SECURE DATA STORAGE IN CLOUD-TO-FOG COMPUTING USING CP-ABE

Padmavathi. S

Department of Computer Science & Engineering,
Sri Krishna College Of Technology, Kovaipudur, Coimbatore, Tamil Nadu, India.
padmavathi.s@skct.edu.in

Swetha. S

Department of Computer Science & Engineering,
Sri Krishna College Of Technology, Kovaipudur, Coimbatore, Tamil Nadu, India.
18tucs241@skct.edu.in,

Swethaa. C

Department of Computer Science & Engineering,
Sri Krishna College Of Technology, Kovaipudur, Coimbatore, Tamil Nadu, India.
18tucs242@skct.edu.in

Abstract **- Cloud Computing in the current world faces many challenges in the security side. So as a part in this work cloud users can be able to exchange their documents (i.e. text format) safely. Users may effortlessly alter and share data as a group using cloud data storage and sharing services. Once a user is revoked from the group for security concerns, all blocks that were previously signed by this revoked user must be re-signed by an existing user. Due to the vast quantity of shared data in the cloud, the simple technique of allowing an existing user to download the relevant part of shared data and re-sign it following user revocation is wasteful. In the proposed work we consider the security of the users, so that by using CP-HABE the file is decrypted and encrypted and the files which is bigger in size can be split into blocks using block chain splitting method. So that the file can be reached the user at the other end without any malicious attacks. With this work it enhances the integrity of sharing data in cloud environment.**

I.INTRODUCTION

Distributed storage is an assistance where information is somewhat kept up with, made due, and supported up. Another type of Internet-based registration is distributed computing, which provides advantageous, on-demand network connectivity. By examining random square layouts, Provable Data Possession (PDP) guarantees the information's reliability.

A. Public sector auditing

Auditing in the public sector The public-area review climate is one in which state-run administrations and other public-area entities are held accountable for the use of assets obtained via tax collection and other sources in the delivery of services to citizens and other beneficiaries. These aspects are in charge of their administration and execution, as well as the use of assets, both for those who provide the assets and for those who rely on the administrations delivered using those assets, such as inhabitants.

B. Financial audit

Audit of financial statements It focuses on determining if a substance's monetary information is provided in accordance with the material monetary announcing and administrative system. This is accomplished by obtaining appropriate and suitable review proof, which allows the examiner to provide an opinion on whether the monetary data is free of material misquote due to extortion or mistake.

C. Performance audit

The purpose of a performance audit is to determine whether or not
Intercessions, initiatives, and foundations are all examples of this.
acting in accordance with economic norms
proficiency and adequacy, as well as whether or if there is any
an opportunity to improve Execution is the final step in the process. Models were compared to the results, and justifications for breaking those regulations, or Various concerns are investigated. The idea is to answer critical review questions and provide feedback proposals to go forward.

D. Compliance audit

Auditing for compliance It focuses on whether a certain issue is consistent with experts who have been designated as standards. Consistency inspecting entails determining if exercises, monetary exchanges, and data are, in all material respects, in accordance with the professionals in charge of the inspected element. Public-area reviews include something like three separate

gatherings: the evaluator, a party in question and expected clients. The connection between the gatherings ought to be seen inside the setting of the particular sacred game plans for each kind of review.

E. Materiality

Materiality is pertinent in all reviews. A subject can be judged to be important if the information included in it has the potential to influence the decisions of the intended clients.
Determining materiality requires expert judgement and relies on the reviewer's knowledge of the clients' needs. Materiality considerations impact the character, timing, and degree of overview structures, as well as the evaluation of overview findings.

F. Evidence

Proof evaluation proof is any records used by the examiner to determine if the topic is of the same opinion with the pertinent models. Proof can take several forms, including electronic and paper records of interactions, written and electronic contact with pariahs, the evaluator's impressions, and the examined substance's oral or written declaration. Strategies for getting review proof can incorporate assessment, perception, request, affirmation, recalculation, re-performance, scientific methods as well as other examination procedures.

