Data Accuracy and Integrity for Cloud Storage using Block Chain

R.Karthik Ganesh
Department of Computer Science and Engineering
SCAD College of Engineering and Technology
TamilNadu, India

A.Afreedha
Department of Computer Science and Engineering
SCAD College of Engineering and Technology
TamilNadu, India
afreedhaaareef@gmail.com

***Abstract*— Cloud computing is the delivery of information technology services over the web. Cloud security involves the procedures and technology that secure cloud computing environments against external and insider security threats. Cloud safety and security management best practices to forestall unauthorized access are required to keep data and applications within the cloud secure from current and emerging security threats. The original data in the proof are masked by random integer addition, which protects the verifier from obtaining any knowledge about the data during the integrity checking process. While transferring some crucial data, intruders can attack the data or file. To overcome this in the proposed system, files with important messages are split into parts and uploaded. Using the key generation technique, we compare the key values from the original keys to determine the changes within the file. The content will be stored and encrypted within the cloud server. Here we are using a blockchain double hashing algorithm for splitting the original file into three different files and storing that files in three different locations in the cloud. If anyone attempt to hack at the cloud end is not possible to interrupt, because of the various blocks. Therefore, the safety of our scheme is robust. The Encryption and Decryption Techniques are done by using Cryptographic hashing techniques. Anyone can download the files from the server with the file owner's permission. A key is generated at the time of download, and it will be sent to the file owner. We can download that file by using the verification key. Sometimes the hackers can hack the file and take a look to download it. However, once they attempt to download the file, without the verification key one can't open the file.**

Keywords—random integer addition, blockchain, encryption, decryption

I. INTRODUCTION

Distributed computing has been envisioned because of the accompanying creation of information development (IT) plan for endeavours, because of its broad summary of unparalleled inclinations within 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 enormous consequences, distributed computing is changing the method for how associations use information advancement. One fundamental piece of this standpoint is that data are being united or outsourced to the. From customers' view, including together individuals and IT tries, securing data remotely the in a very versatile on-ask for strategy brings engaging focal points: landing of the load for space for storing organization, vast data access with put self-sufficiency, and avoidance of benefits costs on hardware, programming, and staff frameworks of help, etcetera.

While distributed computing makes these compensations more captivating than another time in persistent memory, it also passes on new and testing security risks to customers' outsourced data. As organization providers (CSP) are part of administrative components, data outsourcing is surrendering customers' last control over the fate of their data. As a problem of first significance, despite the way that the structures underneath are more powerful and trustworthy than individual enlisting devices, they are still before the broad assortment of inside and outdoors risks for data respectability.

Cloud computing is the provision of a variety of web-based services. Such resources include tools and applications such as data storage, networking, databases, software and servers.

For various reasons, cloud computing is a popular option for individuals and companies, including cost savings, timeliness and efficiency, enhanced productivity, performance and safety. Instead of storing files on a proprietary hard drive or local device, cloud storage allows many files to be stored in a remote database. As long as an electronic device has access to the network, it can access the data and the software to execute it.

Over the last few years, in particular, cloud storage has become emerging and widely accepted by most people due to the growth in smart devices and wireless broadband networking. While these cloud-based services can be accessed anytime, anywhere, new problems and challenges are emerging. Security is one of the barriers to the broad acceptance of cloud services. Since cloud data can be accessed directly through the Internet, the Cloud Service Provider (CSP) must provide specific mechanisms to confirm data security. As a result, an effective access control mechanism is necessary to maintain the benefit of cloud-based collaboration in the security context.

The access policy describes the attributes of users authorized to access the data. Each data user could acquire a secret key to spot his/her attributes. A data user can decrypt ciphertext if and on the condition that the user's attributes embedded in the secret key match the access policy embedded in the ciphertext. In CP-ABE, there must be an authority to blame for key management. Because the authority is ready to generate the secret key [1] for any data user, it must be trusted.

Otherwise, there is a security risk of allowing an attacker to execute collusion attacks with the compromised authority. There will be three layers of cloud storage for the file splitting process [2]. Many approaches are proposed to scale back the protection risk of the attacks. To forestall the attacks, we include encrypted and decrypted processes [3]. However, although these approaches reduce security risk, attackers can still execute collision attacks to steal data if there is any untrusted authority. Ciphertext-policy attribute-based encryption (CP-ABE) is proposed to produce identity-based access control, which is suitable for cloud storage services. In CP-ABE, it must be trusted because the authority is accountable for key management. Encrypt(PK, M, P), the data owner's encryption process encrypts a message M with the corresponding access policy P using PK and outputs the ciphertext CT. Decrypt(SK. CT). The decryption process, executed by the data user, decrypts CT using SK and then output M if and only if the attributes in SK match the access policy P. To verify the file [4] and according to the owner's knowledge [6] and permission any other user can share the file [5].

