IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10751

Efficient Dynamic Auditing for Cloud Storage Security and Integrity of Data in Cloud

Varsha[1], Vijaya bharathi[2], A.S.Balaji[3]

Student, B.E. Computer Science and Engineering , Anand Institute of Higher Technology, Chennai, India[1,2]

Assisstant Professor, CSE, Anand Institute of Higher Technology, Chennai, India[3]

Abstract : The cloud security is one of the important roles in cloud, here we can preserve our data into cloud storage. More and more clients would like to store their data to PCS (public cloud servers) along with the rapid development of cloud computing. Cloud storage services allow users to outsource their data to cloud servers to save local data storage costs. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. In our system we are using checksum Algorithm for our own auditing based on the token generation. Using this key generation technique, we compare the key values from original keys and we can find out the changes in the file. The content will be stored and also encrypted in the cloud server. Here we are using block chain double hashing algorithm for splitting the original file into three different files and to store that files in three different locations in cloud. The Encryption and Decryption Technique are done by using Cryptographic Hashing techniques. Anyone can download the files from the server with file owner permission. At the time of download key will be generated (code based key generation) and it will send to the file owner. We can download that file by using verification key.

Keywords: Data security and privacy, Advance Encryption Standard Technique (AES), Blockchain Technology.

I. INTRODUCTION

Distributed computing has been envisioned as the accompanying creation information development (IT) plan for endeavors, due to its broad summary of unparalleled inclinations in the IT history: on-ask for self-advantage, inescapable framework get to, zone self-choosing resource pooling, quick resource adaptability, use based assessing and transference of peril.

As an aggravating development with huge consequences, distributed computing is changing the specific method for how associations use information advancement. One fundamental piece of this standpoint changing is that data are being united or outsourced to the. From customers' view, including together individuals and IT tries, securing data remotely to the in a versatile on-ask for strategy bring engaging focal points: landing of the weight for storage space organization, vast data access with put self-sufficiency, and avoidance of advantages costs on hardware, programming, and staff frameworks of help, etcetera

While distributed computing make these compensation more captivating than some other time in ongoing memory, it also passes on new and testing security risks to customers' outsourced data. As organization providers (CSP) are part administrative components, data outsourcing is truly surrendering customer's last control more than the fate of their data. As an issue of first significance, in spite of the way that the structures underneath the are altogether more powerful and trustworthy than individual enlisting devices, they are still before the broad assortment of both inside and outside risks for data respectability.

As a problematic innovation with significant ramifications, processing is changing the plain idea of how organizations utilize data innovation. One essential part of this outlook changing is that information Are being brought together or outsourced to the . From clients' point of view, including the two people and IT ventures, putting away information remotely to the in an adaptable on-request way brings engaging advantages: alleviation of the weight for capacity administration, general information access with area freedom, and evasion of capital consumption on equipment, programming, and work force systems for upkeeps, and so on.

1.1 OBJECTIVE

Objective of proposed system to implement an autolysis of data system and data privacy are as follows:- specialist organizations (csp) are separate authoritative elements, information outsourcing is really giving up client's definitive control over the destiny of their information. Thus, the rightness of the information in the is being put in danger because of the accompanying reasons.

1.2 SCOPE

The system can be used for security purpose in the cloud server. It is also used for sharing the file securely and can be

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10751

accessed behalf of the data owner. It is used in several applications such as:

- Medicine
- Biodiversity information systems
- Digital libraries
- Crime prevention
- IT industry
- Commercial purpose
- Education Applications

II. ANALYSIS

3.1 SYSTEM ANALYSIS

System Analysis is a combined process dissection the system responsibilities that are based on problem domain characteristics and user requirement.

3.1.1 Problem Definition

Cloud provide security and storing data and accessing that data from the Internet instead of Using Traditional hardware for most of the operations. But those existing system provides only security and Sharing of data to multiple users over cloud without permission of data owner. Therefore, the proposed system lead to advance security like time validity and private key is sent via email to particular user when data owner upload and share the file in cloud. This leads to improve efficiency in increasing level of security and hacking can be minimized.

3.1.2 Existing System

In open condition, most customers transfer their information to PCS and check their remote information's trustworthiness by Internet. At the point when the customer is an individual administrator, some reasonable issues will happen. Here outsider open inspecting plan for the recovering code-based capacity. To take care of the recovery issue of fizzled authenticators without information proprietors, if these information can't be handled in the nick of time, the supervisor will confront the loss of financial intrigue.