G. Shared data

Data that is shared in any case, the Cloud is vulnerable to a variety of security and protection threats. As previously said, the most significant impediment to the Cloud's progress and widespread use is the security and safety concerns it raises. Obviously, many security and protection attacks originate from within the Cloud provider, since they typically have direct access to store information and remove it to sell to outsiders for profit. As seen, there are several instances of this scenario in actuality.

The following are some of the most important requirements for securing data in the cloud. To begin, the data owner must be able to specify a group of customers who are authorized to view their information. Any member of the group should be able to access the data at any time and from any location without the need for the records owner's intervention.

Nobody, aside from the information owner and the people from the collection, need to get close sufficient to the information, consisting of the Cloud provider company. The data owner must likewise have the choice to deny get entry to privileges towards any man or woman from the gathering over their commonplace records.

No character from the collection must be approved to repudiate freedoms or be a part of new clients to the collection. One insignificant solution for engaging in cozy facts participating in the Cloud is for the records proprietor to scramble his records prior to placing away into the Cloud, and consequently the records continue to be facts hypothetically comfy in opposition to the Cloud supplier and different vindictive clients.

At the factor whilst the records owner wishes to share his information to a meeting, he sends the key utilized for records encryption to every individual from the gathering. Dispensed computing and how work may be forestalled protection and safety breaks of 1's very own records in the Cloud. It investigated elements that affect overseeing facts safety in Cloud figuring. It makes experience of the critical safety desires for ventures to get the factors of facts safety inside the Cloud.

H. Cloud computing

The following are some of the most important requirements for securing data in the cloud. To begin, the data owner must be able to specify a group of customers who are authorised to view their information. Any member of the group should be able to access the data at any time and from any location without the need for the records owner's intervention.

"Distributed computing is a concept for providing a shared pool of customizable processing property (such as networks, servers, capacity packages, and administrations) that can be easily furnished and delivered with low administrative effort to a helpful, on-request community." Virtual Private Network (VPN) administrations with almost equivalent management at a substantially lower cost.

At first before VPN, they gave committed highlight point information circuits which was a wastage of data transmission. Yet, by utilizing VPN administrations, they can change traffic to adjust use of the general organization. Distributed computing currently stretches out this to cover servers and organization foundation.

II.RELATED WORK

In the Existing framework, Iolus approach proposed the thought of pecking order subgroup for adaptable and secure multi-cloud. In open examining for shared information denial, a huge correspondence bunch is partitioned into more modest subgroups. At a point when a gathering part joins or leaves just influence subgroup just while the other subgroup won't be impacted.

It has the downside of influencing information way. This happens as in there is a requirement for deciphering the information that goes from one subgroup, and consequently one key, to another. This arise to be significantly more hazardous when it considers that the PDP needs to deal with the subgroup and play out the interpretation required.

Designers with inventive ideas for new Internet services will no longer need to invest heavily in technology or

human resources to run them. In this study, G. Ateniese, R. Consumes, and others proposed proved information ownership (PDP), which allows a buyer who has saved facts at an untrusted server to test that the server owns the initial information without having to recover it.
By detecting irregular square preparations from the server, the model provides probabilistic Evidences of Possession, which cuts I/O costs dramatically. The client keeps a consistent measure of metadata to examine the evidence. The test/reaction convention limits network communication by transmitting a modest, continuous quantity of data. Under this study, H. Shacham and B. Waters, et al. [4] argue that in a proof-of-retrievability architecture, an information stockpiling focus should demonstrate to a Verifier that he is genuinely keeping all of a client's information. The main goal is to create structures that are both artistic and reassuringly comfortable.

To help talented treatment of various examining assignments, In this further investigate the procedure Of bilinear overall mark to make bigger our primary outcome into a multi-consumer setting, in which TPA can play out one-of-a-kind evaluating errands at the identical time.

III.PROPOSED SYSTEM

CP-HABE is a revolutionary multi-cloud authentication convention that includes two plans. Every subgroup is treated as if it were a separate multi-cloud group, with a trusted security middle person personality in charge. Hierarchal Attribute Primarily based scattered proven information ownership (CP-HABE). This is a useful feature, especially for large-scale network architectures, because it eliminates the problem of concentrating responsibility on a single piece.

A. PANDA Overview

In light of the new intermediary re-signature plot and its properties in the past area, in this currently present Panda a public evaluating system For imparted records to gifted client denial.

