International Journal for Rapid Research in Engineering Technology
Vol IX Issue I January 2023
ISSN (Online):- 2455-4723

Roll Back Operation HSDRT Based Data Backup and Security in Cloud Computing

Teena chouhan, Asst. Prof. Ms. Priya Sen
Department of Computer Science & Engineering
Swami Vivekanand College of Engineering
teenachou012@gmail.com, priyasen@svceindore.ac.in,

Abstract: In cloud computing, the amount of data generated by electronic forms is huge. To properly maintain these data, it is necessary to provide data recovery services. We present a standard algorithm he developed instead of the remote, the seed blocking algorithm to solve this problem. The purpose of the algorithm is twofold. First, it can help users gather information from any remote location without a network; second, you can restore files when the files delete, and the cloud is destroyed for whatever reason. The proposed seed protection algorithm also solves the time-related issues so that the recovery time will take the least amount of time. The proposed algorithm also focuses on the idea of securing the files it prepares instead of being stored on a remote service without using encryption technology The proposed HSDRT and roll back operation is proposed in this thesis this algorithm can these problems so that the recovery process takes the least processing time. The proposed HSDRT algorithm with AES encryption technique will also focus on the security of backed up files stored on remote servers. Cloud storage provides online storage where data is usually stored in the form of a virtual pool hosted by a third party. We have designed a hybrid model on the Java platform to solve all the problems, the hybrid model consists of ROLLBACK+HSDRT+AES with hash function This proposed system follows three modules, first is Backup modules will be formed by rollback operation, and second is Recovery modules will be performed by HSDRT, and third is security modules will Be Performed by AES and hash function. The idea that was put forward gave First of all, it lets people get information from anywhere, even if they don't have a network connection. Second, it helps users get their files back if they accidentally delete them or if the cloud is destroyed. Lastly, it helps users keep their data safe when it's stored in the cloud.

Keywords: Cloud, Encryption, Descrtyption ,Cloud Server, Security ,rollback, HSDR

I Introduction

Smart Data Back-up Technique for Cloud Computing using Secure Erasure Encoding ", the purpose of the algorithm proposed by this journal is twofold. First, it can help users to gather information from any remote location without any connection between them. On the network, files are deleted or restored if the cloud is damaged for any reason. So the recovery time will take less time in particular. The proposed SEC also focuses on recovering deleted files stored in Security software, not using any current encryption t technology. It is a remote data backup server in the cloud computing platform. While the main cloud can still provide data to users, the cloud can connect to a backup server that stores independent data.[1]

Roll Back Operation -In database technology, rollback is an operation that returns the database to its previous state. The return is important for database integrity because recovery means that the database can be restored to a clean copy even if the wrong action is performed. Data damaged by any reason can be recovered through a rollback. Provides a restore function that can roll back databases or tables in Tencent Cloud based on data backup. Supports real-time data retrieval. By reconstructing regular images and real-time transactions, the Tencent DB MySQL return function can roll back a database or table to a specific time and ensure that the time schedule for all data is the same. A new database or table is generated in the original instance. During this process, the original database or table can be opened normally. When the rollback is complete, you can see the new database and the original database or table. This is how rollback works the recall function can scroll the database or table back to a specific time based on cold data backup and the corresponding bin log backup.

AES Encryption -The AES encryption/decryption structure is shown in Figure 2 The number of turns shown in Figure 2 and 10 is for the case where the encryption key is 128 bits long. (As mentioned earlier, if the key is 192 bits, the number of circles is 12; and if the key is 256, it is 14.) Before starting the circle-based encryption process, XOR the sequence used in the first four words of the key

scheme. The same thing happens during decryption — the difference is that we now XOR the setting of the ciphertext state with the last four words given by the key.[2-3]

