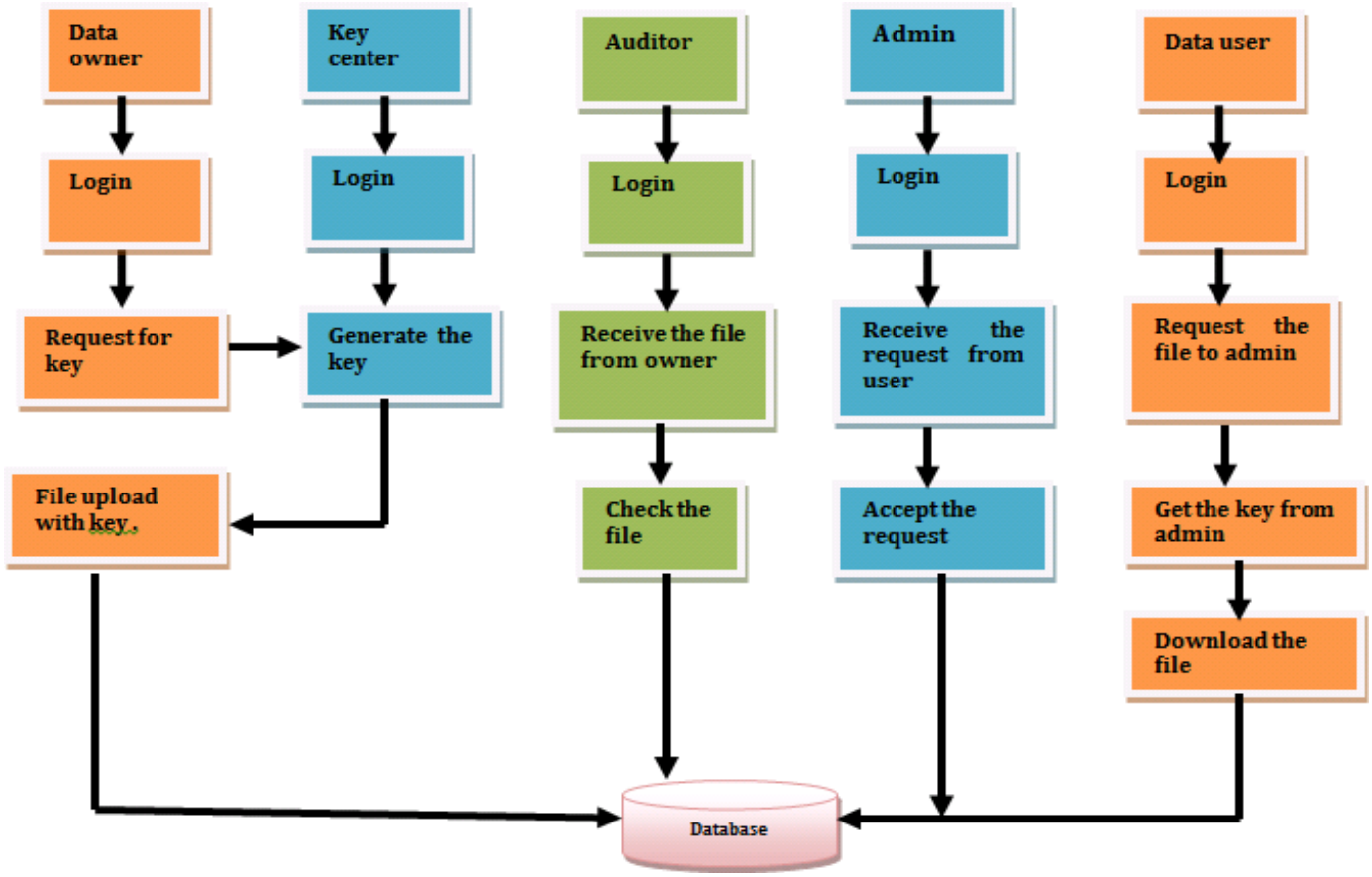

Fig-1: Architecture Diagram

8. ALGORITHMS USED

8.1 AES

It is an encryption algorithm which uses same key for encryption as well as decryption. It has key sizes of 128 bits, 192 bits and 256 bits and the number of round for each size is as follows:

- 10 rounds for 128 bits
- 12 rounds for 192 bits
- 14 rounds for 256 bits

It is much faster and stronger than DES. Encryption is done by following the process of sub bytes, shifting rows, mixing columns and adding round key and this process runs for certain number of rounds for each of the three different variants of the algorithm. The AES 256 algorithm is the strongest of all and has not yet been broken. The encrypted data is stored in the form of 4*4 matrix as show in "Figure 2" and later decrypted to plain text of the original form.

In this proposed paper, it is used for the secure transformation of the information or data between the various components involved such as from Data Owner to Auditor and from Auditor to Cloud Storage so that the intruders cannot make use of this data

The below diagram "Figure 2.", represents the AES arrangement of the letters in the sentence 'This is a text…'.

