Reliable Sharing Of Data in Mobile Cloud Using CP-HABE Algorithm

Dr. S. Russia
Department of Computer Science and Engineering
Velalar College of Engineering and Technology
Thindal, Erode – 638012

Abisaran E
Department of Computer Science and Engineering
Velalar College of Engineering and Technology
Thindal, Erode – 638012

Gurudeva T
Department of Computer Science and Engineering
Velalar College of Engineering and Technology
Thindal, Erode – 638012

Jegathsuriya P
Department of Computer Science and Engineering
Velalar College of Engineering and Technology
Thindal, Erode – 638012

Abstract—Users of the cloud can validate the data integrity without downloading the complete file thanks to Provable Data Possession (PDP). Every PDP scheme currently in use depends on public key infrastructure (PKI). The system allows private, delegated, and public verification and is effective and adaptable. Due to its inability to attain soundness, ID-DPDP has a defect. Address the problem by offering a standardized construction. By incorporating several clouds into the original ID-PDP protocol, a new ID-DPDP protocol is created. Users may quickly change and share data among themselves using cloud-based data storage and sharing services. Each block of shared data must have signatures calculated by group members to ensure that third parties can independently verify its integrity. Separate blocks of shared data are often signed by different users due to data modifications made by several users. For security concerns, the blocks that were previously signed by a user who has been kicked out of the group must be re-signed by an active user.

Keywords—ID-PDP, Attribute based encryption, Cipher text-policy hierarchical attribute based encryption.

I. INTRODUCTION

Cloud Storage is a service where data is remotely maintained, managed, and backed up. An innovative form of Internet-based computing called cloud computing offers easy, on-demand network access. Provable Data Possession (PDP) samples random sets of blocks to check the data's integrity.

Cloud Computing

The term "cloud computing" describes a computing system in which one party can outsource its processing needs to another party, which can then use the computing power or resources, such as databases or emails, as needed. Cloud computing has caused a shift in computation and data from desktop and mobile devices to enormous data centers. Users don't have to pay for infrastructure expenditures like installation, upkeep, and necessary manpower, which is the core advantage of cloud computing.

As service providers started deploying virtual private network (VPN) services for data communications, the word "cloud" first appeared in the telecommunications industry. Cloud computing is the delivery of processing, software, data access, and storage services without necessarily requiring end-user awareness of the physical location and system setup. With the advent of cloud computing, processing and data are being moved from desktop and mobile Computers to huge data centers.

A concept known as "cloud computing" permits quick supply and release of a pool of shared reconfigurable computing resources (such as networks, servers, storage applications, and services) with little administrative labor or service provider interaction.

Services from virtual private networks (VPNs) that offer equivalent service quality at a considerably lesser price. Prior to VPN, they first offered specialized point-to-point data lines, which wasted bandwidth. Yet, they may change traffic to balance network usage by employing VPN services. This now includes servers and network infrastructure thanks to cloud computing.

Specifications of Cloud Computing

No matter what device they are using or where they are, cloud computing users can use a browser to access data, applications, and other services. Infrastructure that is normally provided by a third party is accessed over the internet. The cost is greatly reduced because the infrastructure is offered by a third party rather than having to be bought for irregular use. Rehabilitation and continued operations. Sadly, there are times when a lot of cloud computing services go down, leaving their users essentially powerless.

Infrastructure may be used effectively when expenditures and resources are shared across a lot of users. Because they do not need to be installed on every user's computer, maintenance is simpler with cloud computing. Infrastructure may be used effectively when expenditures and resources are shared across a lot of users. Because they do not need to be installed on every user's computer, maintenance is simpler with cloud computing.

Due to providers' ability to allocate resources to addressing security challenges that many customers cannot pay, security can be as good as or better than traditional systems. Even though the data is fairly private, security is still a major worry. This slows down the spread of cloud computing a little.

A cloud client is a piece of computer hardware or software that uses cloud computing to provide applications or that is created particularly to deliver cloud services. A cloud application eliminates the requirement to install and operate the application on the user's computer by delivering "Software as a Service (SaaS)" over the internet. Platform solutions. A platform is provided via "Platform as a Service (PaaS)" employing cloud infrastructure.

