BLOCKCHAIN-BASED PUBLIC INTEGRITY VERIFICATION FOR CLOUD STORAGE AGAINST PROCRASTINATING AUDITORS

PA. Dhakshayeni[1], P. Tamil vanan[2], B.P. Tamizh selvan[3], V. Vijaya murugan[4]

[1]Assistant Professor, Dept. of IT, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu
[2, 3, 4]B.TECH., Dept. of IT, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu

---

Abstract - *The preparation of cloud storage services has important edges in managing knowledge for users. However, it conjointly causes several security issues, and one amongst them is knowledge integrity. Public verification techniques will change a user to use a third-party auditor to verify the info integrity on behalf of her/him, whereas existing public verification schemes square measure prone to procrastinating auditors WHO might not perform verifications on time. moreover, most of public verification schemes square measure created on the general public key infrastructure (PKI), and thereby suffer from certificate management downside. during this paper, we tend to propose the primary certificate less public verification theme against procrastinating auditors by victimization blockchain technology. The key plan is to need auditors to record every verification result into a blockchain as a dealing. Since transactions on the blockchain square measure time-sensitive, the verification will be time-stamped when the corresponding dealing is recorded into the blockchain, that permits users to see whether or not auditors perform the verifications at the prescribed time. Moreover, CPVPA is constructed on certificate less cryptography, and is free from the certificate management downside. we tend to gift rigorous security proofs to demonstrate the safety of CPVPA, and conduct a comprehensive performance analysis to point out that CPVPA is economical. Key Words*: Blockchain technology, key generation, public verification, CVPA.

1. INTRODUCTION

With cloud storage services, users supply their data to cloud servers and access that data remotely over World Wide Web. These services supply users Associate in nursing economical and versatile because of manage their data, whereas users ar free from serious native storage costs. Although users relish nice blessings from these services, data outsourcing has together incurred necessary security issues. One of the foremost necessary security problems is data integrity. In distinction to ancient data management paradigm, where users store their data domestically, users would not physically own their data once having outsourced the data to cloud servers. Therefore, users ar unceasingly distressed regarding the data integrity, i.e., whether or not or not the outsourced data is well maintained on cloud servers. The integrity of outsourced data is being place in peril in apply. As an example, the cloud servers would possibly unceasingly conceal incidents of data corruption for good name, or would possibly delete a section of data that is never accessed to reduce the storage costs. Moreover, Associate in Nursing external resister would possibly tamper with the outsourced data for cash or political reasons. Therefore, the integrity of outsourced data need to be verified periodically. The verification is also performed by the users themselves. Public verification techniques amendment users to supply the data integrity verification to a fervent third-party auditor. The auditor periodically checks the data integrity, and informs the users that the data might even be corrupted once the checking fails. In most of public verification schemes, the auditor is assumed to be honest and reliable. If the auditor is compromised, these schemes would be invalid. as an example, Associate in Nursing unaccountable auditor would possibly unceasingly generate AN honest integrity report whereas not taking part in the verification to avoid the verification costs. In such the manner, the auditor is sort of non-existent. moreover, a malicious auditor would possibly conspire with the cloud servers to urge a bias verification result to deceive the users for profits. to substantiate the protection inside the case that the auditor is compromised, the users ar required to audit the auditor's behaviors once each verification and additionally the auditor records the information accustomed verify the data integrity, that allows the user to audit the validity of the auditor's behavior.

1.1 What is Blockchain?

A block chain, may be a growing list of records, known as blocks, that area unit connected victimization cryptography. Every block contains a cryptologic hash of the previous block, a timestamp, and dealings information (generally drawn as a Merkle tree). A blockchain is usually managed by a peer-to-peer network jointly adhering to a protocol for inter-node communication and verifying new blocks. Once recorded, the info in any given block can not be altered retroactively while not alteration of all subsequent blocks, which needs agreement of the network majority. Though blockchain records don't seem to be unalterable, blockchains could also be thought of secure intentionally and exemplify a distributed ADPS with high Byzantine fault tolerance.

Localized agreement has thus been claimed with a blockchain.