A. *Scope of the paper*

As rapid systems and omnipresent Internet get to finish up accessible as recently, numerous administrations are given on the web to such an extent that clients can utilize them from any place whenever. Information vigour may be an essential prerequisite for capacity frameworks. There is numerous proposition of putting away information over.

B. *Need for the paper*

One essential a 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 load for capacity administration, general information access with area freedom, and evasion of capital consumption on equipment, programming, and workforce systems for upkeeps, and so on.

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

C. *Objective of the paper*

Specialist organizations (CSP) are separate authoritative elements; information outsourcing is abandoning clients' absolute control over the destiny of their information. Thus, the rightness of the information is being put at risk due to the accompanying reasons. Above all else, even though the foundations are substantially more ground-breaking and solid than individualized computing gadgets, they are thus far confronting the broad scope of both inward and outdoors dangers for information respectability. This project has the vision to provide 100% satisfaction for every web user or web client. Even though it may be unachievable in reality, from this system, every user may get what their exact requirement from the user inputs is. However, all users may get a more effective file system with fewer response times for every user input. Establish the effect of the unsecured file system on this present advanced technology period. Determine if processed files make depression worse. Identify the encrypted and decrypted file to enable and improve security level. Measure the responses time with every module like secret key generation [1], file splitting, file encryption, file decryption, and file downloading

II. RELATED WORK

Cloud-based services have gained significant interest with a growing adoption for personal and business uses. The main idea involves shifting traditional computational tasks on users' devices to the cloud server/processor-accessible through some communication channels. This approach has enabled several functionalities, especially for small and less powerful devices, considering two-user secret key generation problems through an intermediate relay. In the untrusted relay setting, the goal is to establish the key agreement between the two users at the highest key rate without leaking information about the key to the relay. Kittipong Kittichokechai et al. [1] characterize inner and outer bounds to the optimal tradeoff between communication and key rates. The inner bound is based on the scheme, which combines binning, network coding, and key aggregation techniques. The optimal communication-key rate tradeoff for the trusted relay setting with a public broadcast link is provided for a special case where the two sources are lossless at the relay. In this work, we characterize inner and outer bounds to the optimal tradeoff region of communication and key rates. The inner bound is based on an achievability scheme that involves a novel combination of binning, network coding, and key aggregation techniques.

Data sharing in cloud computing enables multiple participants to freely share the group data, which improves labour efficiency in cooperative environments and has widespread potential applications. However, there are formidable challenges to ensuring the security of data sharing within a bunch and efficiently transferring the outsourced data in a group manner. Note that key agreement protocols have played a significant role in secure and efficient group data sharing in cloud computing. In this paper, by taking advantage of the symmetric balanced incomplete block design (SBIBD), Jian Shen et al. [2] present a unique block design-based key agreement protocol that supports multiple participants, which might flexibly extend the number of participants in a very cloud environment according to the structure of the block design. Based on the proposed group data-sharing model, we present general formulas for generating the common conference key K for multiple participants. Note that by taking advantage of the (v, k + 1, 1)-block design, the computational complexity of the proposed protocol linearly increases with the number of participants and the communication complexity is significantly reduced. Additionally, the fault tolerance property of our protocol enables the group data sharing in cloud computing to resist different critical attacks, which is comparable to Yi's protocol. The advantage of the proposal is it allows multiple data owners to share the outsourced data with high security and efficiency freely. Attackers or the semi-trusted cloud server have no access to the generated key; thus, they can't access the original outsourced data. The drawback of the system is it doesn't provide an authentication service, which makes it liable to man-in-the-middle attacks. One cannot guarantee that all participants within the group are honest, and the existence of malicious participants can seriously destroy the conference.