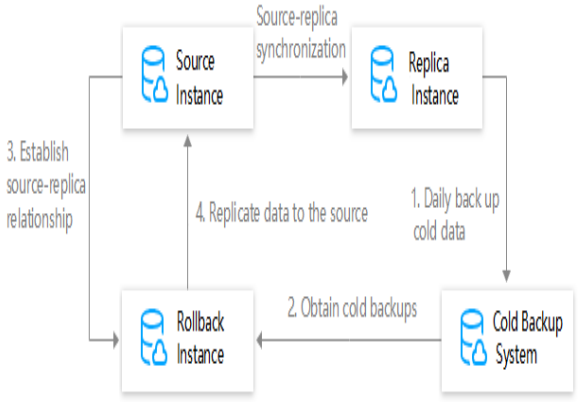

Fig.1 Roll Back Operation

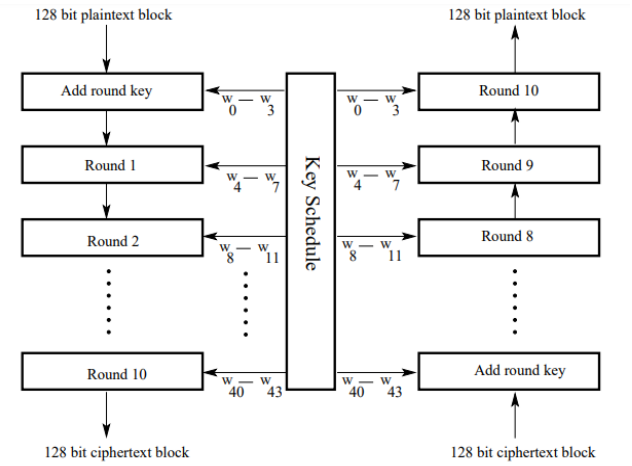

Fig 2: The overall structure of AES for the case of 128-bit encryption key.

For encryption, each cycle consists of the following four steps

1) Replace bytes,
2) Move lines,
3) Merge columns and
4) Add round keys. The final step requires XORing to exit the first three steps with the four words in the main program.

For decryption, each round consists of the following four steps:

1) Repeat the sequence in the reverse order,
2) replace the bytes in the sequence,
3) Add a round

Key, and 4) Repeat mixed columns. The third step requires XORing to output the first two steps with the four words in the main program. Note the difference between replacing and modifying a function in a circle and the order of a similar function in a circle. The final round of encryption is without a "mixed" process. The final round of termination is devoid of the "opposite mixing column" process.

Data Security Challenges -When entering the Internet-based cloud model, we need to emphasize data security or privacy. Data loss or data leakage can significantly force a company's brand, brand, and credibility. Prevention of data disclosure is considered to be the most important factor, 88% of which are major challenges and very major confront. Likewise, data privacy or security accounts for 92% of security issues.

Security-When many institutes share property, data abuse is at risk. Therefore, to avoid potential risks, data or data stored in the storage, transmission or processing must be protected. Data security is the biggest challenge in cloud computing. To improve cloud computing safety, it is imperative to provide data verification, authorization, or contact control for the data accumulated in the cloud.

Confidentiality: -Check for major vulnerabilities to guarantee that data is confined from data attacks. Therefore, safety testing must be done to defend the data from malicious users, such as cross-site scripting, monitoring mechanisms etc.

Reliable: -If you want to provide data protection for your customers, don't use thin clients with only a few sources of information. Users should not store individual data (such as passwords) to ensure trustworthiness.

Locality-In cloud computing, data is shared across multiple regions, and it is difficult to find where the data is located. When data is transferred to another geographic position, relevant laws may also change. Then, there are issues with conformity or computer privacy laws. Customers should know the location of their data, and the location should be provided by service provider.

Integrity-The organization should preserve safety so that only authorized personnel can edit the data. In a cloud-based setting, data veracity must be carefully preserved to prevent data loss. In general, all exchanges in cloud calculate should follow ACID characteristics to maintain data honesty. Most Internet services often face a lot of exchange management troubles due to use of HTTP services. The HTTP service does not maintain secure exchange or transmission. It can be obtained by executing the exchange organization in API itself.[4]

Access-Data access refers to data protection policy. In an institute, workers will be granted contact to a portion of data following their company's safety policy. Other employees in the same organization cannot get the same data. Various recording technologies and major supervision mechanisms guarantee that the data is shared with authorized users. Use various power distribution mechanisms to distribute keys only to authorized parties. To protect the data of unauthorized users, the data protection policy should be strictly chased. Since all cloud users are granted access through the Internet, it is necessary to grant users access rights. Users can use data encryption or security to protect against potential threats.

Segregation-One of the distinguishing individualities of cloud computing is the durability of many. Because multi-tenancy allows multiple users to store data on a cloud server, there is a risk of data access. By entering client code or using any function, this can be circumvented. Therefore, it is necessary to store the data discretely database. You can use tests such as SQL injection aws, data justification, or insecure storage to perceive or perceive vulnerabilities in data input.

Storage- When data is kept in virtual computers, one of the many problems that can come up is how reliable the data storage is. There are also many other things to think about. Requiring physical infrastructure to be used to store virtual machines opens up the system to possible flaws.

Data center operations-In the event of bottlenecks and natural disasters, organizations using cloud computing need to guard their data without incurring losses. If the data is not properly supervised, there are problems with data storage and data contact. In the event of an accident, the cloud provider is responsible for data loss.[5]

II Headings and Footnotes

M We recommend that you use encryption as a better new security solution. Before you store the data on a cloud server, it is better to hide data first. The data owner can grant agreement to members of a particular group so that they can simply contact database. Heterogeneous data-centric security will be used to control data admission. The data safety model includes verification, data protection and data integrity and data recovery. User protection must be considered to recover data safety in cloud. To ensure the protection of privacy or data, data defense can be used as a service.