2. MODULES DESCRIPTION

2.1 USER INTERFACE DESIGN

This is the primary module of our project. The necessary role for the user is to maneuver login window to user window. This module has created for the protection purpose. During this login page we've got to enter login user id and watchword. It'll check username and watchword is match or not (valid user id and valid password). If we tend to enter any invalid username or watchword we tend to can't enter into login window to user window it'll shows error message. Therefore we tend to square measure preventing from unauthorized user moving into the login window to user window. It'll give an honest security for our project. Therefore server contain user id and watchword server conjointly check the authentication of the user. It well improves the protection and preventing from unauthorized user enters into the network. In our project we tend to square measure victimization JSP for making style. Here we tend to validate the login user and server authentication.

2.2 DATA OWNER REQUEST FOR KEY

Here data owner will register and login and request for key to upload the files. With the use of key only he can upload a file in the cloud. Data owner will request for key to the key center.

2.3 KEY CENTER GENERATES THE KEY FOR THE OWNER

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

2.4 DATA OWNER UPLOADS FILE WITH THAT KEY

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

2.5 SEND FILE FOR AUDITING

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

2.6 AUDITOR CHECKS 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.

2.7 DATA USER REQUEST FOR FILE

Here data user will register and login and request for some files uploaded by the data owner. Data user can view the all files uploaded in the database. Files will be viewed as a encrypted text to the data user. They click on request button it will be sent to admin.

2.8 ADMIN ACCEPTS THE REQUEST

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

2.9 ADMIN MAINTAIN 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 the file key. Admin maintains the files in the database.

2.10 DATA USER DOWNLOAD THE FILE

Here the response notification will be received with the key. The file key sent by admin in the backend for downloading the file. When he downloads the file it asks for entering the key. If it is matched it will be downloaded otherwise key will be wrong.

3. SYSTEM TECHNIQUES

Technique: AES

AES has a place with a group of figures known as square figures. A square figure is a calculation that encodes information on a every square premise. The size of each square is typically estimated in bits. AES, for instance, is 128 bits in length. This means, AES will work on 128 bits of plaintext to create 128 bits of figure content. Encryption works by taking plain content and changing over it into figure content, which is comprised of apparently arbitrary characters. Just the individuals who have the uncommon key can unscramble it. AES utilizes symmetric key encryption, which includes the utilization of just a single mystery key to figure and decode data. AES-256 (Advance Encryption Standard) with 256 piece key is the most development cryptographic calculation till date and not have been broken at this point. The Advanced Encryption Standard, or AES, is to secure grouped data and is actualized in programming and equipment all through the world to encode touchy information.

SYSTEM ARCHITECTURE:

