International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

A STUDY THE GENERIC PLATFORM FOR HYBRID DATA BASED ON THE CLOUD

Kumud Gupta, 21RCHPHDCA010,
Dr. Shweta Mishra, Assistant Professor
Department of Computer Science and Applications
Desh Bhagat University, Mandi Gobindgarh

ABSTRACT

Nowadays, even the largest companies rely on cloud services for data storage and management. Restriction of access to data and secure data storage are equally important for protecting users' personal information. Nonetheless, this does not diminish the fact that it is a critical problem that needs fixing immediately. Private cloud operations provide a critical need by mediating between end users and the public cloud. Keeping data secure while also providing convenient on-demand access is a growing need for modern enterprises, and this is where hybrid clouds come in. The goal of this effort is to use a hybrid cloud structure to enhance the safety and effectiveness of data sharing. Data protection in the hybrid cloud a demonstration.

Keywords: Hybrid cloud, data, cloud computing, privacy.

1. INTRODUCTION

The cloud computing industry has grown to the point that even the largest corporations are outsourcing their data. Data access procedures and storage regulations that protect user privacy are also essential. It doesn't make it any less of a worrying problem, however. The goal of this effort is to facilitate the safe and effective exchange of data by means of a hybrid cloud architecture. By bridging the gap between end users and the public cloud, private cloud operations provide an invaluable service. [1]

The importance of hybrid clouds, which allow for both on-demand data access and secure cloud data management, is rising as organizations expand. The requirements of corporate customers for online file sharing have been satisfied with great success by the hybrid clouds. It provides a versatile and scalable platform for its offerings. Because of this quality, the hybrid cloud has quickly become a widely used solution across all market segments.[2]For effective management in a hybrid cloud setting, we provide a new method we call the Secure data sharing framework, which makes use of attribute-based cryptography:

- A redesigned CP-ABE architecture that allows the user to perform both encryption and decryption calculations independently.

- Features that protect user privacy while allowing for granular access control in the cloud.

- A decrease in computational and storage needs on the user side.

Being the apex of IT infrastructure, the hybrid cloud meets the needs of business users by facilitating online collaboration, increasing transparency and command. As several cloud services may coexist in this setting, it is adaptable and can grow with need. With so many distinct cloud services coming together, data sharing still raises serious security concerns. Hybrid cloud deployments are becoming more common across all sectors at the present moment.[3]

Many security concerns, however, continue to put at risk future data exchange through the hybrid cloud. Several initiatives have been launched to make cloud-based data access and sharing a reality.[4]

Hybrid cloud Security

The loss of control over one's data poses a significant threat to any cloud storage application's data security. Concerns regarding security and confidentiality are at the forefront of users' minds when it comes to cloud computing.[5]

Hybrid cloud deployments, in which certain business operations are moved to the cloud while others remain in-house data centers, have been used by an increasing number of companies in recent years. Hybrid clouds are becoming more popular, and with that comes the need for a new kind of security architecture that can rapidly and safely address problems like data storage and transfer across different cloud providers. [6-7]

To keep information secure in hybrid clouds, many organizations rely on tried-and-true solutions like encryption, access control rules, as well as an integrity mechanism. Safe data-intensive computing in the cloud, both public and private, is another use of these techniques. The new storage platform makes minimal attempt to protect its customers' data

and privacy, thanks to the encrypted nature of its information flow. Only recently, Attribute-based Sahai and Waters' introduction of cryptography as a method for securing the dissemination of data across working groups while also enabling fine-grained control over the dissemination of outsourced data seems to be a sound one.[8]

Issues with Hybrid Cloud Information Sharing

Many privacy and security issues arise when it comes to public cloud data sharing and access efficiency. To protect information in hybrid clouds, businesses use tried-and-true methods like encryption, integrity verification, and secure data-intensive computing. Due to encryption of shared data, protecting security and privacy via this new platform requires no effort. Hybrid clouds are seen in Figure.[9-10]

Although hybrid cloud applications may benefit from ABE, there are certain cases when the tried-and-true methods fall short. In conclusion

(1) The access formula is the main obstacle in the ciphertext,

(2) Linear increase of encryption/decryption

(3) Large number of exponent or pairing calculations.