To prevent other users from accessing the data, data encryption is not entirely feasible, and conventional encryption may make it difficult to use. Users are advised to check if the data is stored on a backup disk before uploading the data to the cloud, and to keep your password in the file unchanged. Before entering the hash value of a file on the cloud server, calculating the hash value will guarantee that data does not change. Hash calculations can be used for data integrity, but they are difficult to maintain. By combining identity-based encryption and an RSA signature RSA control can be provided. SaaS guarantee that there must be clear restrictions between physical level or level of application to differentiate the data available between different users. Circulated control architecture can be used to manage access to cloud computing. If you want to identify unauthorized users, it is better to use a policy based on permission or account creation. The license as a service can be used to tell the user a portion of the available data. The natural access manage mechanism allows owner to transfer most of the work to the cloud server without revealing contents of the data. The data system can be configured to ensure secure data processing or sharing among cloud users. Online access prevention systems are used to recognize real threats. If you want to store many files of unusual sizes or solve Cloud Computing Security and Backup Issues [6]

The cloud is vulnerable to several security threats, ranging from network-level threats to application-level threats. To keep the cloud safe, these safety threats must be prohibited. In addition, data found in the cloud is also vulnerable to several threats and various issues, such as security issues, convenience issues, confidentiality and data integrity. External threats, so that a strong and mutual understanding is established between customer and their cloud service provider. This article addresses various security issues connected to three basic services provided by the cloud computing situation and discusses solutions to avoid these issues.[7]The purpose of the SBA proposed in this article is restore files if the cloud is corrupted or deleted in the cloud. The main advantage of SBA is that it spends the least amount of time in the recovery process. In this article, when SBA analyzes the Blockchain algorithm, they also focused on the security considerations of the files they prepared instead of those stored in remote software without using existing encryption technology[8].We talked about worries about where data is kept, how it is stored, how secure it is, how easy it is to get to, and how well it is kept. One way to get past these worries about safety is to build trust with each other. This can make it easier to connect heart to heart in a short amount of time.. The issues mentioned above will become a hot spot of research for cloud computing. [9] They proposed and demonstrated the validity of a new long-term recovery protocol for

cluster-based recovery systems. Compared to existing solutions, this protocol has obvious advantages, and it is well-adapted to adapt to various important aspects, such as load balancing or performance exchange. Working on a central platform makes it easy to change the protocol for many different uses, in addition to the traditional ones it already supports. File systems and distributed objects are two examples of these kinds of applications. [10]

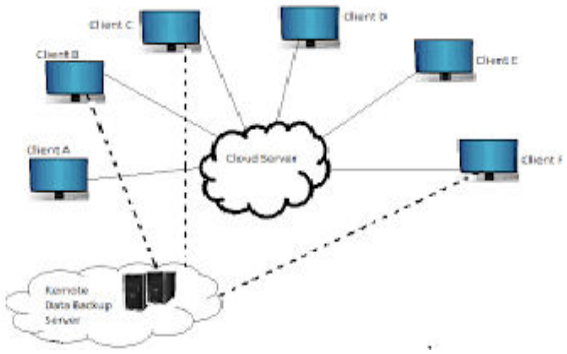

Fig 3 Remote data backup Server Architecture [23]

The purpose of the proposed algorithm is twofold. First, it can help users gather information from any remote location without a network; second, you can restore files when the files are deleted or the cloud is destroyed for whatever reason. Time-related issues are also resolved by the proposed SEC, so recovery time will take the least amount of time. The proposed SEC will also focus on protecting the files it prepares instead of those stored on remote software that does not use current encryption technology.

[8]. the purpose of the recovery technique is to help the user collect information from the server they have planned instead when the server is unable to provide data to the user. Many recovery systems can be used to restore data in the cloud, such as HSDRT, ERGOT, LINUX BOX, PCS, COLD, and COLD/HOT recovery schemes. However, these technologies have some limitations, such as difficulty in implementation, security issues and long search times. Therefore, an intelligent backup algorithm called block of seed algorithm is proposed. The purpose of the proposed SBA is to restore files if the cloud is corrupted or the files may be deleted from the cloud. The main advantage of SBA is that it spends the least amount of time in the recovery process.[11]. This article uses cloud computing as its delivery platform. This is a new way to store user data and give people and businesses safe access to their information. Provide a service that lets people make requests online. Even cloud computing creates an environment that makes it easier to manage data and get to it. Also, it will have consequences, like sensitive data being stolen or leaked.

III Tables, Figures and Equations

The proposed model will be able to solve all the problems of the cloud system, Will design the proposed model in such a way that it can solve the various problem like data security, data privacy, data backup, data recovery. Rolling back operation implement in the proposed model to solve the restore problem of cloud system rollback operation server can be helpful when you have experienced performance issues, and the server will not boot or operate as it should.