In our approach, the initial customer serves as the gathering director, with the authority to disavow clients from the gathering as necessary. Allow the cloud to continue in the meanwhile since the semi-confident in intermediate and decipher markings for customers in the amassing with keys. As previously stated in continuing work, it is critical for cloud specialist firms to capacity information and keys independently on multiple servers inside the cloud over time for the purpose of security.

As a result, in our system, we'll assume the cloud contains a server for storing shared data and another for overseeing key management. Extra components, for example, can be employed to ensure the security of cloud shared information at the same time. The finer points of information security are outside the scope of this study.

The principle focal factor of the paper is to review uprightness of cloud shared information.

B. Support Dynamic Data

Another problem to consider while putting together the entire instrument is how to assist dynamic information during public evaluation. Because the square identifier is included in the computation of a mark, traditional procedures - which use the square's record as the square identifier - are ineffective. In particular, assuming a solitary square is embedded or erased, the records of squares that after this adjusted square are totally different, and the difference in those lists requires the client to re-register marks on those squares, Despite the fact that the squares' content remains unchanged.

By leveraging record hash tables, a client will be able to efficiently change a single square without affecting the square IDs of other squares. In Appendix A, the nuances of record hash tables are explained. Each square is also connected with an underwriter identifier in addition to a square identifier and a signature.

An underwriter identifier can be used by a verifier to determine which key is expected during confirmation, and it can also be used by the cloud to determine which re-marking key is required during client repudiation.

C. Construction of Panda

Panda does the following six calculations: Proof Gen, Proof Verify, Key Gen, Re Key, Sign, Re Sign, Proof Gen, Proof Verify Each client in the gathering produces his or her own public and private key in Key Gen. In Re Key, the cloud processes a re-marking key for each Sets of customers within the accumulating. In event that the outcome, the verifier accepts that the uprightness of the relative multitude of squares in shared records M is proper. In any case, the public verifier yields zero.

D. Overall problem description

A measure of cryptography procedure Is presented in the current situation. There are many benefits and impediments during the ones calculation. Cryptography by means of utilizing encryption and decoding techniques it changes the data from typical structure over to disjointed structure so the data is gone through One of a type cloud organizations and is available to all assailants. The cryptography ensures that the records inside the cloud server should be sent with none modifications and best the approved person might be equipped for open and perused the documents.

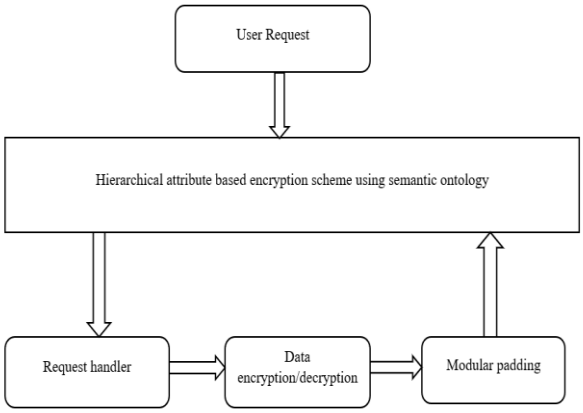


Figure 1. Data flow diagram

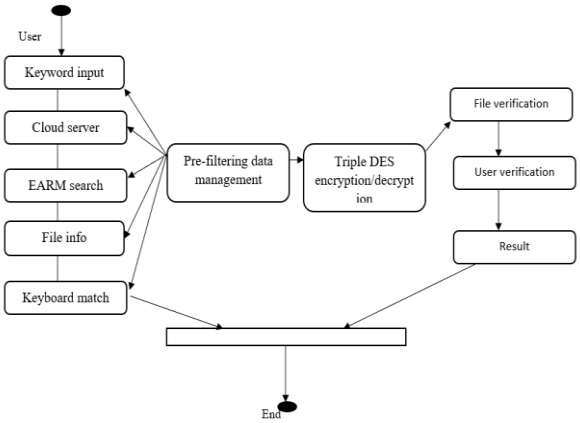


Figure 2. System flow diagram

E. Multi cloud group member registration & login

The most important The user enters a username, a secret word, and selects a gathering id before registering with Data Cloud Server. This particular gathering was included in the client's request. Then, for login, input the username, secret phrase, and the client's collecting id.