Public cloud storage is an essential cloud computing service. Currently, most owners of enormous data outsource their data to cloud storage services, even high-profile owners like governments. However, public cloud storage services don't seem optimal for ensuring the possession and integrity of the outsourced data. This situation has given rise to several proposed provable data possession check schemes (PDP). A PDP scheme allows data owners to efficiently, periodically and securely verify that a cloud storage provider possesses the outsourced data. Most currently available provable data possession check schemes make selective (i.e., probabilistic) checks using random data blocks to verify data integrity instead of checking the complete dataset. Therefore, these schemes are considered inadequate by critical infrastructure sectors that involve sensitive data (critical data). Walid I. Khedr et al. [3] proposed a new and efficient deterministic data integrity check scheme called cryptographic-accumulator provable data possession (CAPDP). CAPDP surpasses the common limitations exhibited by other currently proposed methods. The underlying technique of CAPDP relies on a modified RSA-based cryptographic accumulator that has the following advantages: i) It allows the data owner to perform a vast number of data integrity checks. ii) It supports data dynamics. iii) It's efficient in terms of communication, computation and storage costs for both the data owner and the cloud storage provider. iv) The verification operation within the proposed scheme is independent of the number of blocks being verified. v) It minimizes the burden and price of the verification process on the data owner's side, enabling verification to be performed even on low-power devices. vi) It prevents tag forgery, data deletion, replacement, and data leakage attacks and detects replay attacks. Moreover, the prototype implementation and experimental results show that the scheme applies in real-life applications. The system's merits are that it allows the data owner to perform many data integrity checks. It supports data dynamics, and it's efficient in terms of communication, computation and storage costs for both the data owner and, therefore, the cloud storage provider; The demerits of the system are data owners worry about the likelihood of uploaded data being modified or erased without their knowledge or permission. There'll be no burden on the data owner side.

People endorse the excellent power of cloud computing but cannot fully trust the cloud providers to host privacy-sensitive data because of the absence of user-to-cloud controllability. To make sure confidentiality, data owners outsource encrypted data rather than plaintexts. Ciphertext-Policy Attribute-based Encryption (CP-ABE) may be used to conduct fine-grained and owner-centric access control to share the encrypted files with other users. Nevertheless, this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provides the potential to verify whether a downloader can decrypt. Therefore, these files should be available to everyone and accessible to the cloud storage. A malicious attacker can download thousands of files to launch Economic Denial of Sustainability (DDoS) attacks, which can consume the cloud resource essentially. The payer of the cloud service bears the expense. Besides, the cloud provider serves both the accountant and, therefore, the payee of resource consumption fees, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. Kaiping Xue et al. [4] described an answer to secure encrypted cloud storage from DDoS attacks and supply resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with the arbitrary access policy of CP-ABE. We present two protocols for various settings, followed by performance and security analysis. The system's benefits are efficient access control for the cloud provider, which must not add excessive overhead. Data owners who store files on cloud servers still want to manage the access in their own hands and keep the data confidential against the cloud provider and malicious users. The disadvantages are that if the cloud cannot do cloud-side access control, it is to permit anyone, including malicious attackers, to download freely, although just some users can decrypt. The server is liable to resource-exhaustion attacks. When malicious users launch the DoS/DDoS attacks on the cloud storage, the resource consumption will increase.

With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. However, the user's data is ultimately stored in cloud servers in the current storage schema. In other words, users lose their right to control data and face privacy leakage risk. Traditional privacy protection schemes are usually based on encryption technology, but these methods cannot effectively resist attacks inside the cloud server. Tian Wang et al. [5] proposed a three-layer storage framework based on fog computing to unravel this problem. The framework can take full advantage of cloud storage and protect data privacy. Besides, the Hash-Solomon code algorithm divides data into different parts. Then, we can put a tiny part of the data in the local machine and fog server to guard the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in the cloud, fog, and native machine. Through the theoretical safety analysis and experimental evaluation, the feasibility of our scheme has been validated, which is a potent supplement to the existing cloud storage scheme. The merits are that it protects the image content and features well from the semi-honest cloud server and deters the image user from illegally distributing the retrieved images. It is secure and might resist possible attacks. The demerits are that the users lose their right of control over data and face privacy leakage risk. The local machine's capacity cannot satisfy the user's requirement.

Attribute-based keyword search (ABKS) as a vital sort of searchable encryption that has been widely utilized for secure cloud storage. In a key-policy attribute-based quick keyword search (KP-ABTKS) scheme, a private key is related to an access policy that controls the searchability of the user, while a search token is related to a time interval that controls the search time of the cloud server. However, after a careful study, we uncover that the sole existing KP-ABTKS construction is not secure. Through two carefully designed attacks, we first show that the cloud server can search the ciphertext anytime. As a result, their scheme cannot support quick keyword searches. To deal with this problem, Kai Khangi et al. [6] proposed an enhanced KP-ABTKS scheme and prove that it is selectively secure against chosen-keyword attacks within the random oracle model. The proposed scheme achieves both fine-grained search control and quick keyword search simultaneously. Additionally, the performance evaluation indicates that our scheme is practical. The benefits of the system are that it is safer against selective adversaries. It achieves both fine-grained search control and quick keyword search simultaneously. The disadvantages of the system are that the encryption schemes make data retrieval impossible by the user. It is insecure and cannot achieve quick keyword searches as they claimed.

