Data Accuracy and Integrity for Cloud Storage Using Block Chain

Divya.J[1], K. Sathish [2]
[1] PG Scholar, [2] Assistant professor
Department of Computer science and Engineering,
Gojan School of Business and Technology, Redhills, Chennai

Abstract— Cloud security involves the methods and approaches that protect cloud computing environments against security risks. Cloud security procedures are implemented to check unauthorized access and to keep original data and applications in the cloud from emerging security threats. While storing and transferring some important data and file on cloud, both external and internal intruders can attack the file. When anyone try to hack at the cloud end, is not possible to break the different blocks stored in different locations on cloud because the security of our scheme is very strong. While using a cloud computing service provided by a public cloud provider, the integrity of the data and applications are verified by third party auditing, however in our scheme the data was held within a self-controlled network where the data owner justifies the outsourced file when shared with other users. Ensuring data security is the vital step to build a cloud service strategy. Block chain technology is used to store data by encrypting the files and distributing them across the decentralized network by making it harder for hackers to access the data. The private keys are controlled entirely by the user, making it impossible for a third party to access the files. Splitting the files makes it impossible to view the contents of the complete file, providing even more privacy. If anyone try to hack at the cloud end is not possible to break the different blocks because the security of our scheme is very strong. At the time of upload a key will be generated and it will send to the file owner. We can download that file by using verification key when it is shared by the owner. Any change in the content of the file can be identified by comparing the ASCII values which is initially stored in the database. Understanding your security responsibility is important to build a cloud security strategy.

Index Terms— Cloud computing, Block chain, Hash Function, Simple Mail Transfer Protocol.

1 INTRODUCTION

Dispersed registering has been imagined as the going with creation data advancement (IT) plan for attempts, because of its expansive outline of unmatched tendencies in the IT history: on-request self-advantage, certain structure get to, zone self-picking asset pooling, fast asset versatility, utilize based evaluating and transaction of danger.

As an irritating improvement with colossal results, disseminated registering is changing the strategy for how affiliations use data headway. One major piece of this stance changing is that information is being joined together or moved to the. From clients' view, including together people and IT has a go at, getting information from a distance to the in a flexible on-request system bring drawing in central focuses: arriving of the load for extra room association, huge information access with put independence, and evasion of benefits costs on equipment, programming, and staff structures of help, etc.

While appropriated processing makes these pay more spellbinding than later in continuous memory, it additionally gives new and testing security dangers to clients' revaluated information. As association suppliers (CSP) are part managerial parts, information rethinking is really giving up client's last control more than the destiny of their information. As an issue of first importance, regardless of the way that the designs under the are out and out more impressive and dependable than individual enrolling gadgets, they are still before the expansive combination of both inside and outside takes a chance for information decency.

1.1 CLOUD COMPUTING

Cloud Computing provides us means by which we can access the applications as utilities over the internet. It allows us to create, configure, and customize the business applications online. Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data center.

Small as well as large IT companies, follow the traditional methods to provide the IT infrastructure. That means for any IT company, we need a Server Room that is the basic need of IT companies.

- In that server room, there should be a database server, mail server, networking, firewalls, routers, modem, switches, QPS (Query Per Second means how much queries or load will be handled by the server), configurable system, high net speed, and the maintenance engineers.
- To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence.

1.2 HTML

The **Hyper Text Markup Language**, or **HTML** is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript.

Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document.

HTML elements are the building blocks of HTML pages. With HTML constructs, images and other objects such as interactive forms may be embedded into the rendered page. HTML provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. HTML elements are delineated by *tags*, written using angle brackets. Other tags such as **<p>** surround and provide information about document text and may include other tags as sub-elements. Browsers do not display the HTML tags but use them to interpret the content of the page.

HTML can embed programs written in a scripting language such as JavaScript, which affects the behaviour and content of web pages. Inclusion of CSS defines the look and layout of content. The World Wide Web Consortium (W3C), former maintainer of the HTML and current maintainer of the CSS standards, has encouraged the use of CSS over explicit presentational HTML since 1997.[2] A form of HTML, known as HTML5, is used to display video and audio, primarily using the **<canvas>** element, in collaboration with javascript.