F. Efficient key generation & controller using CP-HABE

Each client in the gathering generates a public and private key in the Key Generation module.
The client generates an irregular public key and private key. Accept client u1 as the initial client in the process, who is the creator of shared information, without oversimplification. The initial customer also creates a purchaser list (UL), which contains the ids of the collection's relative number of consumers. The client list is open to the public and has been endorsed by the first client.

G. Upload file to data multi cloud server

The client is responsible for transferring a file. As a consequence, the client partitioned the data into several squares. After that, encrypt each square with the public key. For validation reasons, the client then creates a mark for each square. Then provide the signature, block id, and endorser id for each square code text. These details and information are maintained in Public Verifier and are accessible to anybody.

H. Download file from data multi cloud server

A record must be downloaded by the next client or gathering component. As a result, the client provides the filename and receives the mysterious key. Then there was this mysterious key. On the off chance that this mysterious key is genuine, the client is prepared to decrypt the downloaded document. Otherwise, if the subsequent client input the erroneous mystery key, Public Verifier will block the user1. In the event that this mystery key is legitimate, decode each square and confirm the mark.

I. Public auditing with user collision in public verifier

In the public verifier technique, the user who supplied an unacceptable mystery key was subsequently obstructed by the public verifier.
After that, the client added a list of public verifier impact clients to the mix. After that, the client must try to download any record, and the Data Cloud Server must reply to his data being impeded. The client then has to un-crash, so they seek help from the public verifier. This client was finally unrevoked by the public verifier. The client is now ready to download any document that has a secret key associated with it. When a client in the gathering crashes, the Data Cloud Server can re-sign the squares that were encouraged by the impact client using this technique, which makes use of the capability of intermediary re-marks.