A. Existing system

Several critical security problems still exist when data are outsourced to cloud storage. The semi-trusted cloud server without accurate data cannot generate the proper data integrity proof. Data privacy is preserved against the TPA. There are several remote data integrity checking schemes are presented. The remote data integrity checking scheme enables a client to efficiently audit the integrity of outsourced data on a cloud server without downloading them.

Disadvantages of Existing System

- Files are often easily hacked or attacked by intruders.
- Security is not enhanced.

B. Proposed System

In our proposed system, we upload and securely download the file using the subsequent technique. Using this key generation technique, we compare the key values from the original keys to determine the changes within the file. The content will be stored and encrypted within the cloud server. Here we are using a blockchain double hashing algorithm for splitting the original file into three different files and storing that files in three different locations in the cloud. The Encryption and Decryption Techniques are done using Cryptographic Hashing techniques to download the file. Anyone can download the files from the server with the file owner's permission. A key will be generated and sent to the file owner at the time of download. Using the unique key, they can download the file.

Advantages of the Proposed System

- Security is far enhanced.
- Users can download the file with the unique key generated.
- The file will be downloaded only with the owner's permission.

III. OVERVIEW OF THE PROPOSED WORK

The architecture of this project comes under a cloud computing system, which is a combination of SOA (Service Oriented Architecture) and EDA (Event-Driven Architecture). Client infrastructure, application, service, runtime cloud, storage, infrastructure, management and security are the components of cloud computing architecture.

A. Frontend

The frontend of the cloud architecture refers to the client-side of a cloud computing system. It contains all the user interfaces and applications used by the client to access the cloud computing services/resources—for example, the use of a web browser to access the cloud platform.

- Client Infrastructure: Client Infrastructure is a part of the frontend component. It contains the applications and user interfaces required to access the cloud platform. In other words, it provides a GUI(Graphical User Interface) to interact with the cloud.

B. Backend

Backend refers to the cloud itself, which the service provider uses. It contains the resources, manages them, and provides security mechanisms. It includes enormous storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

- Application: Application in the backend refers to a software or platform the client accesses. This means it provides the service in the backend as per the client's requirement.
- Service: Service in the backend refers to the major three types of cloud-based services SaaS, PaaS and IaaS. It also manages which kind of service the user accesses.