	0	1	2	3
0	T		a	s
1	h	i		t
2	i	s	t	.
3	s		e	.

Fig-2: AES Block Diagram

8.2 SHA-256

It is a hash function which is used to generate hash values for the blocks in the blockchain where 256 represents the size of the hash value as shown below in "Figure 3". It never changes irrespective of the input data whether it is 'abc' or

an entire textbook and the value will never be the same for two different inputs. In the blockchain to get the hash value, the data of the block is passed through this algorithm to get the hash code of that particular block. The SHA has 6 other variants in their family. It can be executed in Java using the MessageDigest class.

Here, in this paper we used SHA as a hashing algorithm to generate random hash values while the auditor uploads the audited paper in the cloud storage for the Data Users to Download. These values ensure that the blocks of data are linked sequentially and that there was no manipulation done by the others. The hash values differ for different text data sent by the Data Owner, which in-turn is uploaded into the virtual data storages by the auditor once the checking is completed.

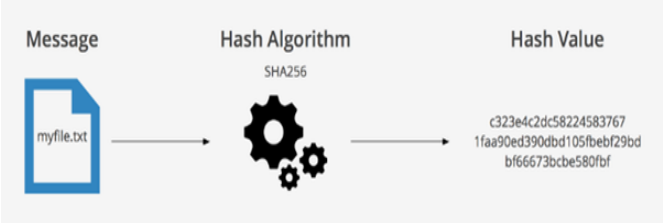

Fig-3: SHA-256 Overview

9. SNAPSHOT

The screenshot "Figure 4",of the web application proposed in this paper is the Main Menu of the application created using the JavaScript. From here the respective members of the system, such as Data Owner, Auditor, Admin and Data User must register and login to continue their operations

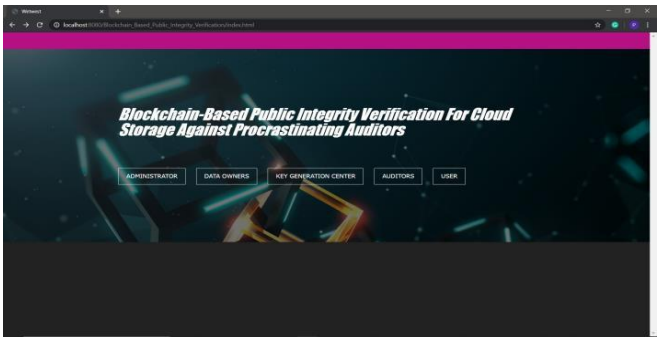

Fig-4: User Interface Screenshot

10. ADVANTAGES

Here, we utilised the CPVPA technique, so there will not arise a problems for managing a certification from any of the third party certificate authorities. So, our work becomes a bit easier and less complex here. Also that , as we employed the blockchain technique which is used when the auditor uploads the files after checking, the data user can find whether he is working properly in time as every transaction on the block chain gets time stamped.

11. FUTURE ENHANCEMENTS

For the long run work, we are going to examine a way to develop CPVPA on alternative frameworks. Developing CPVPA on alternative blockchain frameworks will spare vitality. Be that because it could, it needs an explained structure to accomplish a similar security guarantee while guaranteeing the high productivity. These remaining parts an open research issue that needs to be more investigated. we are going to likewise examine a way to use blockchain innovation to boost distributed storage frameworks as a way of security, execution, and utility.

11. CONCLUSION

In summation, we have presented a certificate less public verification scheme against the procrastinating auditor with the concept of CPVPA. With the use of onchain currencies such that whatever the verification is done by the third party auditor the verification result is reported as a transaction with the hash codes and time mention on it. Hence the user can observe the behaviour of the auditor. Moreover it is economical in nature as there will be no need to manage certification which is one of the disadvantages of the currently existing system. We have projected that it the utmost security when compared to the present available scheme for the above mention properties of the project system and also that it very consistent..

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyberphysical social systems," ACM Transactions on CyberPhysical Systems, vol. 3, no. 1, p. 8, 2018.
[2] F. Armknecht, J. Bohli, G. O. Karame, and W. Li, "Outsourcing proofs of retrievability," IEEE Trans. Cloud Computing, to appear, doi: 10.1109/TCC.2018.2865554.
[3] J. Li, H. Ye, W. Wang, W. Lou, Y. T. Hou, J. Liu, and R. Lu, "Efficient and secure outsourcing of differentially private data publication," in Proc. ESORICS, 2018, pp. 187–206.
[4] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. of ASIACRYPT, 2003, pp. 452–473.
[5] B .Wang, B. Li, H. Li, and f. Li "Cerficateless public auditing for data integrity in the cloud" in Proc of IEEE CNS, 2013, pp. 136-144
[6] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacypreserving attribute-keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116– 131, 2017.
[7] W. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "SCLPV: Secure certificateless public verification for cloud- based cyber-physical- social systems against malicious auditors," IEEE Trans. Computa- tional Social Systems, vol. 2, no. 4, pp. 159–170, 2015.