Infrastructure services are the necessary infrastructure as a service, or "Infrastructure as a Service (IA as)". Clients are not needed to buy the necessary servers, datacenter, or network resources.

A. Shared Data

The Cloud, however, is vulnerable to numerous security and privacy assaults. According to, the privacy and security concerns around the Cloud are the main impediment to its development and widespread use. While the Cloud provider typically has direct access to the stored data and steals the data in order to sell it to other parties for profit, it is evident that many privacy and security threats originate from within the Cloud provider itself. As was noted, there are several examples of this occurring in reality. There is a critical need to disseminate information to groups of people worldwide in today's world. Many consumers are still wary of trusting their most important data with the Cloud due to the numerous privacy risks it has with other users.

Some of the essential elements for secure data communication in the cloud are the ones listed below. The data owner should initially be able to specify a set of people who are allowed to read that data. Any group member should be able to view the data at any time, from anywhere, without the data owner's participation. Only the group members and the data owner should have access to the data, not the Cloud Service Provider. The owner of the data should permit the addition of new users to the group. The owner of the shared data should also be able to revoke any group member's access privileges. The owner of the data should permit the addition of new users to the group. Access privileges for any group member should also be revocable by the owner of the shared data. New users should be able to join the group with the permission of the data owner. Access privileges for any group member should also be revocable by the owner of the shared data. No group member should have the authority to alter the composition of the group.

If the data owner encrypts his data before keeping it there, the data will stay information-theoretically secure against the cloud provider and other malevolent users. This is a simple method for securely sharing data on the cloud. The encryption key is sent to each group member when the data owner wants to share his material with others.

The revoked member's key is no longer useful since the data owner needs to re-encrypt the information using a new key. The new key must be distributed to the group's remaining users when the data is re-encrypted, which wastes computational resources and puts an undue strain on the data owner for huge group sizes that could number in the millions of people.

What can be done to prevent security and privacy breaches of a person's personal data on the cloud using cloud computing? It examined variables that have an impact on cloud computing information security management. It covers the fundamental security requirements for businesses to comprehend the dynamics of cloud-based information security. For data sharing, cloud models like Platform-As-A-Service (PaaS) and specifically Infrastructure-As-A-Service (IA as) are required. In order to assess the user experience of cloud computing, a number of users were polled. It was discovered that all users' top concerns were trust and how to select the best Cloud Service Provider.

The impact of the Internet on information exchange between many organizations, including businesses and government agencies. Record matching, query restriction, and data distribution are the three categories into which they split data sharing. They also provide a framework for efficient and secure data sharing online. This is advantageous because it alerts organizations to the possibility that the data, they decide to make public may still raise privacy issues and may not guarantee user anonymity.

II. LITERATURE REVIEW

1*A view of cloud computing*

In this work, M.Armbrust, A. FoxPro. Griffith, et.al [2] has proposed the long-held concept of computing as a utility, cloud computing, has the potential to revolutionize a significant portion of the IT sector by increasing the appeal of software as a service and influencing the creation and acquisition of IT hardware. Innovative Internet service providers no longer need to invest significant sums of money in expensive gear or hire a huge staff to run it.

The term "cloud computing" describes both the hardware and system software in the datacenters that provide the applications as services via the Internet. Long-standing terminology for the services is "Software as a Service" (SaaS). We'll refer to the hardware and software in datacenters as a cloud. We refer to a Cloud as a Public Cloud when it is made available to the general public on a pay-as-you-go basis; the service being offered is Utility Computing. The internal datacenters of a company or other organization that are closed off to the broader public are referred to as private clouds.

2 *Provable Data Possession at Untrusted Stores*

In this work, G.Ateniese, R. Burns,et.al[3] has proposed Provable data possession (PDP) enables a client to save data on an untrusted server and to confirm, without retrieving the data, that the server actually has the original data. The model significantly lowers I/O costs by generating probabilistic proofs of possession from samples of random sets of server-side blocks. To validate the proof, the client keeps a consistent quantity of metadata. The challenge/response protocol minimizes network communication by transmitting a small, constant quantity of data.

