International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Generic Framework for Sharing Data Using Attribute Based Cryptography in Hybrid Cloud

E.Poornima*[1], Srinivasulu Sirisala[2], P.Dileep Kumar Reddy[3] ,G. Ramesh[4]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Now a days, large organizations are re-appropriating their information to the public cloud. But we should be cautious and improve the security about the data which is being shared. Maintaining the confidentiality among this public data is a major concern. To accomplish this a hybrid cloud Computing was intended to help safe & proficient contribution of information. Private cloud capacities go about as extension among clients & public cloud. As the organizations expand and create the hybrid Cloud requirement that can securely monitor information in clouds by entering interest. By providing online record sharing on the internet, the hybrid cloud has successfully met the needs of business customers. It offers an adaptable and versatile administrative environment. This property has made the hybrid cloud as mainstream administration in all businesses. This Work presents another plan of secure information sharing structure utilizing Proper cryptography for active assembly in hybrid cloud environment, which has the following features: Improved development of Ciphertext-Policy Attribute-Based Encryption through assigning ability of mutually encryption/decoding computation from client. Efficient access control through protection safeguarding highlights in cloud, In the client side decrease of calculations.

Keywords*: Enter key words or phrases in alphabetical order, separated by commas*

1. Introduction

Hybrid cloud[1], [2], [3] is normally viewed as zenith for IT framework as shown in Figure 1, obliging the necessities of industry clients by empowering web based sharing, consequently empowering both information and control simultaneously. This environment is adaptable and versatile for a few administrations provided by the cloud. Because of the varied cloud conditions being available, security remains the significant concern during information sharing. Formerly, Hybrid cloud[3] is being usage in all Hybrid enterprises. However, a few security issues[4][5][6] continue to endanger information sharing in the cloud soon. A few activities are made to acknowledge effective information contact and distributing of the information in cloud.

The data owners first encrypt their data until they are stored on cloud servers as a trivial workaround for data exchange in cloud dynamic communities. In order to keep data safe from the cloud providers and malignant users, the data owner will then distribute encryption key to each user in the community. Authenticated user from the group will then retrieve the cloud stored information and decrypt them with the given encryption key. However, user revocation is the key issue with this approach.When the data owner wishes to revoke one of the users in the group, he must re-encrypt the data with a new encryption key and redistribute the new key to all the remaining users in the group. This renders the revoked user's key useless and he or she will thus not be able to access the data contents. This process of re-encrypting the data and redistributing keys to all the remaining users in the group every time a user is revoked access can place a huge burden on the data owner. This is especially the case when the group size is very large, in excess of thousands to hundreds of thousands (eg, everyone in an organization or online community).

Data security is a critical issue in cloud computing. The fact that users no longer physically possess their data makes it very challenging to protect data confidentiality and secure data sharing in Cloud Computing.

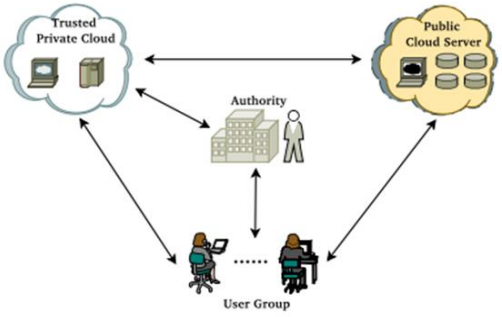

Figure1: Hybrid Cloud Computing Model

[1] *S.Associate Professor,Department of AIML,Gokaraju Rangaraju Institute of Engineering& Technology,Hyderbad,*
ORCID ID : 0000-0003-0438-0867
[2]*Associate Professor,CVR College of Engineering,Hyderabad,Telangana*
ORCID ID : 0000-0003-0106-2134
[3] *Associate Professor,Department of CSE, Narsimha Reddy Engineering College, Hyderabad, Telangana State omputer Eng., Selcuk University, Konya – 42002, TURKEY*
ORCID ID : 0000-0002-0521-8370
[4] *Associate Professor,Department of Computer Science and Engineering Gokaraju Rangaraju Institute of Engineering and Technology,Bachupally, Hyderabad,Telangana*
ORCID ID : 0000-0003-2519-3120
Correponding author mail-id:poornima1704@grietcollege.com