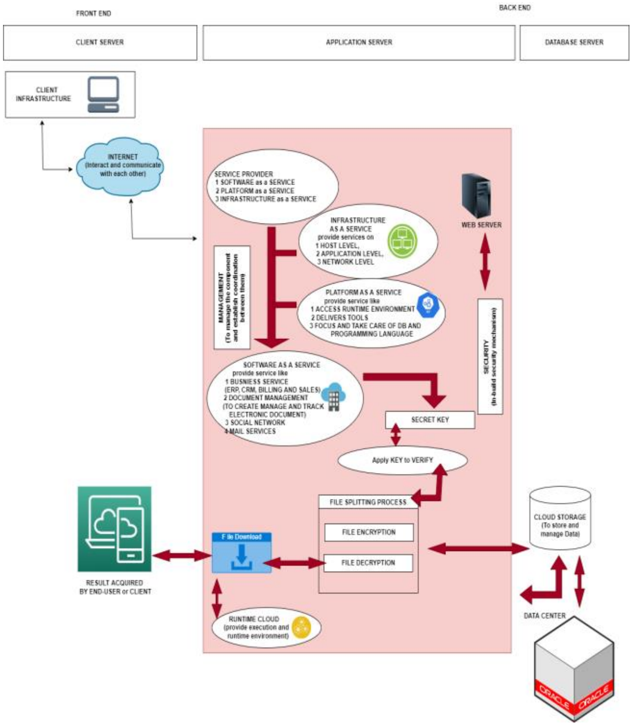

FRONT END
BACK END
CLIENT SERVER
APPLICATION SERVER
DATABASE SERVER
CLIENT INFRASTRUCTURE
INTERNET (Interact and communicate with each other)
SERVICE PROVIDER
1 SOFTWARE as a SERVICE
2 PLATFORM as a SERVICE
3 INFRASTRUCTURE as a SERVICE
INFRASTRUCTURE AS A SERVICE provide services on
1 HOST LEVEL,
2 APPLICATION LEVEL,
3 NETWORK LEVEL
WEB SERVER
MANAGEMENT (To manage the component and establish coordination between them)
PLATFORM AS A SERVICE provide service like
1 ACCESS RUNTIME ENVIRONMENT
2 DELIVERS TOOLS
3 FOCUS AND TAKE CARE OF DB AND PROGRAMMING LANGUAGE
SECURITY (In-build security mechanism)
SOFTWARE AS A SERVICE provide service like
1 BUSNIESS SERVICE (ERP, CRM, BILLING AND SALES)
2 DOCUMENT MANAGEMENT (TO CREATE MANAGE AND TRACK ELECTRONIC DOCUMENT)
3 SOCIAL NETWORK
4 MAIL SERVICES
SECRET KEY
Apply KEY to VERIFY
FILE SPLITTING PROCESS
FILE ENCRYPTION
FILE DECRYPTION
CLOUD STORAGE (To store and manage Data)
File Download
RESULT ACQUIRED BY END-USER or CLIENT
RUNTIME CLOUD (provide execution and runtime environment)
DATA CENTER
ORACLE
ORACLE

Fig. 1. System Architecture

C. *Service Oriented Architecture*

SOA (Service Oriented Architecture) is of categories into the below types

IaaS: Infrastructure as a Service is also known as Hardware as a Service (PaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per-use model. The following are the service provided by IaaS.

- Compute: Computing as a Service includes virtual central processing units and Virtual Main Memory for the VMS that is provisioned to the end end-users.
- Storage: IaaS provider provides backend storage for storing files.
- Network: Network as a Service (NaaS) provides VMS networking components such as routers, switches, and bridges.
- Load balancers: These provide load balancing capability at the infrastructure layer.

PaaS: Platform as a Service (PaaS) provides a runtime environment. It allows programmers to create, test, run, and deploy web applications. You can purchase these applications from a cloud service provider on a pay-as-per-use basis and access them using the Internet connection. In PaaS, backend scalability is managed by the cloud service provider, so end-users do not need to worry about managing the infrastructure. PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle. The following are the service provided by PaaS. PaaS providers Programming languages, Application frameworks, Databases, and Other tools

SaaS: Software as a Service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end-users over the Internet. An independent software vendor (ISV) in this model may contract a third-party cloud provider to host the application. SaaS works through the cloud delivery model. A software provider will either host the application and related data using its servers, databases, networking and computing resources, or it may be an ISV that contracts a cloud provider to host the application in the provider's data centre. The application will be accessible to any device with a network connection. SaaS applications are typically accessed via web browsers. SaaS providers provide the following services.

- Business Services: SaaS Provider provides various business services to start up the business. The SaaS business services include ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), billing, and sales.
- Document Management: SaaS document management is a software application offered by a third party (SaaS providers) to create, manage and track electronic documents.
- Social Networks: As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for convenience and to handle the general public's information.
- Mail Services: To handle the unpredictable number of users and load on e-mail services, many e-mail providers offer their services using SaaS.

D. *Event-Driven Architecture(EDA)*

At the beginning stage, a key is generated to provide a secure process with source and destination keys to produce the safe and secured document. We can identify the changes in both files in the system. With the help of a cloud server, the file content may store according to the available cloud database. Here we use a blockchain double hashing algorithm to split the original file into three different files [2] and store that file in three other locations in the cloud. The Encryption and Decryption techniques are generated using Cryptographic Hashing techniques to download the file. Anyone ready to use the system may download the files from the server with the file owner's permission. After the Owner's permission is granted, the secret key[1] may get input, allowing the user to download the exact file. As a consequence of this system, downloading the file may get to conclude the system for a particular user, and the user may acquire the secured file with this cloud computing system.
Runtime Cloud: Runtime cloud in the backend provides the virtual machine's execution and Runtime platform/environment.

Storage: Storage in the backend provides flexible and scalable storage service and management of stored data.
Infrastructure: Cloud Infrastructure in the backend refers to the hardware and software components of the cloud, including servers, storage, network devices, virtualization software, etc.
Management: Management in the backend refers to the administration of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms.
Security: Security in the backend refers to implementing different security mechanisms in the backend for end-users to secure cloud resources, systems, files, and infrastructure.
Internet: Internet connection acts as the medium or a bridge between frontend and backend and establishes the interaction and communication between frontend and backend.