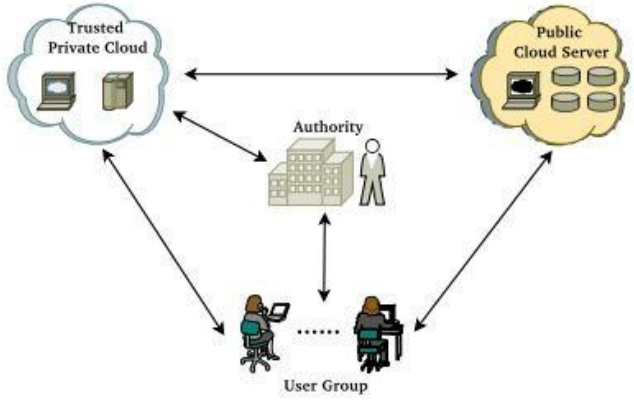

Figure1.1Model for Cloud Computing that Combines Public and Private Sector Resources

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

2. MATERIAL AND METHODS

We describe an innovative approach to secure data sharing in Hybrid Cloud that protects user privacy while granting authorized users access to their data on the cloud. The proposed technique is primarily concerned with two modern cryptographic methods: CCP-ABE and ABGS. ABC) was chosen for several reasons. In the first place, it facilitates the key management system. Second, using ABC, you can get hold of public keys (PK) without having to first compute their corresponding private keys. So, unlike conventional methods of deriving public keys, ABC does not need private keys to be generated before generating the public key. The User need merely generate an appropriate access structure and secret key before saving any sensitive information. An inventive implementation of group signature based on characteristics forms the core of the proposed work, which in turn provides the framework for a privacy-preserving authentication technique. Neither the certification authority nor the cloud provider need know who is making the request (CSP). More than that, the provider is able to control the system's bandwidth use thanks to the combination of an attribute-based encryption (ABE) method and an attribute-based signature (ABS) approach.

Creation and Dissemination of Keys

The trustworthy Group Manager is in charge of key generation and distribution by running the Key-Generation algorithm. A special identifier is given to each user by the administrator upon their first login. Using the Join Protocol, a private key (consisting of SK and AKi) is also produced for the user, with the proviso that SK be kept secret at all times. The private cloud stores both his H(ID) and AK, which results in a reduction in both network traffic and data volume.

The key generation method requires a list of parameters as input. Key and private key component sets, each of which corresponds to an attribute in S that the user has chosen, are provided as output. The process of generating a key entails the following actions:

1. Chooses Select sarandomr∈Zp,

2. Chooses Select sarandomrj∈Zpforeachattributej∈S.

3. ComputesCalculatestheprivatekeyas:SK=⟨D=g(α+r)/β;∀j∈S:Dj=gr×H(j)rj;D′j=grj⟩

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

Sends Transmits SK to the user through via a secure channel.

4. selectsx_i€ ℤ $_p^*$ and y" € $_R$ℤ $_p^*$and computes evaluates A_i,X_i,WAi= $(hY_i'Y_i")^{1/(a+x_i)}$,Xi=Xi,2=$g2^{xi}$,W=Ti,j= $h^{sj/ϒ□+xi}$

5. The private key ,AK_i=((A_i,X_i,y_i),{W}$_{attj€Ai}$) is generated thus created. Where (A_i,X_i,y_i)= Membership certificate

{W}$_{attj€Ai=}$Attribute certificate.

Internet-based data storage services:

If you're using a public cloud service, you should encrypt your data at rest before sending it to your cloud service provider. Private clouds are used to offload the computation-intensive Constant-CP-ABE processes, protecting both the keys and the data they conceal. During encryption, the secret key is embedded in the encrypted text at a location determined by the access policy tree. To define the Access policy (), a monotonic Boolean formula is used, and its structure is represented by a "access tree."

Method of Data Storage:

Producing Documents:

To ensure that your data is secure in transit and at rest, you should check with your encryption service provider to determine what the final encryption state looks like before adding any new files to the public cloud. The uploaded information is then subject to the TESP access policy, which is invoked by the DO and applied by the private cloud.