IV.OUTPUT

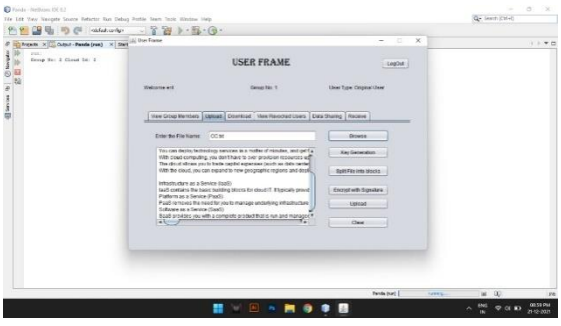


Figure 3. Uploading file in cloud

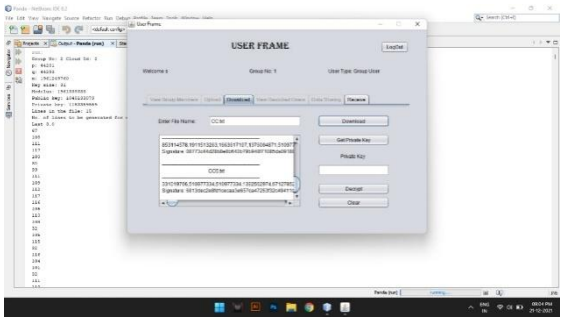


Figure 4. Download

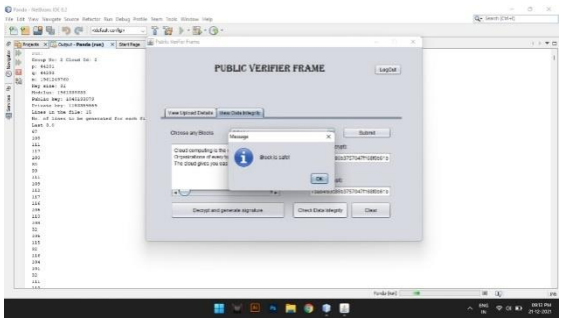


Figure 5. Security of file

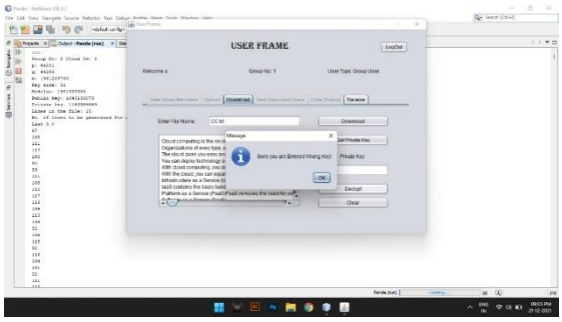
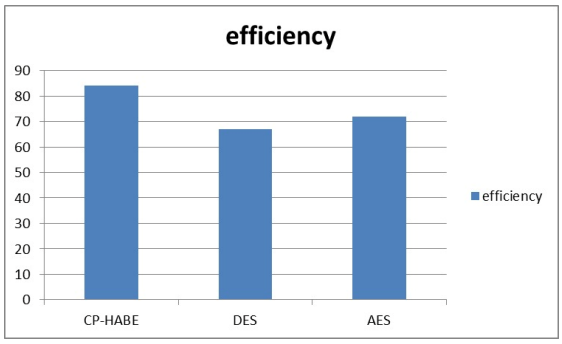


Figure 6. Data integrity

IV.RESULTS AND DISCUSSION

When a group member's access is revoked, the semi-trusted cloud can utilize proxy re-signatures to re-sign blocks that the revoked user has previously signed. According to the findings of the trials, the cloud may improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation. Our data in the cloud was successfully and safely merged with the other end cloud users using cypher text policy based hierarchal attribute based distributed verifiable data possession. In the this the data can be exchanged from users of same group but in the future work we can able to exchange the data from one group user to other group users that is from google cloud to amazon cloud. This part of implementation of exchanging the data across same group users with integrity is successful.

ALGORITHM	EFFICIENCY
CP - HABE	84%
DES	67%
AES	72%



V.CONCLUSION

The semi-believed cloud can re-signal squares that were encouraged by the disavowed patron employing intermediate re-marks when a client inside the gathering is renounced. The study's findings show that the cloud might increase the efficacy of client disavowal, and that current customers in the group could save a lot of time calculating and contacting clients during repudiation. With the assistance of code text strategy based hierarchal quality based circulated provable information ownership our Statistics inside the cloud were effectively and securely coordinated to the opposite end cloud clients. In the this the information can be traded from clients of same gathering yet later on work we can ready to trade the information from one gathering client to other gathering clients that is from google cloud to amazon cloud. This genuinely honest piece of execution of trading the information across same gathering clients is fruitful.

VI.REFERENCES

[1] B. Wang, B. Li and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, Jan.-Feb. 2015, doi: 10.1109/TSC.2013.2295611.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. 2010. A view of cloud computing. Commun. ACM 53, 4 (April 2010), 50–58. DOI:https://doi.org/10.1145/1721654.1721672.

[3] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner,

Zachary Peterson, and Dawn Song. 2007. Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA, 598–609. DOI:https://doi.org/10.1145/1315245.1315318.

[4] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.

[5] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, "Ensuring data storage security in Cloud Computing," 2009 17th International Workshop on Quality of Service, 2009, pp. 1-9, doi: 10.1109/IWQoS.2009.5201385.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011, doi: 10.1109/TPDS.2010.183.

[7] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," 2010 Proceedings IEEE INFOCOM, 2010, pp. 1-9, doi: 10.1109/INFCOM.2010.5462173.

[8] Y. Zhu, G. -J. Ahn, H. Hu, S. S. Yau, H. G. An and C. -J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," in IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227-238, April-June 2013, doi: 10.1109/TSC.2011.51.

[9] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," in IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, April-June 2012, doi: 10.1109/TSC.2011.24.

[10] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, “LT Codes-based Secure and Reliable Cloud Storage Service,” in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

[11] J. Yuan and S. Yu, “Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud,” in Proceedings of ACM ASIACCS-SCC’13, 2013.

[12] H. Wang, "Proxy Provable Data Possession in Public Clouds," in *IEEE Transactions on Services Computing*, vol. 6, no. 4, pp. 551-559, Oct.-Dec. 2013, doi: 10.1109/TSC.2012.35.

[13] B. Wang, B. Li and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," in IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43-56, Jan.-March 2014, doi: 10.1109/TCC.2014.2299807.