In the model for data recovery that is being shown, HSDRT is used. Recovery technology is supposed to help the user get the data they need from another server, like a backup server, when a server can't give them what they want. HSDR is one way to recover lost data from the cloud. The suggested system is built in HSDRT mode so that it can recover files from the cloud if the cloud gets corrupted or if files are accidentally deleted from the cloud. The main advantage of HSDRT is that it can spend the least amount of time on the recovery process. AES and hash features have also been added to this research work to achieve a high level of data security. The main goal of AES is to create an encryption method that is irreversible without a key that uses a key that cannot be cracked by guesswork Or atrocious Force.

SYSTEM ANALYSIS:

The purpose of the research to secure data as well as performed rollback operation on cloud server. HSDRT it can help users gather information from any remote location without any connection to the network; second, it can restore files when the files are deleted or the cloud is destroyed for whatever reason. Often, the first cloud backup server is a copy of the first cloud. When this dedicated server resides in a remote location (i.e. away from the main server) and has the nature of a large cloud, the backup software is called a data backup server. A large cloud is called a storage center, and a remote cloud is called remote storage. To solve challenges such as implementation complexity, low cost, security, and time-related issues, we offer HSDRT and AES encryption algorithms with rollback functionality.

This system model represents four different applications to support users, data owners and cloud service providers. It represent following application 1) Data owner application 2) User Application 3) Storage Server 4) Group authority. The data owner enrolls into the cloud for uploading his/her own data into the cloud by customizing its accessibility functions. The storage server encrypts the owner data by employing AES cryptography model produces symmetric key to the group of users. But the data accessibility control is granted through the data owners only. The group authority organizes the group of users and offers group privilege services. The storage server maintains the access control list and group signature list. The storage server grants a permission to the data owner files to the valid users based on the secrete key management mode. The figure-4 represents the tradition system model with four different components.

It needs effective data security and data recovery so that customers can connect to their planned server instead, storing data independently on a backup server with high reliability and whenever the big cloud can't provide the data to users. In this proposed work focus on the data security and data back on the cloud platform. These technologies must also have a small amount of money to implement solutions to recovery problems and easily recover data after a natural disaster. Therefore, the demand for cloud computing recovery and recovery technology comes from its customers 'savings. Many users share storage and other resources, and other customers may access your data as well. Human malfunctions, device failures, network connections, malfunctions or criminal intent can compromise our cloud storage. In addition, changes to the cloud are also frequent. We can call this data dynamics various operations such as inserting, deleting, and blocking validation of the supporting data. Because the service is not limited to this, data can be stored and backed up; remote data reliability is also needed. Because data integrity is always focused on the server's integrity and full state integrity, the server must process a large number of generated data that remains unchanged during storage and transmission to the server.

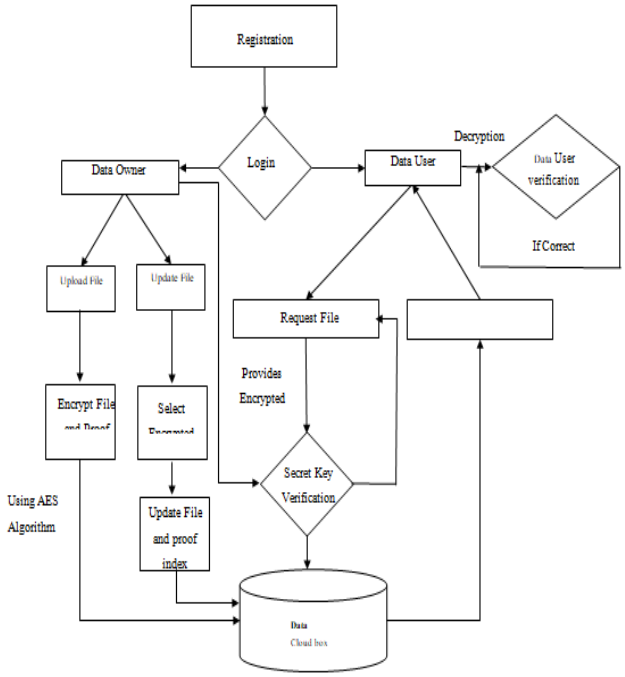

Figure 4 Flow Diagram

HSDRT (High Speed Data Rake technology)

HSDRT has become an effective technology for mobile computers, mobile phones and other mobile customers. However, it cannot manage the low cost required to recover, and it cannot control the data recovery. It is a new file editing concept, which uses widespread data transfer mechanics and high-speed data processing technology.

HSDRT is an innovative file retrieval concept that uses a wide-ranging and efficient data transfer mechanism with high-speed technology.