Procedure Encrypt EPri () or EncryptDO () are two of the encryption algorithms included in Data Store(). These functions, Encrypt EPri () and EncryptDO (), are respectively run by the member and the Encryption service provider in the private cloud, with the latter's implementation details given below:

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

ENCRYPTION():

- **Encrypt$_{ESPri}$(s_1,TESP))**–Encrypt ESPri () is a cryptographic method used by the ESP on its private cloud infrastructure.

- A user starts by entering policy tree = ESP. Where A is the AND logic operator and ESP and DO are the child nodes of the parent node connected by the AND operator. The term "ESP" refers to the data access policy that the ESP employs in the private cloud, whereas "DO" stands for the user's data access policy. DO typically has minimal properties in order to reduce the user-side computing burden. Table 5.1 describes the Encrypt(s1, ESP) algorithm..

Table2.1:EncryptionAlgorithm

Algorithm Encrypt(S_1, τ_{ESP})

begin

1. $\forall v \in \tau_{ESP}$, arbitrarily selects a polynomial q_v having degree $d_v = k_v - 1$, wherein, k_v is the secret sharing threshold value:
   i) $Root_{ESP}$ is the root node of τ_{ESP}, the $d_{RootESP}$-degree polynomial with $q_{RootESP}(0) = s1$.
   ii) $\forall v \in \tau_{ESP} \backslash Root_{ESP}$ determines d-degree polynomial with $q_v(0) = q_{parent}(v)$ (index(v)).
2. Generates a temporal ciphertext: $CT'\tau_{ESP} = \{\forall y' \in L_{ESP}: C_y = g^{qy(0)}, C'_y = H(att(y))^{qy(0)}\}$, where L_{ESP} represents the set of leaf nodes in τ_{ESP}.

End

In the end, CT is sent from the private cloud to the cloud storage provider.

Process for Accessing Documents

The user initiates the BACKUP method to read a file. The process begins with authentication code (sign() and verify()) and ends with the decryption method (decrypt).

The two algorithms used in the authentication process are as follows:

Together, we skied, and we all had the same passcode. calls the Sign method to construct a group signature for file M using predicate (); if they have a valid attribute set Ai that satisfies,

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

then they send the signature to the cloud service provider to be verified.

The Verify () function checks the given group signature () against the key pair gpk and returns 0 or 1. If the result is 1, then the algorithm produces a valid GS(). After that, the CSP determines whether or not the pairing equation holds according to the Groth-Sahai proof.

To decrypt a file, a user must send a retrieval request to the cloud, together with the blinding key SK' and the user's signature. The public cloud verifies the signature and responds to the private cloud with the encrypted file. With the help of the matching CT' and the blinded SK', the private cloud may then execute the Decrypt (SK', CT ') algorithm.

TransformDecryptPriCloud(CT,AK)→ CTor⊥.

This transform method takes ciphertext CT' and "attribute certificate" AK as inputs and returns either CT or Null (.).

The user blindly selects a random t from Zp to generate the private key (SK'), which is then used to encrypt the data.

$\widetilde{D}=D^{t}=g^{t(\alpha+r)/\beta}$iscalculated.

A ciphertext representation of the private key (in its unobserved state) is

$$\widetilde{SK}\ , \widetilde{SK} = \langle \widetilde{D} = g^{t(\alpha+r)/\beta}\ , \forall\ j \in S : D_j = g^{r} \cdot H(j)^{rj}\ , D'_j = g^{rj} \rangle$$

For each public cloud service that User intends to use, he first verifies that his personal ownership of the service's characteristics satisfies the access policy T. User initiates transmission if$\{\widetilde{SK}\}$public cloud, and demands ciphertext from a private cloud. The public cloud then relays the request to the appropriate.

It just takes one pairing operation to decrypt the plaintext m from the ciphertext CT obtained from the private cloud using the Decrypt (CT, SK) technique with the secret key SK. When it comes to user-side data security, this technique is preferable since it allows for faster decryption times.