Provable Data Possession (PDP), which offers probabilistic evidence that someone else is keeping a file. The model differs from all other strategies in that it permits the server to access only a limited amount of the file in order to produce the proof. We provide the first remote data verification mechanism that can be proven to be secure inside this model. To validate the server's proof, the client stores a modest quantity of metadata.

3 *Compact Proofs of Irretrievability*

In this work, H. Shachamand B. Waters,et.al [4] has proposed A data storage canter must demonstrate to a verifier that it is genuinely storing all of a client's data in a proof-of-irretrievability system. Building systems that are both effective and indubitably secure is the main difficulty. a technique for proving irretrievability where the client query and server response are both very brief.

With cryptographic methods, customers of external storage services (or their representatives) could confirm that their data is still accessible and prepared for retrieval, should the need arise. Storage providers may find value in such a capacity as well. Consumers can be hesitant to give their data to a startup they don't know; an auditing method might reassure them that their data is still accessible.

The most crucial crypto metric test is whether the protocol genuinely stipulates that any server, including hostile servers that display arbitrary, early papers on cryptography lacked formal security models and even proofs.

4 *Ensuring Data Storage Security in Cloud Computing*

Cloud computing moves databases and application software to massive data Centre’s, where the management of the data and services may not be totally dependable. The data that is saved in the cloud can routinely be added to, removed from, modified, appended, and reordered, etc. by users. Consequently, when updating

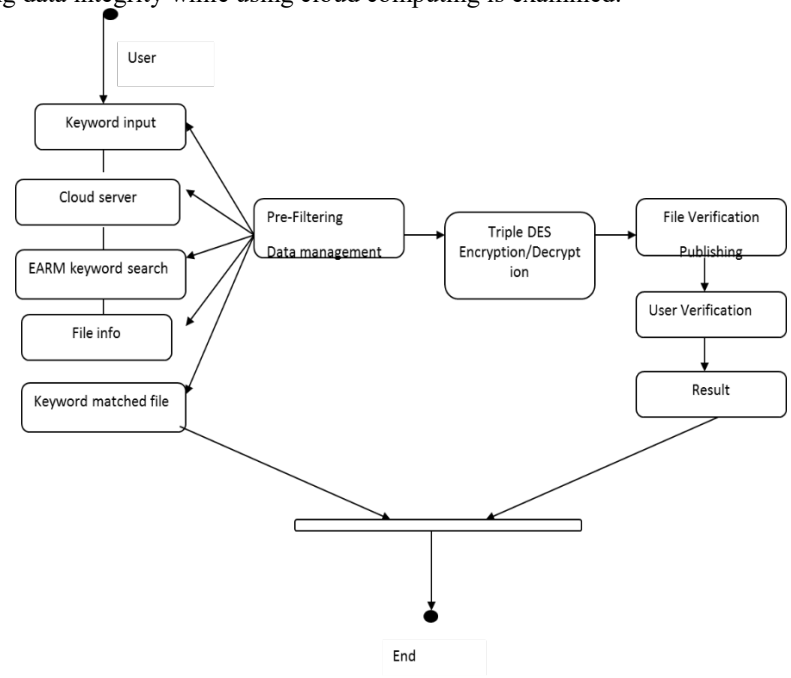
dynamic data, it is imperative to preserve storage correctness. a reliable distributed system that is efficient and flexible and has explicit support for dynamic data.
Security issues of two main categories can affect cloud data storage. A CSP may be vested in their own interests, unreliable, and even malignant. The adversary wants to tamper with user data files that are housed on individual servers.

5 Key-Policy Attribute-Based Encryption

A cryptographic concept that is frequently used to implement granular access control systems for encrypted data. In the key-policy flavor, access structures that define which cipher texts a user is allowed to decrypt are coupled with secret keys and used to annotate cipher texts. In the majority of key-policy attribute-based encryption (KP-ABE) constructions now in use, the size of the cipher text is proportional to the number of attributes associated with it, and the cost of decryption is related to the number of attributes used during decryption. In this paper, we introduce a novel KP-ABE construction. The KP-ABE system we propose is the first to combine constant-size cipher texts, rapid decryption, expressiveness, and robustness (allowing arbitrary monotonic access patterns). Our design's flaw is that there are twice as many properties for secret keys.