Roll Back Operation

In database technology, rollback is an operation that returns the database to its previous state. The return is important for database integrity because recovery means that the database can be restored to a clean copy even if the wrong action is performed. Data damaged by any reason can be recovered through a rollback. Provides a restore function that can roll back databases or tables in Tencent Cloud based on data backup .Supports real-time data retrieval. By reconstructing regular images and real-time transactions, the TencentDB MySQL return function can roll back a database or table to a specific time and ensure that the time schedule for all data is the same. A new database or table is generated in the original instance. During this process, the original database or table can be

opened normally. When the rollback is complete, you can see the new database and the original database or table. This is how rollback works the recall function can scroll the database or table back to a specific time based on cold data backup and the corresponding bin log backup.[17]

EXPERIMENTAL SETUP:

In this project, designed the cloud cryptography security application using the JAVA language. First installed NetBeans to set up the project environment. Initially created user interface applications using java swings and security features, and classes were imported from java cryptography and security packages. And configured supported cryptography and security library APIs. Designed group authority and storage server applications to dealt with the data access control and group signature functionaries. configured MySQL database to organize users and data owner information with the help of JDBC and MySQL drivers here below mentioned the execution graph of proposed solution this is the process of registering or registering in the cloud. To take advantage of cloud documents, all data owners and data users must register.

Data Owner-Data Owner extracts keywords of each data also figures a keyword Index. Data Owner encrypts documents r keyword Index using a key and outsources in cloud. Data Owner provides the Public Verification Key and Proof Index to the Data User via Cloud for document verification. Data Owner is the only authorized person to add, modify, or delete the document(s) from the cloud.

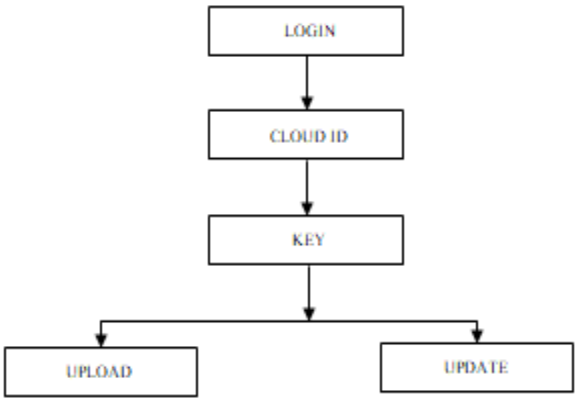

Figure 5 Data Owner

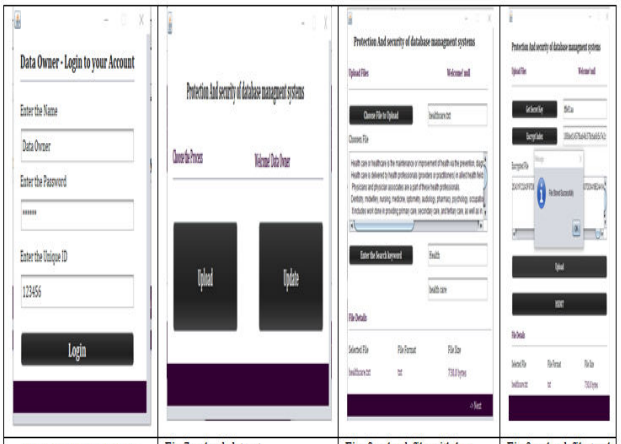

Fig 6 Data owner login | Fig 7 upload dataset | Fig .8 upload file with key | Fig 9 upload file to clo

Data Owner extracts keywords of each data also figures a keyword Index. Data Owner encrypts documents keyword Index using a key and outsources in cloud. Data

AES- The appended text are encrypted using AES encryption.
Add Padding Bits with Based Encode-64- After the AES encryption, some padding bits are added either to the left or right of the base64 encoded data to get the final encrypted text.

Decryption

Remove Padding Bits- In this step the padding bits are removed from the cipher text with decode-64 process.

AES Decryption- After the padding bits are removed, the data is decrypted using AES.

Now, as the data gets stored on the main cloud and then by using the EXOR technique it is stored on the Remote server, the question of providing security arises. The user of the data should be authenticated, which will authenticate the data before storing it on the cloud. For this purpose, various kinds of cryptographic techniques can be used taking into consideration the advantages and disadvantages of the methods, encryption using the public and the private key is done on the data. The encrypted data is then Ex-ored and stored on the Remote Server. For storage on the Cloud Server the data can be stored in its original form or in the encrypted form. For the proposed approach the work proceeds as follows. There are three components namely the admin, the information seeker and the information provider. The admin assigns the tokens to the seeker as well as the information provider. The seeker or the provider on presenting the token to the admin when asked will then be given the admin's secret key, which can be used for the encryption or the decryption purpose. The admin will keep a record of all the members it has provided with token and ones involved in the communication. After this

check is done the provider encrypts the message. The ciphertext is generating to encrypt the message and then send it to the remote server by applying the EXOR technique. When the main cloud has crashed or the original file has lost from the main cloud, it can be retrieved from the remote server. The seeker gets the Exored file, which has to be decrypted by using the public and the private key. Again the admin checks its database for all the registered and authorized users