2. LITERATURE SURVEY

2.1. Hybrid cloud protection

A significant problem in distributed storage function is information safety, which principally happens because of the loss of authority over information. Privacy and security are the two principle parts of client's interests about distributed computing innovation. In the recent years, a few enterprises[7][8] are progressively deciding for moving towards cloud environments, in which they shift a portion of outstanding burden to public cloud while still has server form to hold different excellent tasks at hand. With the developing utilization of Public cloud, there is an arising need of security model that shows multiple difficulties, for example, stock market issues and sharing the information in various cloud benefits safely and productively. By and large ordinary procedures like encryption, access control strategies, trust worthiness system are utilized for ensuring information in encryption[9],[10][11], Access Control Mechanisms[12], Verification tools[13] and safe information concentrated registering in cooperation with Public and Private Clouds. Because of the information sharing, there is small attempt to give safety & protection insurances in this novel stock stage. As of late, Attribute-based Cryptography[14].[9],[15],[16].[17] appears as a fit strategy, intended for safe information contribution for dynamic gatherings guaranteeing Proper information organize for which were rethought and which was presented by Sahai & Waters[15],[18].

Data security is a critical issue in cloud computing. The fact that users no longer physically possess their data makes it very challenging to protect data confidentiality and secure data sharing in Cloud Computing.

Attribute Based Encryption[15] seems to be an excellent option. This technique is known to be a public key cryptography with a set of attributes in it. In this method ,Ciphertext-policy attribute-based encryption (CP-ABE),Data owners should specify access controls across attributes and predicates (e.g. and, or) in an encryption method so that users who have attributions which meets the policies can only decrypt data by means of decryption. There are indeed still some practical problems when applying conventional ABE technique in applications over hybrid cloud The problems that are araised when applying this technique are described below:The access policies embedded in the ciphertext is complicated, the computational cost of encryption/decryption is increased linearly with the access formula and requires a lot of exponents or pairings for performing computation

As a result most of the research is focused on privacy and security during data sharing in data security .As well this can be applied to different areas or fields like health,Social Networks,Agriculture etc.Some Common Mistakes

2.2. Troubles on information contribution in the hybrid cloud

Guaranteeing expert information admission and sharing will in general increase different safety worries identified with protection out in the Public cloud. Associations upgrade their customary procedures, such as encryption, confident confirmation, protected information concentrated in both kinds of cloud registration, to protect hybrid cloud information. There is no effort to ensure security and privacy in this new stage due to the encryption of information exchanged. Anyway there additionally restrictions to the utilization of rational ABE plans to crossover cloud applications. To sum up

(1) The main issue is access formula for the cipher text,

(2)Encryption is increased linearly

(3) Huge amount of Pairing calculations will be required .

Motivation:

The decision of Attributed Based Cryptography (ABC) is assured by following reasons.

i. It has easier key management system and there is no need of certificates for authentication.

ii.ABC has the feature i.e. inferring public keys with no requirement for past calculation of corresponding private keys.That is, in spite of conventional generation of public key schemes, in ABC there is no need to produce the private key before the public key. To be sure, clients have just to create access structure and the related encryption key to incrypt the information prior to outsourcing the data for storage.Based on attribute-based group signatures, this research work introduces a privacy preserving authentication scheme.

In this scheme the identity of the client is ensured against the cloud service provider as well as certifying authorities.Also, the integration of attribute based signature scheme and attribute based encryption mechanisms allows the cloud provider to consume the less bandwidth and iot also assures the system's availability.. Moreover, the combination between attribute based encryption mechanisms and attribute based signature scheme allows the cloud provider to control the bandwidth consumption, and then, the system's availability.

The challenges and issues regarding data storing and data sharing in the hybrid cloud will summarize our work and contributions in this way.

(i) In this paper,an algorithm named a Constant Ciphertext-Policy Attribute-Based Encryption has been proposed to achieve confidentiality and privacy by delegating encryption/decryption processes in the private cloud In our proposed technique complex operations required for computations such as exponential at encryption side and bilinear pairings at decryption side are carried out by the private cloud. In this method,the responsibility of the private cloud is to maintain a part of the user decryption key along with the attributes. At the time of revocation,it is the duty of a data owner for defining the new access policy .Once it is defined re-encryption must be done by the private cloud..