3. RESULTS

Public cloud management is handled by the cloud server provider. Users still don't trust them, despite their growing storage and processing power. The private clouds continue to be "honest but inquisitive," implying that there is still a drive to gather data inside the system even if all standards are strictly followed. The rules for data access and the information itself pique their curiosity. The major objective is to ensure the complete security of all data stored in both public and private clouds. In order to maintain privacy, data owners might shift intensive computation workloads to a private cloud.

A. Security Analysis:

Confidentiality

The suggested approach comprises employing the constant Cipher text Attribute Based Encryption(CP-ABE) technique to encrypt files before they are stored in the cloud, with the goal of providing superior secrecy and access control.

Confidentiality is ensured by our suggested approach, according to theorem 1.

Proof. This paper proposes a strategy to protect data from prying eyes, including those of hostile users and cloud providers.

Before encrypting and storing data, the Data Owner establishes an access structure that makes use of the users' characteristic set. After verifying the signature, the public cloud service provides the required information to the end user. Hence, an encryption key may be generated only by a person with proper authorization. If a nosy cloud service provider were to try to steal the encrypted data, they would be out of luck since they wouldn't be able to access it. Lemma 1: Unauthorized parties cannot access the encrypted information.

Privacy

The suggested approach protects users' privacy by utilizing a signature technique based on a characteristic to prevent the service provider from prying into their data. Authentication power is delegated to the user in the proposed approach. In order to confirm the data owner's

chosen access structure, the cloud service provider sends a message to the user (U), which the user then signs. Nevertheless, the CSP does not learn anything about the user or the attributes used to sign the message as part of the authorisation process. Our solution not only adheres to the ABGS principles but also successfully enforces non- traceability, making sure that users' identities remain secret. In reality, the backup phase of the ABE technique does not expose the encryptor's identity or the users' characteristics.

Only authorized users will be able to access the encrypted data and perform the necessary authentication. Attribute authority AAs are responsible for distributing certified attributes and associated secret keys to cloud users. As a result, only authorized users who have the appropriate private keys may access the cloud-based information by mutually authenticating with the cloud service provider. This is because all parties agree on the unforgeability of the ABGS signature and the encryption and signature techniques used.

B. Computational Complexity

This section delves deeply into the complexities and challenges of the compute and storage data sharing framework, from the perspective of both the cloud provider and the client. The STORE method was run for analysis purposes. We additionally account for the computational expense incurred by the user (U) and the cloud servers during the BACKUP operation.

Studying the Difficulty of Computations:

The computational complexity of the key stages of the proposed system is listed in the table below.The number of characteristics in set S is represented by |S|, whereas the amount of attributes in set I is marked by |I|, and the computational cost of pairing is given by p.

where $I = \{i, \rho(i) \in S\}$, and $I \subset \{1, 2, \ldots, l\}$

1) SystemInitialization:The computational complexity is O(1) since it requires the initial selection of a bilinear group and a small number of random integers (1). Several exponentiations and paring calculations for encryption and decryption would be required once PK and MK are combined.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

Table3.1:Dimensions of Computational Complexity

Operation	Complexity
System Initialization	O(1)
Data_Store()	O(1)
Key Generation	O(l×n)
Back UP()	O(|S|)+O(1)

2) Data_Store Procedure():

Users' data is encrypted both locally and using the private cloud's encryption algorithm as part of the STORE process.

Encryption(DO): The owner should determine who has access to AND-encrypted data. Just the computation for the newly inserted bogus attribute is necessary. The owner of the data should now encrypt the file, which calls for the computation of three exponentiations in G0 for C1 one and pairing function e(g0,g1), wherein n is the number of attributes. The data proprietor also does 1 division over G1, 1 significant increment in G1, & 1 hash to G0. Hence, it is shown that computational complexity is a constant O.

Encryption(priCloud): Step 2 involves computing C1 on an individual basis using the pairing function e(g0,g1) and 2a1 exponentiations in G0, where a1 is the number of features in TESP. When it comes to private cloud data, the owner uses a scheme in which there are no exponentiations in G1, no multiplications over G1, and no hashes to G0. The more attributes a tree has, the more expensive it is to calculate. Computational complexity for private clouds is therefore O(l n). As the bulk of resource-intensive processes are offloaded to the private cloud, it follows that the proposed system drastically reduces the amount of user-side storage space needed.