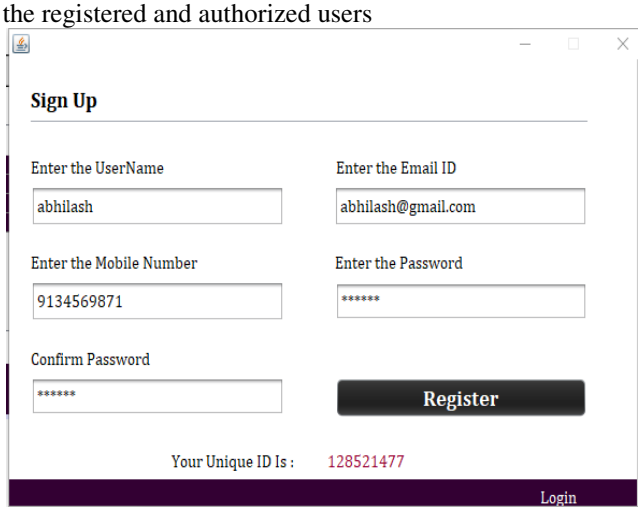

Fig 10 User Signup

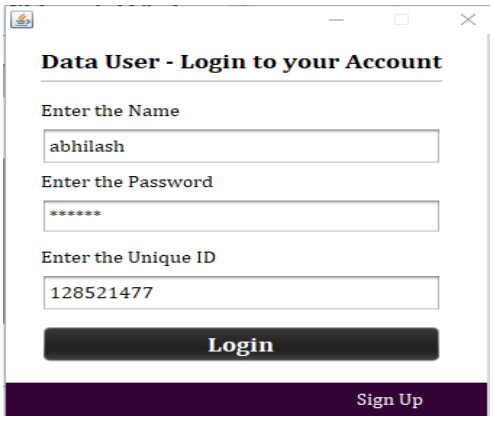

Fig 11 User Login

Data User sends a request to a cloud server. After the request approved from the cloud, the Data User being paid the Public Verification Key from the cloud created by Data Owner.

User Registration -This operation deals with user enrollment in cloud, where the user provides basic information to enroll themselves in cloud. The storage server needs to validate the user details and generate group signature and assigned into the user groups performed by the file owner. The data owner can send a request to the storage server and provide accessibility to the user to access his/her files

Data User- A request is made by the Data User to the cloud server. Once the request has been accepted by the cloud, the Public Verification Key will be sent to the Data User. The Data Owner is the one who will make the Public Verification Key. After the Data User has successfully signed in with the public verification key, they can now decrypt or download encrypted documents. After getting confirmation from the cloud, the person who needs the file will download it as quickly as possible within a strict time limit.

Verification with Proof Index- An organization that makes proofs for cloud investigations that use the Public Verification Key. In this section, users of the data or other people can use the Verification key to check the accuracy of search results.

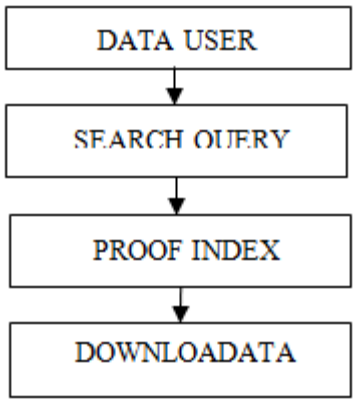

Figure 12 Verification with Proof Index

Key management

Step1 : Initialize two different parameters 1) large prime number q 2) primitive root a each user (e.g. A)

Step 2: Generates their key: chooses a secret key(number): xA< q compute their public key: yA = a^xA mod q public keys are stored in universal directory

Step 3: shared session key for users A & B is KAB: KAB = axA.xB mod q = yA^xB mod q (which B can compute) = yB^xA mod q (which A can compute) KAB is used as session key in private-key encryption scheme between User1 and User2

Step 4: if User1 and User2 subsequently communicate, they will have the same key as before, unless they choose new public-keys

User Registration

This operation deals with user enrollment in cloud, where the user provides basic information to enroll them in cloud.

The storage server needs to validate the user details and generate group signature and assigned into the user groups performed by the file owner.

The data owner can send a request to the storage server and provide accessibility to the user to access his/her files. Then user registers with this distinctive id with owner by providing his own Arcanum (PassW).