(ii) We integrated two most recent methods,named CCP-ABE and ABGS and outsourcing the delegating capabilities for achieving secured data sharing through hybrid cloud which maintains fine grained and privacy access control.

3. The Proposed System in Hybrid Cloud

An epic safe information contribution in Hybrid Cloud for giving protection is discussed here. The proposed system has two latest cryptographic systems, to be specific, CCP-ABE[19] and Attribute based signature[20][19][18][17][16].The choice of property based cryptography (ABC) is provided by numerous elements. This helps will deliver the key administration framework simpler. Besides, ABC permits to get Public Key(PK) ignoring expect of pre-figuring of related Private information. As such, there was no requirement for ABC to create the Private keys before the Public inputs, as on account of customary Public inputs deduction draws near. Clients just require to make the entrance arrangement and the coordinating est ablishment for a security protecting verification scheme, inferred based on execution of gathering scratch dependent on behaviour. The data will be maintained at client is kept divided both from the CA and the cloud Service provider(CSP). Furthermore, the coordination of attribute supported encryption Scheme & Attribute signature method allows the client to control utilization of transfer speed. In real time ,it can be adopted for management of agriculture information and

Health care information..

3.1. System Representation

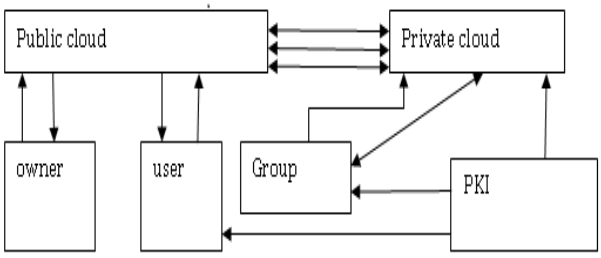

Figure 2. Method Architecture for information Sharing

The Hybrid cloud environment includes numerous Public and Private clouds in which all are organized properly. Every cloud has its individual Security strategy, in order to ensure protection and safety of information. Normal server farm oversee and rearrange every information to be partaken for Private cloud Environment.

There are 2 primary members for this phase: Group Administrator (GA) and Group User (GU).

3.1.1. System Architecture

Five segments were connected in the projected framework representation: Group Administrator (GA), Group User (GU), private cloud , and Public cloud. The framework engineering portrayed in Figure 2 is as a rule broadly utilized and comprises the accompanying clouds, in particular, the general Public and private cloud users Say for instance, an enterprise may secure administrations of information from a Public cloud , comparable with Amazon - S3.

The certificate authority is a crucial expert in this architecture that deals with private (SK and AK) and public parameters production and distribution (PK) keys. A public cloud server provides the data storage service. In the public cloud the user encrypts and saves the file. They specify a policy of access on ther private files and they are encrypted as a policy ciphertext. Group Manager(GM) can give out a few type calculations in the private cloud while as yet guaranteeing the security of access strategy for improving information encryption proficiency Data consumers are entities that have access to files hosted in the public cloud. The customer's private key will decrypt a file if the inserted document is met. A majority of complex pairing operations involved in decryption are conducted in private cloud in order to limit the computational load of decryption for clients.

Initially, an access structure(ψ) is characterized by the GM which divides the individuals who are qualified to get access the information by considering a set of information. Therefore, the encryption of information record is carried under the access structure ψ, based on cipher text-attribute dependent encryption calculation. Which was followed by storing of encrypted information in cloud combined with the group signatures. A client may get the record simply in by getting authenticated . An essential element is obtaining of signature from group Manager, for the access tree ψ. Which was followed by check of correctness to get signature to recover encryption of information file.

The Projected procedure is characterized dependent on resulting 7 calculations. It contains 3systems below 2 distinct stages. In the Essential stage, framework implements setup () methodology. In next stage, when the information proprietors need to impart records to individual clients, which is impacted by Encrypt() a data storage methodology and Access() an data retrival strategy.

Methods includes three randomized calculations for producing public variables which are connected attribute authority group and authenti() for setup, and creates secret inputs for clients dependent on keygen(). The Data_Store() technique characterizes situation for data storage. It involves encryption algorithm. The Decrypt strategy is utilized for recovering verification, for example, sign and confirm calculations and the information decryption algorithms which were indicated as follows:.

Scheme initialization: The confidential association PKI produces universe characteristic groups, & subsequently produces Public input PK and master input MK.

Group (λ, U) → PK, MK. On contribution safety limit λ and a space characteristic deposit U, the team algorithms admits Public bounds PK and master input MK as productivity. The TA initialises by choosing a bilinear plan: e: G0×G0 →G1 with the producer g on leading charge of δ P. following, TA 2 arbitrary α, β ∈Zp are selected. The constraint describing to community are subjected as:

Setup auth():

The group administrator (GA) also phrased that producer is accountable for initializing organization constraints that comprises the following:

- Essential Bilinear records $S=(G_1,G_2,G_T,e,g_1,g_2,p,U)$
- Universal set of characteristics, U=(att1,att2,....attn)
- Distributing the System Parameters sparam=(G_1, G_2, G_T, H,ϒ, gpk, T) in which H symbolizes
- Collision-resistant hash function: $\{0,1\}^* \rightarrow \{0,1\}^l$

& gmsk stand for cluster master secret input worn for tracing, and the numeral of instance phase is symbolized by T.

User Registration:

Each client needs to enlist by means of Group Manager (GM), who finishes validation of behaviour of the client and produces proper private keys. A characteristic is allotted for explaining a client.The owner of information performs the processed listed below to grant the access right

Key Generation & distribution:

Generating & circulation of inputs is the duty of Group Administrator by implementing the key production. At the point when a client joins the framework for first time, an ID is consigned by the administrator. Alongside Private input is additionally created, which incorporates SK and AKi for comparing client Join procedures, wherein, client remain SK classified. Alongside H(ID) in Enrolment record the private cloud likewise provisions AK, which hoard system transmission capacity. The calculation for input age acquires a group of info credits S chose for client is saved as contribution for age of input and private input parts used for comparing each and every characteristic for S, is specified as yield. The input production procedure is specified below:

1. choose one arbitrary r∈Zp,

2 choose one arbitrary rj ∈Zp for every element j∈S.

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

4. Broadcast SK to client by means of a protected path.

5. Choose $x_i \in \mathbb{Z}_p^*$ & $y'' \in_R \mathbb{Z}_p^*$ and assess A_i, X_i, W

$$A_i = (h\, Y_i'\, Y_i'')^{1/(a+x_i)}, \quad X_i = X_{i,2} = g_2^{x_i}, W = T_{i,j} = h^{sj/\gamma + x_i}$$

6. The confidential input ,$AK_i=((A_i,X_i,y_i),\{W\}_{attj} \in A_i)$ was produced appropriately.

$$PK = \langle G0, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha} \rangle.$$

Wherer the master key is MK = ((β, g α), which is only known by the TA.

In which (A_i,X_i,y_i) = Membership certificate

$\{W\}_{attj \in Ai}$ = Quality certificate.

Cloud Storage Providers:

Algorithm Encrypt(s_1, τ_{ESP})

Start

1. $\forall v \in \tau_{ESP}$, randomly choose one polynomial q_v contains grade $d_v = k_v - 1$, wherein, k_v is the secret sharing threshold cost:

i) $Root_{ESP}$ is the origin knob of τ_{ESP}, , $d_{RootESP}$ degree polynomial by $q_{RootESP}(0) = s1$.

ii) $\forall v \in \tau_{ESP} \backslash Root_{ESP}$ decides d-degree polynomial with $q_v(0) = q_{parent}(v)$ (key(v)).

2. Produce a sequential ciphertext: $CT'\tau_{ESP} = \{\forall y' \in L_{ESP} : C_y = g^{qy(0)}, C'_y = H(att(y))^{qy(0)}\}$, in which L_{ESP} symbolize the collection of leaf nodes in τ_{ESP}.

Stop

In a Public cloud, the information is encoded by proprietor preceding individual shipped off CSP. Calculation substantial invariable CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTIONactivities are farm out to confidential cloud accordingly concealing their mystery inputs alongside the substance of information. Secret key is covered up inside the encrypted text according to access policy tree upon encryption. The Admission strategy (ψ) is characterized by Boolean equation & described by an access tree.

(i) File Generation:

Until the latest documents are transferred to the Public Cloud, the Encryption and Last Encryption State is shown as blocks before new records are submitted to the Public Cloud. The DO therefore calls upon the TESP entry strategy of the confidential cloud to be applied on transmitted information. The Data Store() technique combines 2 encryption strategies: EPri() encryption and EncryptDO() encryption. Scramble () is applied in the confidential cloud by an Encryption expert co-op and EncryptDO () has the following subtleties:

- **ENCRYPTION ():** • Encrypt ESPri(s1, TESP)) – It was encryption calculation, Encrypt ESPri (), which was executed in the confidential cloud by the Encryption standard.

Initially, client determines strategy hierarchy $\tau = \tau ESP \wedge \tau DO$, in which ∧ is called AND validation administrator and τESP & τDO were secondary elements which are connected by 'AND' administrator. τESP means the information admission strategy executed by ESP in private cloud & τDO speaks to client's information permission strategy. τDO for the most part comprises of not many attributes in order to reduce the build transparency in client part. Encrypt(s1, τESP) calculation, is shown below.

At long last, ultimately, the private cloud sends CT to the distributed storage supplier to be put away.

(ii) File Access Process:

The support system to get to a record is convene by client. The method was started by validation process, which comprises of signature () and auth() calculations and satisfied by decryption.

- **User Authentication**: For getting to a shared document (ED) put away inside CSP, the client (U) should be verified r, as for the entrance tree ψ related with the confidential information record along with the signature(σ). The CSP demands the gathering chief.

At first, the anonymity key(Ski)is done by client track by calculation of signature(σ)) on the significance which has credits identification, User, ID information, agreed instance and ID information which can be recovered from nearby shared document listing kept up by administrator to the cloud.

The solicitation is trailed by implementation of signature Procedure by the concern authorities to approve the mark and crossing out check with concerned procedure if need emerges. If there should arise an occurrence of productive confirmation, the worker reacts with the mentioned information document.

Approving record and decoding utilizing Decrypt () methodology. Endless supply of the confirmation strategy, the entrance is denied and the information isn't sent.

The validation cycle is made out of two calculations, enrolled as follows:

- **Signature ()–** Algorithm allowing for boundaries similar to gpk, t, ski, a characteristic position, $\zeta \subseteq$ Ai significance M, and the predicate contribution Y and proceeds σ a GS at an occasion stretch t on M.

Gathering individuals, considers private inputs ski. uses the Signature calculation in making a gathering mark for record M by the predicate (Y); if legitimate quality locate Ai is said by them which satisfies, the mark σ is shipped off the cloud specialist organization who affirms concerned mark.

- **Verify()** – It approves the gathering mark (σ) beside gpk and provides any 0 or 1. In the event that 1 is returned, at that point the calculation produces a right GS(σ), or , is invalid. Accordingly, the CSP computes all the matching condition holds according to Groth Sahai confirmation for checking the mark.

(iii) File Decryption ():

On the off chance that a client needs for getting to the record put away in the Public cloud, a recovery demand with unknown input SK' and mark must be coordinated to cloud. Public cloud affirms that mark and transmits the scrambled record as reaction to Private cloud. The private cloud achieves relating CT', sightless key SK' and run the Decrypt (SK', CT ') calculation

This change calculation gets the contribution as cipher text CT' and "property declaration" AK & yields CT or void (⊥). To protect information, the private input (SK') by picking an arbitrary t as of Zp is sightless by client & $\tilde{D} = D\ t = g\ t(\alpha+r)/\beta$ was determined.

The confidential input (blind) is spoken to as

Prior to summoning Public cloud, customer verifies whether its credits possessed by him resolves ful-fill admission strategy T, prior to continuing to conjure the Public cloud. Provided that this is true, client sends $\{(SK)\tilde{}\}$ to the Public cloud, & transmits demands for cipher text to private cloud. On getting solicitation, the Public cloud transmits:

Furthermore, $CT' \subset CT$ to confidential cloud .When the private cloud gets both The private cloud executes the Decrypt $((SK)\tilde{}, CT')$ calculation following both $\{(SK)\tilde{}\}$ and CT′ are gotten.

The accompanying techniques started: everywhere R was base of T.

Subsequent to acquiring cipher text CT starting private cloud, the plaintext m will be decoded by performing Decrypt (CT, SK)

calculation with SK, for which simply a solitary blending activity does the trick. This plan helps decoding at generally higher paces, guaranteeing information security in the client side.

(iv) User Revocation: Revocation is a attribute based crypto framework plans is a significant issue for both property repudiation and client denial. Followed by repudiation, the concerned mystery keys should be refreshed with significant attributes. In any case, giving novel keys oftentimes was dull. The projected method refreshes private cloud's information encryption input. Client will not be consistently in contact for refreshing ambiguity keys. Also, private cloud gets & supplies the updates of the client since confided in power. Upon the repudiation of personality, just persuaded field information were scrambled. The ESP must again be scrambled & information will be transferred on Public cloud in the wake of finishing refreshes, another irregular DEK is encoded by DO and identified with most recent CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION's access strategy in the wake of picking another information access tree which is equipped for denying all earlier recorded information. Furthermore, the DO likewise appends another direct block from document's side. For repudiating particular client for important data, for example, ID,Signature(σ) and so on was sent from the TA to confidential cloud. This is trailed by erasure of relating passage in the prior enrollment catalogue. Hence, the private cloud ends the reaction inception to solicitations of renounced customer. To provide information unavailable to disavowed client, another entrance strategy is picked and the square of the document is exposed to re encryption utilizing indifferent re-encryption. The encoded document CT2 is shipped off the private cloud. The re-encryption forces more modest calculation overhead over the information proprietor. When CT2 is acquired, the legitimacy of the DO as for H(ID) is researched. If there should arise an occurrence of positive outcome, the private cloud runs calculation Encrypt PriCloud() to produce another ciphertext CT which substitutes the previous one in the public cloud, in any case , the refreshed admittance strategy is dismissed.

4. Performance Analysis

The public cloud is operated by the cloud service provider. Despite their versatile storage and computer capability, they remain reliable to clients. The private cloud remains "fair yet inquisitive" which shows that, irrespective of whether the conventions are strictly adhered to, the data acquisition process shows an inherent interest. They are interested in access strategy and information material. The primary aim is to ensure the safety and protection of public and private cloud information. Data proprietors rearrange uncompromising estimation undertakings to private cloud without uncovering information which guarantees information privacy.

4.1. Security Analysis:

The projected effort includes encoding and putting away documents in the cloud by utilizing the consistent Cipher text Attribute Based Encryption(CP-ABE) conspire for guaranteeing capability in classification and access control of information. Hypohesis 1. Our projected plot ensures information classification. Confirmation. The plan introduced in this work intends to ensure privacy of the information from threatening clients and cloud suppliers.

The Data Owner makes an entrance structure concerning the clients arrangement of characteristics to decide whom to allow admittance to the information capacity. The public cloud supplier sends the mentioned information to clients after cross-checking the mark. Consequently, just a client with substantial access structure can create an encryption key. Also, if there should be an occurrence of an inquisitive cloud specialist co-op who endeavours to skive off the scrambled information, the specific individual or gathering would come up short as the rethought information can't be gotten to.

On the premise that the mark conspires in its utilization, the proposed package protects the client from sneaking around a specialist cooperative. The validation authority is dependent on the client in the proposed scheme. As characterized by the data holder the client (U) sign, the message regarding the entrance structure has been received by the cloud organization. The CSP confirms the client's entry rights with no prior personality information or characteristics of the message mark. Not withstanding ABGS properties, our framework properly maintains non-recognisability and secures the characters of the clients along these lines. Truth be told that the ABE conspiracy does not reveal the character of the encryption or assign the clients in the strengthening phase.

The scrambled documents can only be validated and decoded by approved customers. Cloud users need their guaranteed AAs credits and relate mystery keys. As a result, only people with legitimate private keys could get the information in the cloud and confirm it successfully with the cloud worker. This is accurately credited to the encryption & marking calculation of the elements of the ABGS mark.

4.2. Computational Complexity

This section discusses about difficulties experienced in computing registering & storing information membership casing effort at cloud provider and consumer at last part of the range. Considering assessment, The STORE technique was implemented. The expense experienced was executed by mutually client (U) and cloud workers for BACKUP strategy.

Computational Complexity investigation:

The computational Complexity included key strides of the projected framework and has been organized as per the below Table 1.

The quantity of characteristics in S is signified by |S | during system setup phase, Calculation of computational complexity during the data store process and storage overhead at both public and private clouds indicated by p and characteristics in I is indicated by |I|,

1) System Setup: Upon Initialization, a bilinear group & random numbers are considered, subsequently resulting in computational complexity of O (1). At the point where PK & MK were orchestrated, a few exponentiation and mutual calculations would emerge for encryption and unscrambling.

2) Data _Store Process():

The STORE method includes scrambling in user side and furthermore in encryption calculation of the Private cloud. **Encryption(DO):** The information owner characterize an entrance strategy utilizing AND entryway to perform encryption. Just the additional false trait calculation should be completed. The information proprietor ought to encode the information document during this method; accordingly; counts of 3 exponentiations in G0 to figure every one of C1 alongside one blending capacity e(g0,g1) where the number of attributes is represented by n. Additionally, proprietor for information complete, duplication activity for G1, exponentiations in G1and one more mess to G0 elements. So the calculation unpredictability ends up being Order of 1 and it is consistent.

Encryption: For this progression, a solitary access policy E (G0,G1) and exponentiations in G0 to process c1 exclusively, in which A1 is quantity of highlights TESP. Information proprietor

Procedure	Complexity
System Setup	O(1)
Data_Store ()	O(1)
Key Generation	O(l × n)
Back UP()	O(|S|)

Table1: Computational Complexities

for confidential cloud execute 0 exponentiations in G1,0 increase activity more than G1 function & mess to G0 tasks. The expense for calculation ascends in relation to trees. Consequently for confidential cloud the calculation intricacy is O(l × n). This prompts the end for proposed conspire essentially limits client side additional room needed by appointing a larger part of exorbitant methodology to confidential cloud.

Key Generation: Computational Assistance identifying with the input involves every characteristic in the AK age, & 1 for shared secret input in SK age which brings about an complexity of O(|S| + O(1)), in which quantity of the attributes connected to user is represented by S.

Back up(): BACKUP method exemplifies 3 calculations to confirm the calculations executed by community cloud and signature function and Decryption functions run by information client (U). This client initially validates an irregular communication with cloud employee. This client does 2(n+1) exponentiations on G1, as per the duration of the mark. At that point, last directs 2n matching to register thru decryption of information. At some point in confirmation, the CSP performs checking for the calculations which performs n+1 exponentiation in G1 and figuring's on (n+2) matching capacities for Equivalent components.

Cipher text:. This calculation burden varies according to the entrance structure and clients' credits. The confidential cloud requires a1 pairings, 2a1 exponentiations in G1,a1 duplication activity more than G1 , 2a1+1 reversal tasks .

Decryption: Here the Actual text m acquired by client gets implemented by conclusive decryption which requires no pairings by any means, 1exponentiations in G1,1 duplication activity upon G1 and 1 reversal activity.

5. Conclusion

Any data sharing scheme in Hybrid cloud seeks to spread information that has been re-evaluated safely and effectively through dynamic communities. A hybrid cloud architecture is designed to achieve this. Early information revaluation strategies across the Public Cloud posed serious problems and failed to resolve access approaches and privacy found by cloud information collection. A strategy for efficient information sharing is maintained using attribute-based encryption with the expected approach in cloud computing. In CP-ABE, while saving protection and data classification and at the same time allocating encryption to private cloud, decryption is the most complicated operation yet decreases computational costs and decreases the overhead on the customer side. But there is a limitation of our work .Our solution works efficiently ,when the size of the group is large. Data sharing is an important challenge in big data. In the future our work can be extended by testing and analyzing in a distributed technologies and the scheme related to HDFS can be extended for dynamic groups in big data. . As a final mark ,a robust cryptographic mechanism is to be build ,which combines both encryption and signature generation phases that uses single key generation algorithm to reduce computation overhead and storage cost such as key storage cost and key certificate cost.

References

[1] S. U. Khan and N. Ullah, "Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review," *J. Eng.*, vol. 2016, no. 5, pp. 107–118, 2016, doi: 10.1049/joe.2016.0089.

[2] K. Bakshi, "Secure hybrid cloud computing: Approaches and use cases," *IEEE Aerosp. Conf. Proc.*, pp. 1–8, 2014, doi: 10.1109/AERO.2014.6836198.

[3] A. Gordon, "The Hybrid Cloud Security Professional," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 82–86, 2016, doi: 10.1109/MCC.2016.21.

[4] J. K. Wang and X. Jia, "Data security and authentication in hybrid cloud computing model," 2012. doi: 10.1109/GHTCE.2012.6490136.

[5] M. Raza, A. Imtiaz, and U. Shoaib, "A review on security issues and their impact on hybrid cloud computing environment," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 353–357, 2019, doi: 10.14569/IJACSA.2019.0100346.

[6] N. M. Reddy, G. Ramesh, S. B. Kasturi, D. Sharmila, G. Gopichand, and L. T. Robinson, "Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in cloud," *Appl. Nanosci.*, 2022, doi: 10.1007/s13204-021-02174-y.

[7] G. Aryotejo, D. Y. Kristiyanto, and Mufadhol, "Hybrid cloud: Bridging of private and public cloud computing," *J. Phys. Conf. Ser.*, vol. 1025, no. 1, pp. 0–7, 2018, doi: 10.1088/1742-6596/1025/1/012091.

[8] N. Thirupathi, K. Madhavi, G. Ramesh, and K. Sowmya Priya, "Data Storage in Cloud Using Key-Policy Attribute-Based Temporary Keyword Search Scheme (KP-ABTKS)," in *Lecture Notes in Networks and Systems*, vol. 98, 2020. doi: 10.1007/978-3-030-33846-6_67.

[9] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," *J. Comput. Secur.*, vol. 18, no. 5, pp. 799–837, 2010, doi: 10.3233/JCS-2009-0383.

[10] A. Balu and K. Kuppusamy, "An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption," *Inf. Sci. (Ny).*, vol. 276, no. subaward 641, pp. 354–362, 2014, doi: 10.1016/j.ins.2013.12.027.

[11] P. Dileep Kumar Reddy, R. Praveen Sam, and C. Shoba Bindu, "Optimal blowfish algorithm-based technique for data security in cloud," *Int. J. Bus. Intell. Data Min.*, vol. 11, no. 2, pp. 171–189, 2016, doi: 10.1504/IJBIDM.2016.081605.

[12] and M. Z. Yingjie Xia, Li Kuang, "A hierarchical access control scheme in cloud using hhecc," *J. Phys. A Math. Theor.*, vol. 44, no. 8, pp. 1689–1699, 2011, doi: 10.1088/1751-8113/44/8/085201.

[13] Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, "Collaborative Integrity Verification in Hybrid Clouds," no. May 2014, 2012, doi: 10.4108/icst.collaboratecom.2011.247089.

[14] S. Belguith, N. Kaaniche, A. Jemai, M. Laurent, and R. Attia, "PAbAC: A privacy preserving attribute based framework for fine grained access control in clouds," *ICETE 2016 - Proc. 13th Int. Jt. Conf. E-bus. Telecommun.*, vol. 4, pp. 133–146, 2016, doi: 10.5220/0005968201330146.

[15] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6571 LNCS, no. subaward 641, pp. 53–70, 2011, doi: 10.1007/978-3-642-19379-8_4.

[16] N. Eltayieb, P. Wang, A. Hassan, R. Elhabob, and F. Li, "ASDS: Attribute-based secure data sharing scheme for reliable cloud environment," *Secur. Priv.*, vol. 2, no. 2, p. e57, Mar. 2019, doi: 10.1002/spy2.57.

[17] X. Lu, Z. Pan, and H. Xian, "An efficient and secure data sharing scheme for mobile devices in cloud computing," *J. Cloud Comput.*, vol. 9, no. 1, 2020, doi: 10.1186/s13677-020-00207-5.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *Proc. - IEEE Symp. Secur. Priv.*, pp. 321–334, 2007, doi: 10.1109/SP.2007.11.

[19] Z. Zhou, D. Huang, S. Member, and Z. Wang, "Ef fi cient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 126–138, 2015.

[20] S. T. Ali and B. B. Amberker, "A dynamic constant size attribute-based group signature scheme with attribute anonymity," *Int. J. Inf. Privacy, Secur. Integr.*, vol. 1, no. 4, p. 312, 2013, doi: 10.1504/ijipsi.2013.058207.