1.3 Objective

Expert associations (CSP) are independent legitimate components; data rethinking is truly surrendering client's conclusive command over the predetermination of their data. In this way, the rightness of the data is being seriously jeopardized as a result of the going with reasons. Regardless of anything else, in spite of the way that the establishments under the considerably more historic and stronger than individualized registering devices, they are at this point defying the wide extent of both internal and outside risks for data decency.

2 Existing system

Several critical security problems still exist when data are outsourced to cloud storage. The idea of making use of multiple clouds has been proposed by Bernstein and Celeste. However, this previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenario.

The semi trusted cloud server without true data cannot generate the correct data integrity proof. The data privacy is preserved against the TPA. There are several remote data integrities checking schemes have been presented. The remote data integrity checking scheme enables client to efficiently audit the integrity for outsourced data on cloud server without downloading them.

3 Proposed System

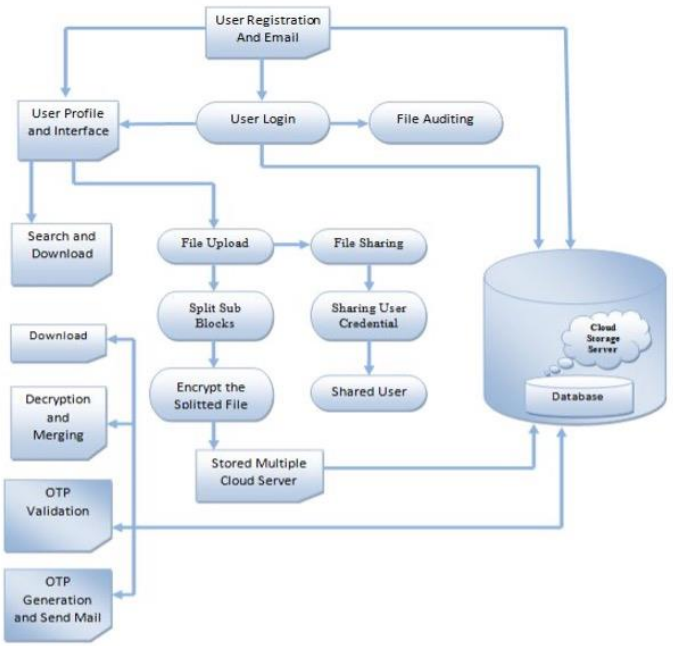
In our proposed system we upload and download file in a secure way by using the key generation technique. Using this technique, we compare the key values from original keys, and find out the changes in the file. The content will be stored and encrypted in the cloud server.

Here we are using block chain double hashing algorithm for splitting the original file into three different files and to store that file in three different locations in cloud. The Encryption and Decryption Technique are done by using Cryptographic Hashing techniques to download the file. Anyone can download the files from the server with file owner permission. At the time of download key will be generated and it will send to the file owner. Using the unique key, they can download the file

Advantages:

1. Enhanced Security
2. Data Integrity is preserved

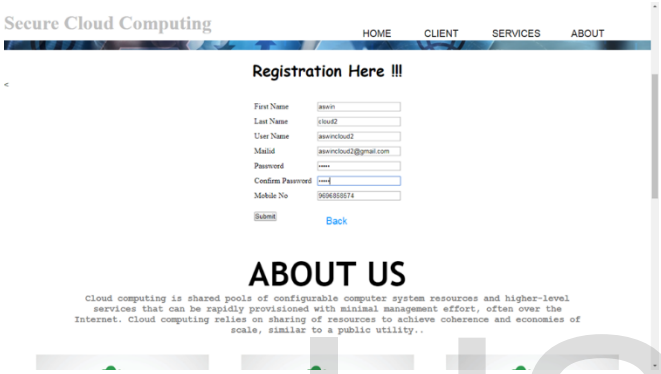
4 System Architecture



5 MODULES

5.1 User Plugin

In our Secure System we have an easy-to-understand UI to communicate with our System. Each client act double job as an information proprietor and information shopper. While transferring document they are the proprietor of that record assuming they search other's record than they are the customer. Clients can make the record them self for that we have new pages, in that page we will get the subtleties from the client, and we produce the record for the clients. We have verification framework; we just permit approved clients to get to our framework.