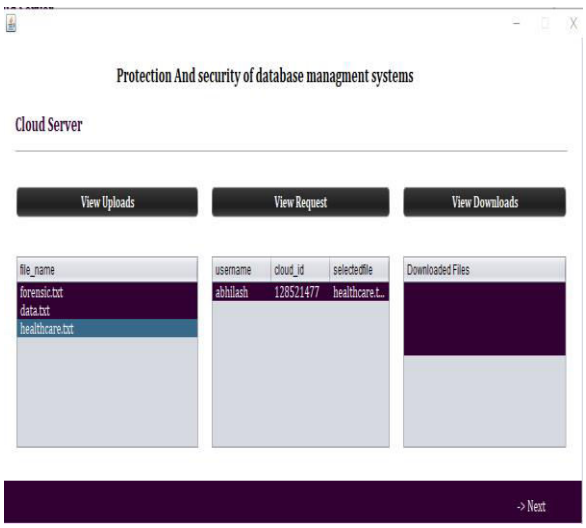

Fig 13 cloud server

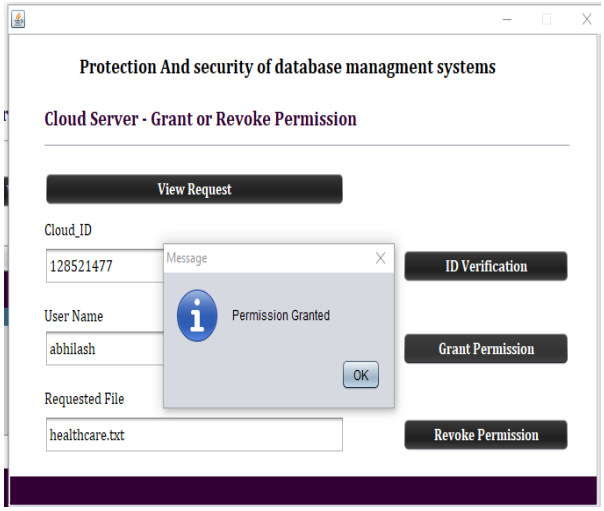

Fig 14 Cloud Data Access Granted

After receiving verification from cloud, the data user will download file within a scrupulous time limit. After receiving a permission and verification from cloud, the data user will download file within a scrupulous time limit.

Registration- This is how you sign up for an account in the cloud. Both the people who own the data and the people who will use the data stored in the cloud need to sign up. During this process, some of your most important information, like your email, contacts, and so on, will be collected and stored in the cloud. During the process of registering a user, a cloud ID will be set up automatically for that user.

Cloud ID- Each user must either make a Cloud ID or use one they already have. This is done to almost securely classify the user. Identifiers don't repeat identifiers that are being changed to identify other identifiers or that will be changed in the future. So, in the future, information marked with Cloud ID by the parties who have given it out can be put in a folder or sent on the same channel without having to deal with a hard conflict between identifiers.

Cloud Service Provider- Every document that is uploaded or sent to the cloud can be seen by the person who made the cloud service possible. Before giving permission, the CSP checks the identity of the data user by getting a document request from the data user. After that, the CSP will either run the query, send back an encrypted document based on the search token, or send back a document with other evidence on it to confirm the search results. Every document that is uploaded or sent to the cloud can be seen by the person who made the cloud service possible. Before giving permission, the CSP checks the identity of the data user by getting a document request from the data user. Data Users can now decode or download encrypted documents after they have used the Public Verification Key to prove who they are.

Public Verification Key- The public corroboration key is a safety number that was made to make sure that your information stored in the cloud doesn't become the target of an attack. By validating each other's public keys, the Data Owner and the Data User can add an extra layer of security to the authorization of each other's characteristics and permissions to store data or files in the cloud.

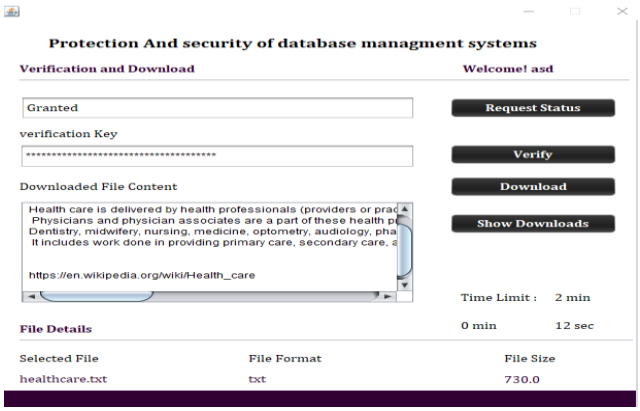

Fig 15 user verify and download

IV Conclusions

Cloud storage provides online storage, which is often stored in the form of a third-party hosted virtual pool. Hosting companies operate big data in large data centers and depending on customer requirements, build a source of that data and present it as a storage pool that can help users store files or data objects. -files. In cloud computing, in order to properly maintain data, it is necessary to provide data recovery services. We present a standard algorithm he developed instead of the remote, the HSDRT with rollback function to solve this problem. we can restore files if they are deleted or destroyed for some reason by the cloud. Time-related issues can also be solved by a seed hedge algorithm, so the recovery time will take the least amount of time. The proposed algorithm also focuses on the security of the files it prepares instead of those stored on remote software without using existing encryption technology.