IV. SYSTEM IMPLEMENTATION

A. User Plug-in

In our Secure System, we have a user-friendly user interface to interact with our System. Every dual Act role as a data owner and data consumer while uploading a file they are the owner of that file. If they search other's files, then they are the consumer. Users can create the account themself. For that, we have new pages, and on that page, we will get the details from the user and generate the account for the user. We have an authentication system; we only allow authorized users to access our System.

In our System, we provide easy file searching Users do not want to keep remembering all uploaded files' exact names; for that, we have given the keywords while uploading the files, which will help to search the file easily.

B. Uploading File

One way to provide data robustness in storing data over storage servers 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. Each of its codeword symbols is stored in a different storage server to store a message. 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.

C. Secret Key Formation

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

D. File Allocation Process

In our application, we can share a file with 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; the same is possible with the edit option.

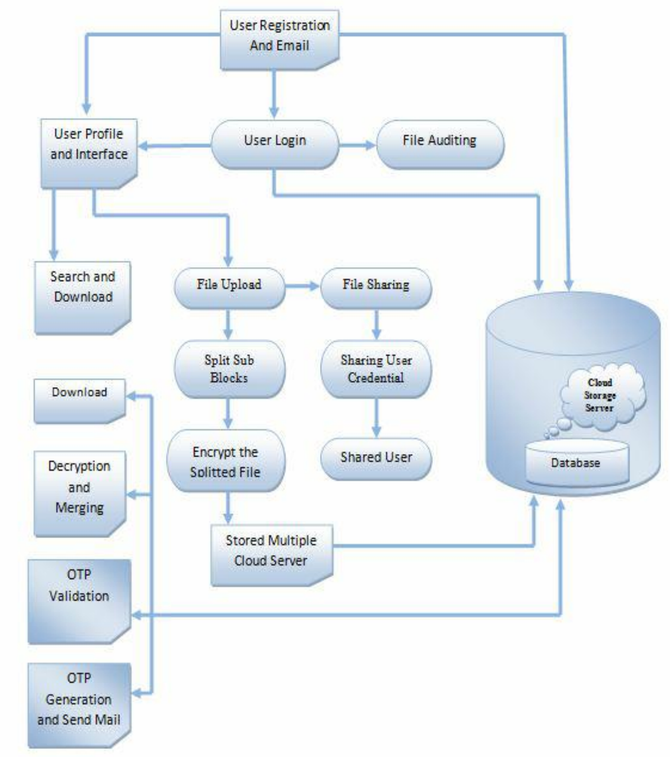


Fig. 2. System Architecture

E. File Analyzing

Auditing is the process of checking whether the file's original contents are changed. This module provides the file owner auditing, which 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 is the file and saves it, a new token will be generated and stored in the DB. If the initial token and the current token are not identical, then a notification will be sent to the file owner.

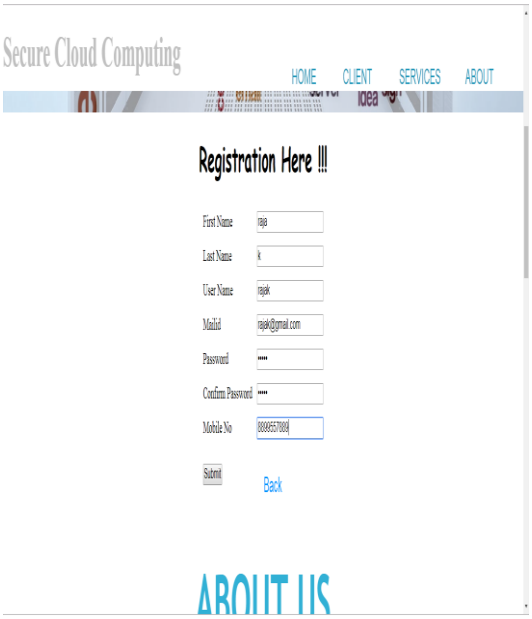
F. File Loading Process

The 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. Storage servers take care of the length of the forwarded message and the computation of re-encryption. Proxy re-encryption Schemes significantly reduce the overhead of the data Forwarding function in a secure storage system.

G. Alert Mail:

The uploading and downloading process of the user is first to 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 is 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. RESULT AND ANALYSIS

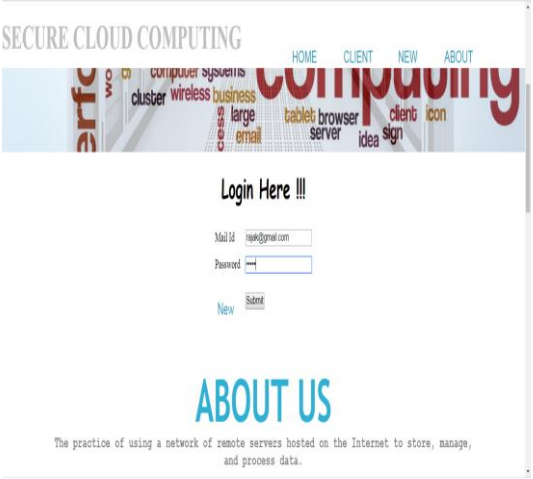


Registration Here !!!