In request to keep the case happening, the supervisor needs to designate the intermediary to process its information. In PKI (open key foundation), remote information uprightness checking convention will play out the declaration administration. When the director appoints a few elements to play out the remote information honesty checking, it will bring about impressive overheads since the verifier will check the authentication when it checks the remote information trustworthiness.

Disadvantages of Existing System:

- In open condition, most customers transfer their information to PCS and check their remote information's trustworthiness by Internet. At the point when the customer is an individual supervisor, some useful issues will happen.
- The calculation overhead of check by the reviewer straightly increments with the span of the confirmed informational collection.
- Here outsider open reviewing plan for the recovering code-based capacity. To take care of the recovery issue of fizzled authenticators without information proprietors, if these information can't be prepared in the nick of time, the supervisor will confront the loss of monetary intrigue.
- In request to keep the case happening, the supervisor needs to appoint the intermediary to process its information. In PKI (open key framework), remote information uprightness checking convention will play out the declaration administration.
- When the chief delegates a few substances to play out the remote information honesty checking, it will acquire extensive overheads since the verifier will check the authentication when it checks the remote information uprightness.

3.1.3 Proposed system

An efficient cloud scheme with data in been made. Here we are using the erasure code technique for distribute the data to locations and access the data from. User can register and login into their account. Provided an option to store, share and access the data from storage. Here we are using the double ensured scheme for storing data into the. Cloud.First is your data or file split into multiple parts and it will store into different server locations. Each and every file generates the key-code for auditing. Then second is each and every split file will encrypt before store into different locations. The shared users can edit the file in the with file owner's permission. That file eligible of own public auditing. Search and download the files, at the time of download user should use the security key. As an authentication success it will be decrypt and combine to get the original data from.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10751

Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based storage.

Advantages of Proposed System*:*

- Compared to a lot of its predecessors, which only provide binary results about the storage state across the cloud servers, the challenge-response protocol in our work more provides the localization of data error.
- Unlike most prior works used for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
- Extensive protection and act analysis demonstrate that the proposed scheme is extremely efficient and resilient beside Byzantine failure, malicious data modification attack, and even server colluding attacks.

III.SYSTEM DESIGN

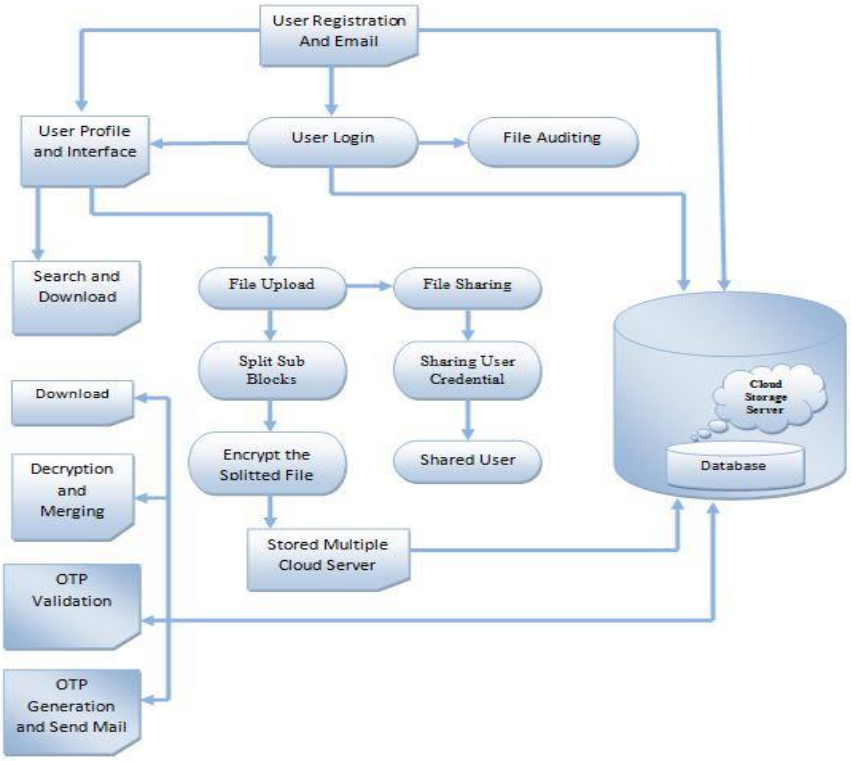

Figure 1.Overall Architecture Design

IV.MODULES

1. User Plug in
2. Uploading File
3. Secret key formation
4. File Allocation process
5. File Analyzing
6. File Loading process
7. Alert mail