The cloud service is in charge of keeping cloud storage safe and making sure it has the best level of security possible. Service providers are responsible for making sure that public data integrity and isolation protections are in place to reduce the risks that users in the cloud pose to each other in terms of data loss, misuse, or privacy violations. When users share data with each other, these things can happen. To say it again, from the cloud service provider's point of view, there should be an active monitoring system in place so that service planning and delivery can go well. The proposed method of key generation shows how integrity can be checked with just a few bits of data being sent and the relevant algorithms being run offline It also gives you a secure access control system, a way to manage access permissions, an audit trail, better performance, and less work for you to do. We extend our study to prevent data theft attacks and organize a role-based access control model to organize a secured authentication process. The rollback-based access control model improves the authentication process, which it can minimize cryptography transactions. Future work will focus on analyzing database services in the cloud and the major security risks associated with them. Due to time constraints, some relevant parties may not conduct investigations while others may not conduct thorough investigations. The encryption considerations for cloud databases have been discussed.

References

1. Yuan Su;Yanping Li;Bo Yang;Yong Ding Decentralized Self-auditing Scheme with Errors Localization for Multi-Cloud Storage IEEE Transactions on Dependable and Secure Computing Year: 2021 DOI: 10.1109/TDSC.2021.307598
2. Parsi Kalpana;A. Venugopal;P. V. Sudha A Contemporary Framework Key Based Crypto Method to Enhance Security in Multi Cloud Ambience 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) Year: 202
3. M.Peter and G. T, The NIST definition of Cloud Computing. 2009
4. Security Guidance for Critical Area of Focus in Cloud Computing,. 2009.
5. R.Chow, et al. Controlling Computation without Outsourcing Control. in CCSW'09, ACM workshop on Cloud computing security. 2009.
6. S.Hanna, A security analysis of Cloud Computing. Cloud Computing Journal.
7. J. Wei, et al. Managing security of virtual machnine images in a cloud environment. in CCSW'09 Proceedings of the 2009 ACM workshop on Cloudcomputing secrity. 2009.
8. S.Srinivasamurthy and D.Q. Liu, Survey on Cloud Computing Security- Technical Report. 2010, Indiana University Purdue University: Fort Wayne.
9. Miranda.M and S. Pearson. A Client-Based Privacy Manger for Cloud Computing. in COMSWARE '09: Proceeding of the Fourth International ICST Conference on COMmunication and middeleware. 2009.
10. Flavio.L and R. D.P. Transparent Security for Cloud. in SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing. 2010
11. T. Mather, S. Kumaraswamy, and S. Litif, Cloud Security and Privacy: An enterprise perspectives on

Risks and Compliance (Theory in Practice). O' Reilly, 2009.
12. IEEE International Conference on Cloud Computing. 2009.
13. P.T.Jaeger, J.Lin, and M. grimes, Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology and politics, 2009. 5(3).
14. Cloud Computing: Clash of the clouds. the economist., 2009.
15. B.P.Rimal, E.Choi, and I.Lumb. A taxonomy and survey of Cloud Computing Systems. in Networked Computing and Advanced Information Management, International Conference. 2009.
16. B.R. Kandukuri, R.P.V., and A. Rakshit. Cloud security issues. in IEEE International Conference on Services Computing (SCC). 2009.
17. L.M.Kaufman, Data security in the World of Cloud Computing. IEEE Security and Privacy, 2009. 7(4):: p. 61-64.
18. Matthew Dickinson;Saptarshi Debroy;Prasad Calyam;Samaikya Valluripally;Yuanxun Zhang;Ronny Bazan Antequera;Trupti Joshi;Tommi White;Dong Xu Multi-Cloud Performance and Security Driven Federated Workflow Management IEEE Transactions on Cloud Computing Year: 2021 DOI: 10.1109/TCC.2018.2849699
19. Qing-Hua Zhu;Huan Tang;Jia-Jie Huang;Yan Hou Task Scheduling for Multi-Cloud Computing Subject to Security and Reliability Constraints IEEE/CAA Journal of Automatica Sinica Year: 2021 DOI: 10.1109/JAS.2021.1003934
20. Cheng Zhang;Yang Xu;Yupeng Hu;J. Wu;Ju Ren;Yaoxue Zhang A Blockchain-Based Multi-Cloud Storage Data Auditing Scheme to Locate Faults IEEE Transactions on Cloud Computing Year: 2021