III. METHODS

The next generation IT enterprise design has been envisioned as being based on cloud computing. It transfers the databases and application software to the centralized, massive data Centre's, in which the administration of the information and services could not be completely reliable. Several new security concerns are presented by this distinct paradigm, many of which are poorly understood. In this piece, the issue of preserving data integrity while using cloud computing is examined.



A. Multi Cloud Group Member Registration & Login

After entering their username and password in this module, the first user selects a group id and registers with Data Cloud Server. This user joined the group in question. He then chose his group ID and entered this username and password.

B. Efficient Key Generation & Controller using CP-HABE

Each user in the group creates a public key and a private key using the Key Generation module. The user creates a random number and outputs both the public and private keys. Without sacrificing generality, let's assume that user u1 is the original user and the one who created the shared data. In addition, the initial user produces a user list (UL) that contains the IDs of each user in the group. The original user has signed the public user list.

C. Upload File to Data Multi Cloud Server

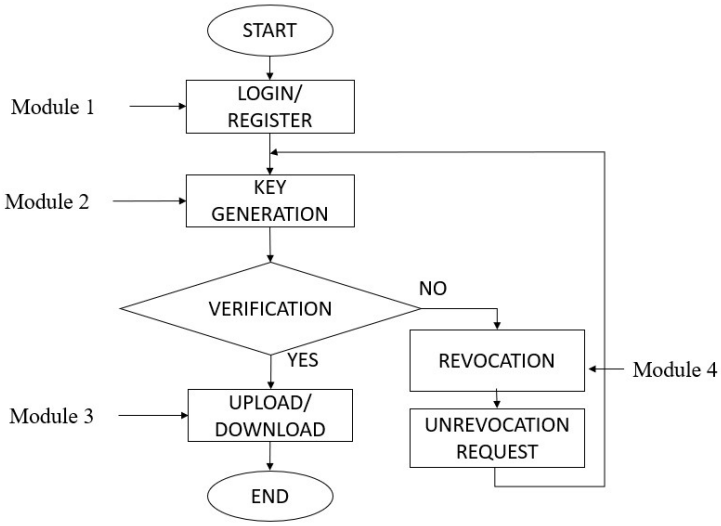
A file upload is requested by the user. The user then divided the files into several blocks. Next, use the public key to encrypt each block. The user then creates a signature for each block for the purpose of authentication. Then, upload each block cypher text together with the block id, signer id, and signature. For public auditing, these metadata and Key Details are kept in Public Verifier.

D. Download File from Data Multi Cloud Server

The following user or group participant requests a file download. The user then receives the secret key after providing the filename. This hidden key was then input. The user will be able to decode this downloaded file if this secret key is genuine. If the following user submitted the incorrect secret key, user 1 would then be blocked by the Public Verifier. Verify the signature on each block and decrypt it if this secret key is genuine. Combine all the blocks to obtain the original file if the two signatures are identical.

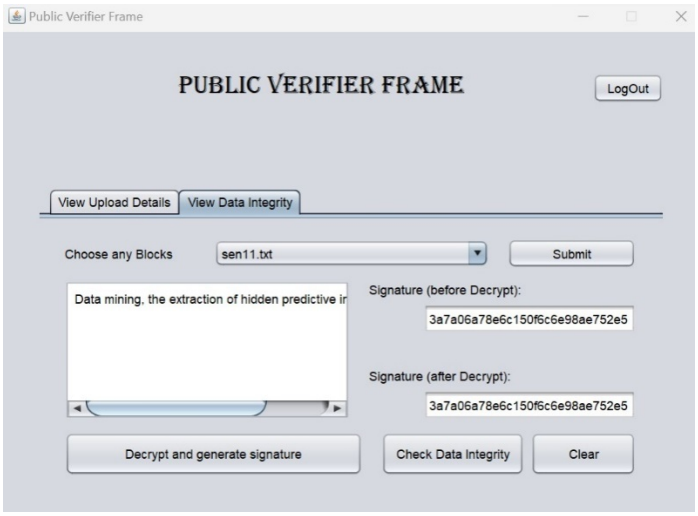
E. Public Auditing With User Collision In Public Verifier