First Name raja
Last Name k
User Name rajak
Mailid rajak@gmail.com
Password •••••
Confirm Password •••••
Mobile No 8899557889

Fig. 3. Registration Page

As per this REGISTER module, users need to input their details to register into the system. The following are the inputs, likely the first name of the user, last name of the user, and user name. To get the mail alert, one needs to enter the mail id, the user's password, and once again confirm their password with the confirmed password and mobile number.



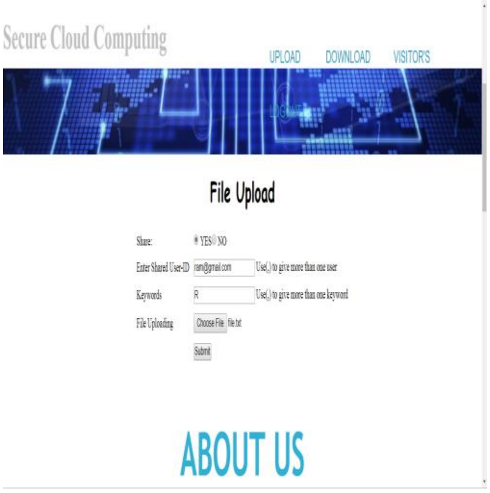
Login Here !!!

Mail Id rajak@gmail.com
Password •••••

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data.

Fig. 4. Login Page

Fig.4 Login Page, as per this LOGIN module, each user needs to input their registered user name and password to get login into the system. After inputting the login details, this system will check the user credentials with the database to determine whether the user is registered or not. The following are the inputs, likely the user name, and the password.



File Upload

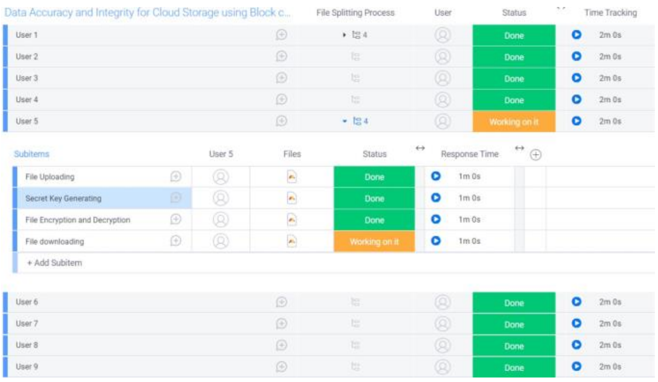
Share: ● YES ○ NO
Enter Shared User-ID ram@gmail.com Use(,) to give more than one user
Keywords R Use(,) to give more than one keyword
File Uploading file.txt

Fig. 5. File Upload

According to the File Upload module, each user must input their file to upload it to the system. The following are the inputs likely optional input to share the file, the need to enter the shared user id of the particular user, an essential key to input as a keyword, and at last, the file they need to input.

A. Experimental SetUp

This implementation of the proposed method has been carried out on a PC with a Pentium Dual Core 2.3 GHz CPU, hard disk of 250 GB or higher, 2GB RAM, and the Windows operating system. Languages used are Java (JSP, Servlet), HTML. Tools used are JDK 1.7, Net Beans 7.0.1, SQLyog. MySQL is used for Backend.



Data Accuracy and Integrity for Cloud Storage using Block c...	File Splitting Process	User	Status	Time Tracking
User 1	4		Done	2m 0s
User 2			Done	2m 0s
User 3			Done	2m 0s
User 4			Done	2m 0s
User 5	4		Working on it	2m 0s

Subitems	User 5	Files	Status	Response Time
File Uploading			Done	1m 0s
Secret Key Generating			Done	1m 0s
File Encryption and Decryption			Done	1m 0s
File downloading			Working on it	1m 0s

User 6			Done	2m 0s
User 7			Done	2m 0s
User 8			Done	2m 0s
User 9			Done	2m 0s

Fig. 6. File Splitting Process

Fig. 6 File Splitting Process shows how each user's files are split and stored in database. Fig. 7 Performance Analysis describes time taken by the system to split the files, generate secret key, encryption and decryption and for uploading and downloading.