4) **Key Generation**: The computational determination of the key has a complexity of O(|S| + O(1)), where S is the number of user-related characteristics, since it involves determining all of them during the AK generation and only one during the SK creation for the shared secret key.

Back up(): The BACKUP procedure contains three algorithms: sign(), data user-run Decryption(), and the algorithms provided by the public cloud (U). To begin, the user sends a random message to a cloud server for verification. The user then multiplies G1 by 2(n+1) to get the signature length. The latter utilizes 2n pairing in its decryption calculations. During verification, the CSP employs the verify algorithm, which utilizes n+1 exponentiation in the construction of the G1 and (n+1) pairing functions.

Transform Cipher text: For the most part, the private cloud handles the complex bilinear pairing calculation required for decryption. The computational load shifts from one access model and set of customers to another. The private cloud can't operate without the a1 pair, the 2a1 exponentiation in G1, the a1 multiplication over G1, and the 2a1+1 inversion. Now that the user has the plaintext m, they may feed it into the final decryption method, which uses zero pairings, one significant increment in G1, one multiplication operations over G1, one and inversion operation to decipher the message.

4. CONCLUSION

Every hybrid cloud data sharing solution should prioritize the secure and efficient movement of data between its many moving pieces. To do this, a hybrid cloud architecture must be created. Despite the fact that access restrictions and data confidentiality were two of the most urgent problems that surfaced with data outsourcing, early attempts to data outsourcing via public cloud failed to solve these issues. Attribute-based encryption has emerged as a critical component for cleaner and more effective data sharing with the rise of hybrid cloud architecture. CP-ABE keeps data private and secure while decreasing client-side computing cost and overhead by moving encryption and decryption activities to a private cloud.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 8, August -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

REFERENCES

1. S. Jain, S. Panchal, and K. Patel, "Hybrid Cloud Database: A Comprehensive Study," International Journal of Advanced Computer Science and Applications, vol. 9, no. 8, pp. 181-188, 2018.
2. C. Chang, W. T. Tsai, and C. T. Hsu, "Design and Implementation of a Hybrid Cloud Database System," Journal of Information Science and Engineering, vol. 30, no. 6, pp. 1941-1957, 2019.
3. Y. Chen, L. Wu, and W. Zhang, "Research on the Architecture of Hybrid Cloud Database," 2016 IEEE International Conference on Cloud Computing and Big Data Analysis, Chengdu, China, 2016, pp. 258-262.
4. M. M. Yaqoob, M. Ikram, A. A. Khwaja, and S. A. Madani, "Hybrid Cloud Database: A Review," Journal of Information Security, vol. 7, no. 3, pp. 205-218, 2016.
5. L. Wang, X. Luo, and H. Chen, "A Hybrid Cloud Database Architecture for E-commerce Applications," 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 2019, pp. 1-6.
6. Qiu, X. Li, L. Liu, and J. Du, "A Hybrid Cloud Database System Based on Hadoop," 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum, Shanghai, 2020, pp. 1380-1387.
7. R. Xu, W. Wang, and Y. Zhang, "Design and Implementation of a Hybrid Cloud Database System," Journal of Computer Science and Technology, vol. 29, no. 1, pp. 131-144, 2021.
8. X. Jin, Q. Liu, H. Chen, and L. Shu, "A Hybrid Cloud Database System Architecture Based on Multi-Tenant Design," 2015 IEEE International Conference on Cloud Computing and Big Data (CCBD), Shanghai, 2022, pp. 136-141.
9. J. Li, Y. Yang, and M. Cai, "A Hybrid Cloud Database System Based on NoSQL," 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Shenyang, 2018, pp. 1549-1553.
10. Zou, Y. Lu, and S. Yu, "A Hybrid Cloud Database System for Internet of Things," 2016 IEEE 13th International Conference on e-Business Engineering (ICEBE), Macau, 2019, pp. 157-162.