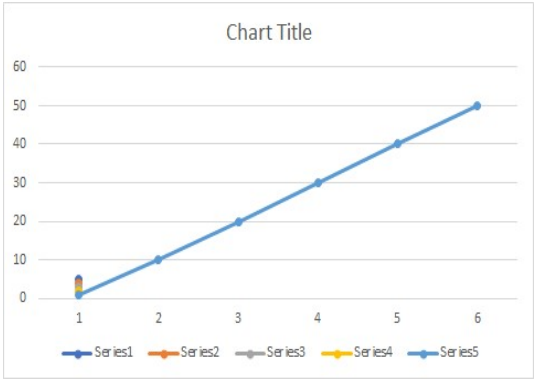
In the public verifier approach, the user who entered the incorrect secret key was subsequently blocked. The user then added a list of public verifier collision users. When a user tries to download a file, the Data Cloud Server responds with information about why it has been banned. The user then asks the public verifier to resolve the collision. The public verifier finally restored this user's account. The user can then use any file's accompanying secret key to download it. In this method, once a user in the group is collision, the Data Cloud Server can re-sign the blocks that were signed by the collision user with a resigning key by utilizing the concept of proxy re-signatures.



IV. RESULT

An amount of cryptography technique is introduced in the current scenario. There are many advantages and disadvantages in the algorithms. Cryptography via using encryption and decryption methods it converts the information from normal form to unreadable form so that the information is travelled through unique cloud networks and is open to all attackers. The cryptography guarantees that the files inside the cloud server need to be sent with none alterations and best the authorized character may be capable of open and read the files.





V. CONCLUSION

It was decided to rethink the identity-based distributed verified data possession approach for multi-cloud storage. The server is still able to provide an accurate certification that the data are still stored intact. A generic ID-PDP protocol design was created, and its security was proven, using wide signature schemes and well-known PDP protocols. We created the ID-PDP protocol itself as well as an enhanced version that is suitable for multi-cloud storage environments. A brand-new open auditing mechanism for shared data in the cloud that enables effective user revocation was also demonstrated. We authorize the semi-trusted cloud to resign blocks that were previously signed by a group member whose membership has been cancelled using proxy re-signatures. The test results demonstrate that the cloud may both benefit current network users and increase the efficiency of user revocation. For multi-cloud storage, the identity-based distributed verified data possession solution was examined. Nonetheless, the server can offer a reliable guarantee that the data are still secure. Broad signature schemes and well-known PDP protocols were used to construct a general design for ID-PDP protocols and demonstrate their security. We developed a genuine ID-PDP protocol in addition to an expanded version that works well in a multi-cloud storage scenario. We also unveiled a fresh, open auditing method for cloud-based shared data that has effective user revocation. When a group member's membership is revoked, we permit the semi-trusted cloud to employ proxy re-signatures to resign blocks that were previously signed by the withdrawn user. The test findings demonstrate that by lowering the amount of computation and communication resources needed for user revocation, the cloud can increase user revocation's effectiveness and benefit current group members. A large amount of computing and communication resources can be saved by current group members after user revocation.

REFERENCES

[1]. Armbrust M, Fox A, Griffith R, Joseph A.D, Katz R. H, Konwinski A., Lee G., Patterson D. A, Rabkin A, Stoica I., and Zaharia M, “A View of Cloud Computing,” Communications of the ACM.

[2]. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.
[3]. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.
[4]. Cao N, Yu S, Yang Z, Lou W, and Hou Y.T, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.
[5]. Shacham H and Waters B, "Compact Proofs of Retrievability," in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.
[6]. Tate S.R., Vishwanathan R, and Everhart L, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware," in Proceedings of ACM CODASPY'13, 2013, pp. 353–364.
[7]. Wang B., Li B, and Li H, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.
[8]. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
[9]. Wang C., Wang Q, Ren K, and Lou W, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.
[10]. Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
[11]. Wang Q, Wang C, Li J, Ren K, and Lou W, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.
[12]. Wang C, Wang Q, Ren K, and Lou W, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.
[13]. Wang C., Wang Q., Ren K, and Lou W, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.
[14]. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.