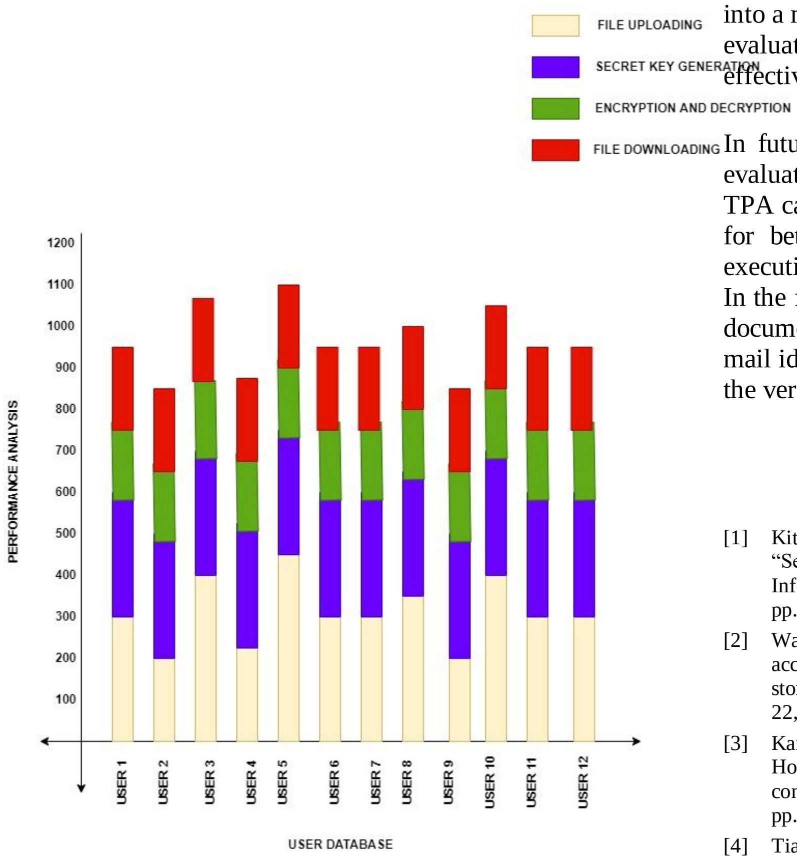


Fig. 7. Performance Analysis

VI. CONCLUSION AND FUTURE WORK

A protection-saving open examining framework for information stockpiling security in processing. We use the straight homomorphism 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 the client from the dreary and perhaps costly examining assignment, yet in addition, reduces the clients' dread of their outsourced information spillage. Considering TPA may simultaneously deal with various review sessions from various clients for their outsourced information records, we expand our security protecting open examining convention into a multiuser setting, where the TPA can play out numerous evaluating undertakings in a bunch way for better effectiveness.

In future, we will expand our protection safeguarding open evaluating convention into a multi-client setting, where the TPA can play out different examining errands in a cluster way for better productivity. In imminent, we will enhance the execution. In this framework, we utilized just content records; In the future we will incorporate the picture, sound, and video documents. In our framework, the OTP is sent to proprietor mail id; the customer will get the OTP on portable by utilizing the versatile number.

REFERENCES

[1] Kittipong Kittichokechai, Rafael F. Schaefer, and Giuseppe Caire, “Secret Key Generation Through a Relay”, [IEEE 2016 IEEE Information Theory Workshop (ITW) - Cambridge, United Kingdom, pp. 196–200, 2016.

[2] Walid I. Khedr, Heba M. Khater, Ehab R. Mohamed, "Cryptographic accumulator-based scheme for critical data integrity verification in cloud storage", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2019.

[3] Kaiping Xue, Senior Member, IEEE, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong, "Combining data owner-side and cloud-side access controlfor encrypted cloud storage", Proceedings of IEEE INFOCOM, pp. 1-9, 2018.

[4] Tian Wang ,Jiyuan Zhou, Xinlei Chen , Guojun Wang , Anfeng Liu , and Yang Liu, Member, "A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing"IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2018.

[5] Zhang, Kai, Ximeng Liu, Yanping Li, Tao Zhang, and Shuhua Yang. "A Secure Enhanced Key-Policy Attribute-Based Temporary Keyword Search Scheme in the Cloud." IEEE Access 8 (2020): 127845-127855.

[6] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, XingmingSun, "Block design-based key agreement for group data sharing in cloud computing", IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2017.