5.2 Uploading File

Putting away information over capacity servers one method for giving information strength is to reproduce a message to such an extent that every capacity server stores a message. Another way is to encode a message of k images into a codeword of n images by deletion coding. To store a message, every one of its codeword images is put away in an alternate stockpiling server. A capacity server relates to an eradication blunder of the codeword image. Assuming the quantity of servers is under the resistance limit of the deletion code, the message can be recuperated from the codeword images put away in the accessible stockpiling servers by the translating system to conquer the some this in our framework we transfer document that can contain a few significant messages. The client can download the record utilizing the key age methods, in the event that we can change in document whenever each time each the key qualities produced from unique keys and we can figure out the progressions in the record. The substance will be put away and encoded in the cloud server.

5.3 Secret Key Formation

The mystery key will, first and foremost, be produced as the underlying step while transferring the record. This key will be taken as a recognizable proof of every record. The mystery key which we are utilizing is a four-digit number we will make it use for both transferring and downloading. Assuming the client needs download some document and assuming he gives the download demand the mystery key of that record will be shipped off the record proprietor of the document perhaps he can share it.

5.4 File Allocation Process

In our application we can share a document to an enlisted client by giving fundamental qualifications, with the sharing choice it is important to give position to the common client whether to see or alter the record. A client can see the **common** record inside the application without downloading it and the equivalent is conceivable with the alter choice.

5.4 File Loading Process

Document downloading process is to get the relating secret key to the comparing record to the client mail id and afterward unscramble the document information. The doc-

ument downloading process, re-scramble the way to capacity servers to such an extent that capacity servers play out the re-encryption Operation. The length of sent message and the calculation of re-encryption is dealt with by capacity servers. Intermediary re-encryption Schemes essentially diminish the above of the information Forwarding capability in a safe stockpiling framework

5.5 Alert Mail

The transferring and downloading cycle of the client is first get the mystery key in the comparing client email id and afterward apply the mystery key to encoded information to send the server stockpiling and unscrambles it by utilizing his mystery key to download the relating information document in the server stockpiling framework's the mystery key change utilizing the Share Key Gen (SKA, t, m). This calculation shares the mystery key SKA of a client to a bunch of key servers.

5.6 File Analyzing

Evaluating is the method involved with checking the document whether the first items in the record is changed. This module gives the record proprietor evaluating, this we accomplish by creating tokens. The tokens are produced with the ASCII upsides of the characters in the document and these characters are put away in the DB while transferring the record. In the event that a common client alters the record and saves it, again another symbolic will be produced and put away in the DB. On the off chance that the underlying token and the ongoing token aren't same, then a notice will be shipped off the record proprietor.

6 Future Enhancement

• We furthermore grow our security protecting open assessing show into a multi-client setting, where the TPA can play out various looking at tasks in a group way for improved efficiency.

- In fast approaching we will upgrade the execution.

• In this structure we used simply satisfied records. In later we will consolidate the image, sound, video records. In our system the OTP shipped off owner mail id, coming up the client will get the OTP on compact by using the adaptable number.

7 Conclusion

A security saving open looking at system for data storing security in handling. We utilize the homomorphism straight authenticator and erratic hiding to guarantee that the TPA wouldn't take in that frame of mind about the data content set aside on the server amid the powerful assessing process, which not simply clears out the heaviness of client off the grim and maybe expensive looking at task, yet what's more diminishes the clients' fear of their rethought data spillage. Taking into account TPA may all the while manage different survey meetings from different clients for their re-appropriated data records, we furthermore grow our security safeguarding open looking at show into a multiuser setting, where the TPA can play out various assessing endeavors in a bundle way for better viability.

8 References

1. Identity-Based Privacy Preserving Remote Data Integrity Checking for Cloud Storage Jiguo Li , Hao Yan, and Yichen Zhang IEEE Systems Journal (Volume: 15, Issue: 1, March 2021)

2. Q.Wang, C. Wang, K. Ren, et al, "Enabling public auditability and data dynamics forstorage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
3. B.Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared datain the cloud," IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2014.
4. B.Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol.8, no.1, pp. 92-106, 2015.
5. H. Wang, and Y. Zhang, "On the Knowledge Soundness of a Cooperative ProvableData Possession Scheme in Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.1, pp. 264-267, 2014.
6. H. Wang, "Identity-based distributed provable data possession in multicloud storage,"IEEE Transactions on Services Computing, vol.8, no.2, pp.328-340, 2015.
7. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud datawith group user revocation," IEEE Transactions on Computers, vol.65, no.8, pp.2363- 2373, 2016.
8. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No.9, pp. 1717-1726, 2013.