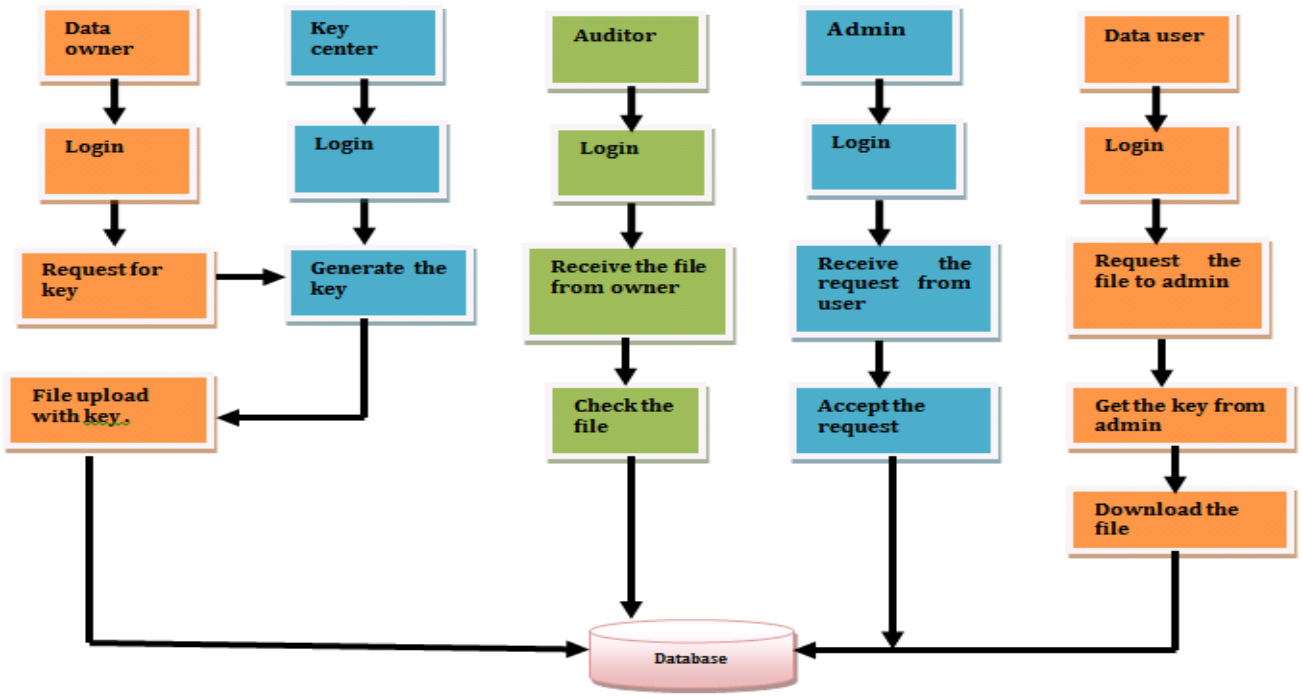

Fig -1: Architecture Diagram

System design is that the abstract model that defines the structure, behavior, and a lot of views of a system. associate design description may be a formal description and illustration of a system, organized during a means that supports reasoning concerning the structures and behaviors of the system. A system design will carries with it system parts and therefore the sub-systems developed, which will work along to implement the system. There are efforts to formalize languages to explain system design; together these square measure known as architecture description languages.

HARDWARE REQUIREMENTS

- **PROCESSOR** : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
- **RAM** : 4 GB DD RAM
- **MONITOR** : 15" COLOR
- **HARD DISK** : 40 GB

SOFTWARE REQUIREMENTS

- **FRONT END** :J2EE (JSP, SERVLETS) JAVASCRIPT
- **BACK END** : MY SQL 5.5
- **OPERATING SYSTEM** : Windows 07
- **IDE** : Eclipse

SNAPSHOT

Fig-2 Welcome page of the application

ADVANTAGES

Here, we develop CPVPA on a settled and generally utilized blockchain framework, as opposed to a recently made one. Besides, CPVPA is based on the certificate less cryptography and maintains a strategic distance from the declaration the executive's issue.

APPLICATION

We propose an easy nevertheless economical model, known as Dual sentiment analysis (DSA), to deal with the polarity shift downside in sentiment classification. By mistreatment the property that sentiment categoryification has 2 opposite class labels (i.e., positive

and negative), we tend to 1st propose a knowledge enlargement technique by making sentiment reversed reviews. the first and reversed reviews area unit made during a matched correspondence.

FUTURE ENHANCEMENT

For the future work, we will examine how to develop CPVPA on other blockchain frameworks. Since the principle downside of verifications of work (PoW) is the vitality utilization, developing CPVPA on other blockchain frameworks (e.g., proofs-of-stake-based blockchain frameworks) can spare vitality. Be that as it may, it requires an explained structure to accomplish the same security ensure while guaranteeing the high productivity. These remaining parts an open research issue that ought to be further investigated. We will likewise examine how to use blockchain innovation to improve distributed storage frameworks as far as security, execution, and usefulness.

CONCLUSION:

In this paper, we've got projected a certificate less public verification theme against the procrastinating auditor, particularly CPVPA. CPVPA utilizes the on-chain currencies, wherever every verification performed by the auditor is integrated into a dealings on the blockchain of on-chain currencies. what is more, CPVPA is free from the certificate management downside. the safety analysis demonstrates that CPVPA provides the strongest security guarantee compared with existing schemes. we've got conjointly conducted a comprehensive performance analysis, that demonstrates that CPVPA has constant communication overhead and is economical in terms of computation overhead.

REFERENCES

[1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," ACM Transactions on Cyber-Physical Systems, vol. 3, no. 1, p. 8, 2018.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.

[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] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Generation Computer Systems, vol. 93, pp. 327–337, 2019.

[5] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870–885, 2019.