5.2.1 User Plug-in:

In our Secure System we have a user friendly user interface to interact with our System. Every Act dual role as a data owner and data consumer while uploading file they are the owner of that file if they search other's file than they are the consumer. Users can create the account them self for that we have new pages, in that page we will get the details from

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10751

the user and we generate the account for the user's. We have authentication system; we only allow authorized users to access our System.

In our System we providing the easy file searching user's don't want to keep remember all uploaded file's exact name, for that we have given the keywords while uploading the files it will help to search the file easily.

5.2.2 Uploading File

Storing data over storage servers one way to provide data robustness is to replicate a message such that each storage server stores a message. Another way is to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different storage server. A storage server corresponds to an erasure error of the codeword symbol. As long as the number of servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process.

5.2.3 Secret Key Formation

Firstly the secret key will be generated as the initial step while uploading the file, every which is uploaded, will have unique secret key. This key will be taken as an identification of every file. The secret key which we are using is a three digit number we will make it use for both uploading and downloading. If the user want download some file and if he gives the download request the secret key of that file will be sent to the file owner of the file maybe he can share it.

5.2.4 File Allocation Process

In our application we can share a file to a registered user by providing basic credentials, with the sharing option it is necessary to provide authority to the shared user whether to view or edit the file. A user can view the shared file within the application without downloading it and the same is possible with the edit option.

5.2.5 File Analyzing

Auditing is the process of checking the file whether the original contents of the file is changed. This module provides the file owner auditing, this we achieve by generating tokens. The tokens are generated with the ASCII values of the characters in the file and these characters are stored in the DB while uploading the file. If a shared user edit's the file and saves it, again a new token will be generated and stored in the DB. If the initial token and the current token aren't same then a notification will be sent to the file owner.

5.2.6 File Loading Process

File downloading process is to get the corresponding secret key to the corresponding file to the user mail id and then decrypt the file data. The file downloading process re-encryption key to storage servers such that storage servers perform the re-encryption Operation. The length of forwarded message and the computation of re-encryption is taken care of by storage servers. Proxy re-encryption Schemes significantly reduce the overhead of the data Forwarding function in a secure storage system.

5.2.7 Alert Mail:

The uploading and downloading process of the user is first get the secret key in the corresponding user email id and then apply the secret key to encrypted data to send the server storage and decrypts it by using his secret key to download the corresponding data file in the server storage system's the secret key conversion using the Share Key Gen (SKA, t, m). This algorithm shares the secret key SKA of a user to a set of key servers.

V.RESULTS AND DISCUSSION

The result analysis was carried out by comparing the security provided by the cloud in existing and proposed systems. The proposed Secure Data Sharing Scheme provide key-policy attribute based encryption with time-specified attributes, a novel secure data autolysis of data scheme in cloud computing. The system is fully featured to provide more security in cloud and preventing the files from hacking.

VI.CONCLUSION

A protection saving open examining framework for information stockpiling security in processing. We use the homomorphism straight authenticator and arbitrary concealing to ensure that the TPA would not take in any information about the information content put away on the server amid the effective inspecting process, which not just wipes out the weight of client from the dreary and perhaps costly examining assignment, yet in addition reduces the clients' dread of their outsourced information spillage .

REFERENCES

[1] B. Wang, B. Li, and H. Li, (2015). "Panda: Public auditing for shared data with efficient user revocation in the cloud" IEEE Transactions on Services Computing.

[2] B.Wang, B. Li, and H. Li, (2013). "Public auditing for shared data with efficient user revocation in the cloud," Proceedings of IEEE INFOCOM

[3] B.Wang, B. Li, and H. Li, (2014) "Oruta: privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing.

[4] C. Wang, Q. Wang, K. Ren, et al, (2010) "Privacy-preserving public auditing for data storage security in cloud computing," Proceedings of EEE INFOCOM.

[5] Q. Wang, C. Wang, K. Ren, et, al, (2011). "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems

