Privacy Preserving and Consistency Check Of Data Store in Cloud Using Attribute Based Encryption

P.Santhi[1], R.Vaneeshwari[2]
[1]Associate Professor, [2]PG scholar
Department of Computer Science and Engineering,
M.Kumarasamy College of Engineering, Karur,India

Abstract **- Cloud computing is a promising knowledge which provider an assortment of opportunities for online distribution of resources or services. The most effective benefit of using cloud computing is higher availability of services with less cost and simple scalability. Cloud provides different type of services and storage security but some challenges are still present in it. Out of which privacy concern, synchronization, scalability, load balancing and replication are important issues. Data replication means maintaining multiple copies of same data on same server or on different servers. In connection with cloud computing data replication can be said as storing multiple copies of same data on different location (servers), locally or at remote sites. If data is present at one site only, then it will be very difficult to touch the requests for access the data. Server will face a heavy load situation and system performance may degrade. So in this project implements secure in ABE approach to fragment data sets which are uploaded by data owner and execute chart based draw near to calculate the distance using T-Coloring method to predict the data nodes for placing split data. This proposed approach is very useful to data owner for shielding data from attackers. Then we extend our approach for checking reliability in cloud system at the time file updating. And propose an Attribute Based Encryption (ABE) which adds appropriate reads to reveal as many violations as possible. It can be done by using user operation table. Every user maintains a UOT for cassette local operations. Each evidence in the UOT is described by three elements: operation, logical vector, and physical vector. Experimental results provide improved security and summary retrieval time for access data from cloud system and implement in real time cloud environments.**

Keywords **- Cloud Data, T-coloring method, Node placement, User Operation, Auditing strategy.**

I. INTRODUCTION

Cloud computing is an emerging technology which provider a lot of opportunities for online sharing of resources or services. Cloud Computing is an internet oriented a computing. It dynamically delivers everything as a service over the internet base and on user demand, such as association, OS, storage devices, hardware, software and assets. Cloud Storage system, is a also known as Data storage as a service, is the abstract of storage last an interface where resources can be administered on demand. Cloud data resources works on sharing file systems because of its ability to handle an infinite volume of data effectively. Storage can be home or isolated. Cloud computing is cost effective, secure and scalable but managing the load of random job available is a difficult work. Data availability means data is accessible when never it is requested. Accessibility of data increases with increment in number of duplication of data. But after reaching a specific level of duplication, there occurs no development in availability. So it is better to find an optimum level of duplication. Availability and duplication ratio also depends on node failure ratio. If failure probability is high, more number of duplication of that data is essential. So if node crash ratio is less, less duplication number is required for maximum file availability.

II. LITERATURE SURVEY

Waters present three structure within our framework. Ours system is confirmed selectively secure under a assumption that we name the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which will be able to be viewed as a sweeping statement of the BDHE assumption. Our next two structures provide concert tradeoffs to achieve verifiable security in that order under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions [3].

Hohenberger at hand the first key-policy ABE system where cipher texts can be decoded with a constant digit of pairings. We show that GPSW cipher texts can be decoded with only 2 pairings by rising the secret key size by a factor of |T|, where T is the set of different attributes that appear in the private key. Then present a general creation that allows each system user to in competition tune various efficiency tradeoffs to their liking on a field where the limits are GPSW on one end and our very fast scheme on the other. This tuning requires no changes to the public parameter or the encryption algorithm. Strategies for choose an individualized user optimization plan are discuss. Finally, we discuss how these ideas can be translate into the cipher text-policy ABE setting at a higher cost[6].

Tysowsk Novel modifications to attribute based encryption are outlook to allow authorized users access to cloud data based on the approval of required attributes such that the superior computational load from cryptoclastic operation is assign to the cloud supplier and the total statement cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally perform by the CSP to reduce the cost of consumer revocation in a movable user setting while preserving the privacy of user data store in the cloud. The proposed protocol has been realized on commercially accepted mobile and cloud platforms to reveal real-

world benchmarks which show the efficacy of the scheme. A replication calibrated with the normal results proves the scalability possible of the scheme in the background of a classic workload in a cloud computing system [5].

Lewko use a novel information-theoretic argument to adapt the dual system encryption method to the more complicated structure of ABE systems. The construct our system in complex orders bilinear groups, where the order is a item for consumption of three primes. We prove the privacy of our system from three static assumptions. Our ABE scheme supports random monotone right to use formulas. Our next result is a fully secure predicate encryption (PE) scheme for inner formation predicates. As for ABE, previous construction of such scheme was only confirmed to be selectively secure. Security is proven under a non-interactive statement whose size does not depend on the digit of query. The scheme is comparably able to existing selectively safe schemes. Also there a fully secure hierarchical PE method below the same statement. The key technique used to get these results is an complex grouping of the dual system encryption methodology and a new move in the direction of on bilinear pairings using the idea of dual pairing vector spaces (DPVS) implement [7].

Kappes develop a new cryptosystem for fine-grained sharing of encrypted data so as to we call Key-Policy ABE. In which cryptosystem, cipher texts are label with sets of attributes and secret keys are connected with right to use structures that manage which cipher texts a user is capable to decrypt. We present the applicability of our creation to giving out of audit-log information and broadcast encryption. Our construction supports designation of secret keys which contains Hierarchical Identity-Based Encryption (HIBE) [1].

III. PROPOSED SYSTEM ARCHITECTURE

Cloud computing service provider requires a system which can hold a large number of needs at a time. For processing the huge cloud of requests for data access permission, services need to be very available. System keeps many copies of the blocks of data on different nodes by duplicate. A large number of replication plans for organization of replicas have been implemented in usual system. As a result of replication, data replications are stored on different data nodes for high consistency and ease of use. Replication factor for each data block and duplication placement sites call for to be determined at initially. In existing support data can be lost so in this paper propose improved secure perform in ABE to protect the data from loss. It present efficient constancy as a service model, where a group of data owners that compose service provider can verify whether the data cloud update the data or not and design user function table to change status of split files with different metrics and proposed in fig 1.

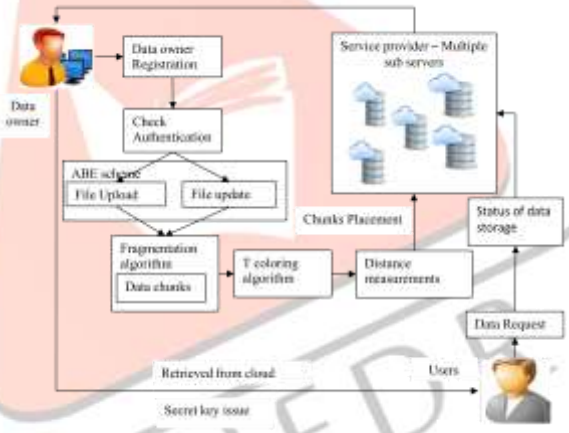

Figure 1. Improved Framework

IV. PROPOSED METHODOLOGIES

ABE Techniques:

Setup ()

The setup algorithm take as input a privacy parameter λ and a small universe description U= {1, 2, 3…, ℓ}. It first runs G (λ) to obtain (p,G,G_T ,e), where G and and G_T are cyclic groups of prime order . It then chooses g, u, v, d ∑ G, and α, sa ∑ Z_p^* uniformly at random,for each attribute i ∑ U. It chooses a random value Si ∑ Z* p and a collision-resistant hash function H:G⟶ Z_p^*,the public parameters PK = (G, G_T ,e,g,u,v,d,g^a , e(g, g)$^\alpha$,$T_i = g^{si}$ ∀ i ,H). It outputs a master public key and master secret key MSK= α.

KeyGen ()

The key generation algorithm at randomly picks t ∑ Z* p

$K = g^\alpha g^{at}$

$K_o = g^t$

$K_i = T_i^t \ \forall\ i \in s$

It yields a transformation key and decryption key.

Encrypt ()

The encrypt algorithm use the public parameters, communication and access structure. Access structure consists of attributes and their drawing.

$C = u^{H(M)} v^{H(M)} d$

$C_1 = M.\, e(g.g)^{\alpha s}$

$C_1' = g^s$

$C_{1,i} = g^{a,A_i,v} T^{-r1,i} \rho(i)$

$D_{1,i} = g^{r1,i} \forall i \in \{1,2,\dots,1\}$
$C_2 = M.e(g.g)^{\alpha s}$
$C_2' = g^s$
$C_{2,i} = g^{a,A_i,v}T^{-r2,i}\rho(i)$
$D_{2,i} = g^{r2,i} \forall i \in \{1,2,\dots,1\}$
It output a ciphertexts CT as,Encrypted data CT= $((A, \rho), \hat{c}, C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i})$

Transform ()

This algorithm will generate the altered cipher text. This algorithm takes as input the public constraints PK, cipher text CT, and the transformation key TKs to generate the transformed cipher text CT'. It send the transformed cipher text to the user.

$$T_1' = [e(c_1', \frac{K'}{[(\prod_{i\in I}(e(C_{1,i}, K_0').e(K'_{\rho(i)}, D_{1,i}))^{\omega i})}]$$
$$= [e(g,g)^{\alpha s/z} e(g,g)^{ats/z} / [\prod_{i\in I}(e(g,g)^{atAi.v\omega i/z}$$
$$= e(g,g)^{\alpha s/z}$$
$$T_2' = [e(c_2', \frac{K'}{[(\prod_{i\in I}(e(C_{2,i}, K_0').e(K'_{\rho(i)}, D_{2,i}))^{\omega i})}]$$
$$= [e(g,g)^{\alpha s'/z} e(g,g)^{ats'/z} / [\prod_{i\in I}(e(g,g)^{atAi.v'\omega i/z}$$
$$= e(g,g)^{\alpha s'/z}$$

Decrypt ()

Decrypt algorithm uses the public parameters, transformed cipher text, and decryption key.

$PK = (G, G_T, e, g, u, v, d, g^a, e(g,g)^{\alpha}, T_i = g^{si} = g \forall i, H)$
$CT = ((A, \rho), \hat{c}, \hat{c}, C_1, C_1', C_{1,i}, D_{1,i}, C_2, C_2', C_{2,i}, D_{2,i}, i)$
$CT' = (T=C, T_1 = C_1, T_1', T_2' = C_2, T_2')$. RKs = z

T-coloring Technique:

The most famous chart coloring problem is certainly the chart coloring problem. The chart coloring is a unique case of chart labeling; it is an assignment of labels traditionally called colors to elements of a chart subject to convinced constriction. The frequency assignment problems are formed as optimization troubles having the next form: Given a collection of nodes to be allocated with proper values that convinces various constraints and that minimizes the accessing time. The frequency constrained approach should be avoided if distance partition is employed to mitigate interference. A proper coloring of a chart is an assignment of colors to the vertices of the chart so that no two closest vertices have the same color, this is called vertex coloring. An edge coloring assigns a color to every edge thus no two closest edges share the same color. The face coloring is a chart assigns a color to each face or region so that no two faces that share a frontier have the similar color. A coloring using almost k colors is called a proper k-coloring. The total coloring is a type of coloring on the vertices and edges of a chart.

In this proposed system, T-coloring technique is used. T-coloring will provide complete value of the difference between two colors of closest vertices must not belong to fixed set *T*. Given a chart, *G = (V,E)* and a set *T* of a non-negative integers containing 0, a T-coloring of *G* is an integer job *f* of the vertices of *G* such that $|f(u) - f(v)| \notin T$ whenever *(u ,v)* $\in E$. The mapping function *f* assigns a color to a vertex. The T-coloring problem for channel assignment allocates channels to the joins, such that the channel is estranged by a distance to avoid intrusion.

Let *T* be a T-coloring problem for a chart *G*. There are three important criteria for measuring the efficiency of *f*:

- The order of a T-coloring which is the number of unlike colors used in *f*.
- The span of f, which is the greatest of $|f(u) - f(v)|$ over all vertices *u* and *v*.
- The edge span of *f*, which is the greatest of $|f(u) - f(v)|$ overall edges *uv*.

V. EXPERIMENTAL RESULTS

The figure 2,3 and 4 shows the results of proposed system as follows,
(i)File status shows the distance position of the uploaded file.
(ii)File store reports where the file is located.
(iii)User download displays how the user downloads files by using the provided secret keys.

File status

Figure 2. File status

File store

Figure 3. File store

User download

Figure 4. User download

VI. PERFORMANCE ANALYSIS

The system performance can be evaluated using following parameters:
(i) Increasing the number of nodes in the scheme,
(ii) Increasing the number of objects keeping number of nodes constant,
(iii) Changing the nodes storage ability, and
(iv) Unreliable the read/write ratio. These abilities are consolidated as capacity of replication node and time of updating. And it can be plotted as chart in fig 5.

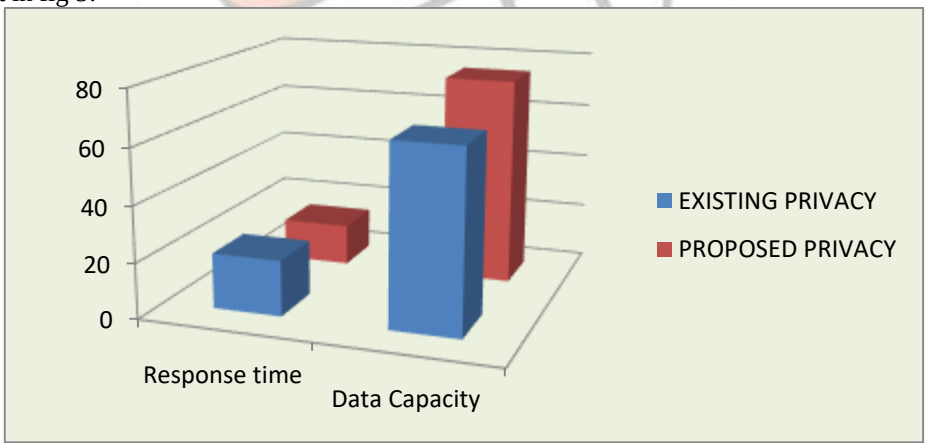

Figure 5. Experimental Results

VII. CONCLUSION & FUTURE WORK

In this paper proposed the current enabling data reliability proof and reliability services over multi cloud system using ABE which helps in informative violation as much as possible. The cloud reliability model and local auditing, global auditing that helps user to confirm the cloud service provider (CSP) provide the promised constancy or not and count the severity of the violations. Therefore system monitor consistency service model as well as level of data uploads which helps the user to get the data in updated version. User can recognize various sub servers in CSP. It is a considered to provide regular update mechanism to confirm fragments simply and provide the data to users after updating only.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptocharty, 2011, pp. 53–70.
[4] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.
[5] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.
[6] S. Rosenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptocharty, 2013, pp. 162–179.
[7] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91.
[8] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R`afols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.
[9] M. D¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626
[10] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in WPES, 2010, pp. 31–42.

Author's Biography:

r.P.Santhi is an associate professor in the Department of Computer Science & Engineering at M.Kumarasamy ollege of Engineering. She received her Ph.D., in Anna University, Chennai. She has more than 10 years of aching experience & she published more than 10 national and international journals. She received the project nds from TNSCST. Her area of interest is Image Processing, Data Mining and Theory of Computation.

R.Vaneeshwari received the B.E degree in Computer Science and Engineering from Anna University, Chennai. She is now doing M.E -Computer Science and Engineering in M.Kumarasamy College of Engineering, Karur. Her area of interest is to Cloud Computing, Operating System