An Efficient Auditing for Data Sharing over Public Clouds using Signature based Elliptic Curve

Meenu Tahilyani[#1], Dr. Amit Dutta [*2]
[#] Department of Computer Science, Sant Hirdaram Girls College, Bhopal, India
[1] meenutahilyani05@gmail.com
[*] Deputy Director, AICTE, New Delhi, India
[2] amitdutta07@gmail.com

***Abstract*— Cloud computing enables allocation of Data and resources over internet. During allocation of information over cloud storage, security is of significant concern; hence, various security algorithms are implemented to provide security from various attacks. Here in this broadside an efficient Data Sharing using Hard Logarithmic based Signcryption and Unsigncryption is implemented which provides security from various attacks and also provides low computational cost and time.**

Keyword- Cloud Computing, Signcryption, Unsigncryption, Signatures, Hard Logarithmic Problem, Elliptic Curves.

I. INTRODUCTION

Cloud Computing deliberated as the prospects of IT design and still undertakes to give unrestricted and expandable storage resource and other computing resources as a consideration to cloud users in a very commercial approach [1] and as an amenity to cloud clients. Now a day's cloud computing is a developed technology to store information from more than one client. Cloud computing is a situation that permits clients to store the information. Cloud computing is a situation that allows users to distantly store their data. Distant backup system is the difficult idea, which decreases the charge for applying more memory in an association. It facilitates activities and government agencies decrease their financial transparency of data management. They can store their data backups distantly to third party cloud storage providers before endure data centres on their individual. An individual or an organization may not need purchasing the required storage devices. As an alternative they can store their data backups to the cloud and documentation of their information to stay away from any data loss in case of hardware / software failures.

Much of the information stored in clouds is extremely at risk such as, medicinal annals and social records over shared networks. Even cloud storage is more elastic how the safety measures and confidentiality are accessible for the outsourced information becomes a serious apprehension. As they offer, the client should confirm itself before commencing any contract and alternatively, it must be guaranteed that the cloud does not alter the information that is outsourced. User privacy is also needed so that the cloud or other clients do not know the distinctiveness of the client. To right of entrance, a protected data transaction in the cloud, the appropriate cryptographic technique is utilized. The data owner must encode the file and then store the file in the cloud. If a third party downloads the file, clients may scrutiny the record if the customer had the key which is utilized to decode the encoded file. Occasionally, this may be a not a success due to the technology expansion and the hackers. The cloud can grasp the client responsible for the information it outsources and equally, the cloud is itself accountable for the services it makes available. The validity of the client who stores the information is also confirmed. With the purpose of guarantee privacy of susceptible information stored in public clouds, a commonly approved approach is to encode the statistics before uploading it to the cloud. Since the cloud does not know the keys utilized to encode the data, the privacy of the information from the cloud is promised. A representative approach used to support fine-grained encryption based right to use organize is to encrypt different sets of data items to which the same access control policy be appropriating with dissimilar symmetric solutions and give customers also the relevant keys [2] or the capability to develop the keys [3], [4].

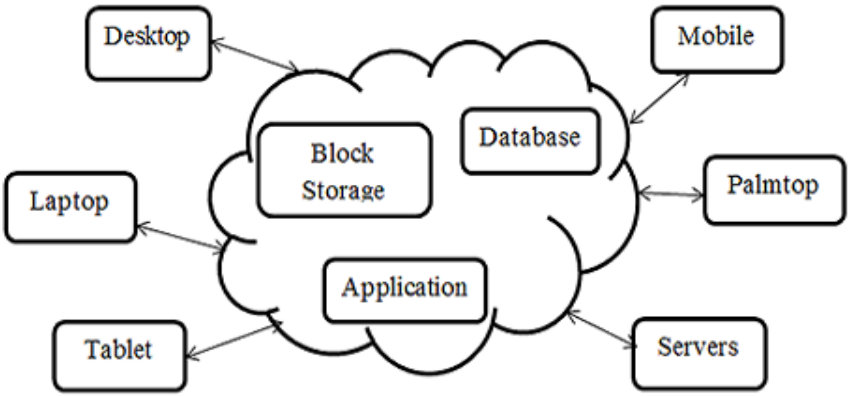

Figure-1: Cloud Data Storage

For avoiding, the cloud from concerning in place and entrusting all the effort of the client is a usual approach to keep away from data leakage. On the other indicator, the restricted computational control on the client side and the high computational operating cost prevents data security. The trouble of safe multi-keyword top-k repossession over encoded cloud information accordingly is: How to make the cloud does more work for the duration of the development of recovery without data leakage. As consider a cloud computing system hosting data service, as demonstrated in Figure 2, in which three diverse entities are concerned: cloud server, data owner, and data user. The cloud attendant hosts third-party data storage and retrieve services. Since information may comprise approachable data, the cloud servers cannot be completely entrusted in protecting information [6]. For this motivation, outsourced records must be encoded. Any kind of data leakage that would influence data privacy is considered as undesirable.

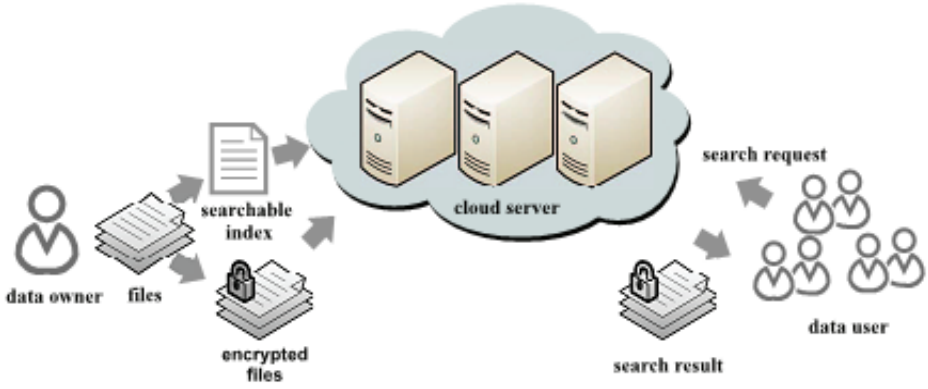

Figure-2: Situation of repossession of encoded cloud information [6].

In Cloud Computing, cloud users and cloud storage providers are approximately certain to be from different trust domains. It tries out that on individual hand susceptible data should be encrypted before uploading to cloud servers; however, a protected client put into effect, data access control technique must be presented before cloud users have the freedom to outsource susceptible information to the cloud for storage. Comparable to any untrusted storage case, here they can determine the problem using a cryptographic-based data access control technique. User revocation is a challenging problem because each attribute is feasibly distributed by multiple clients. Revocation of any particular client would concern others who distribute the similar characteristics. Here they mainly focus on realistic application circumstances for example data sharing and allocation as shown by Figure.3, in which proxy servers are always accessible for providing dissimilar kinds of data services.

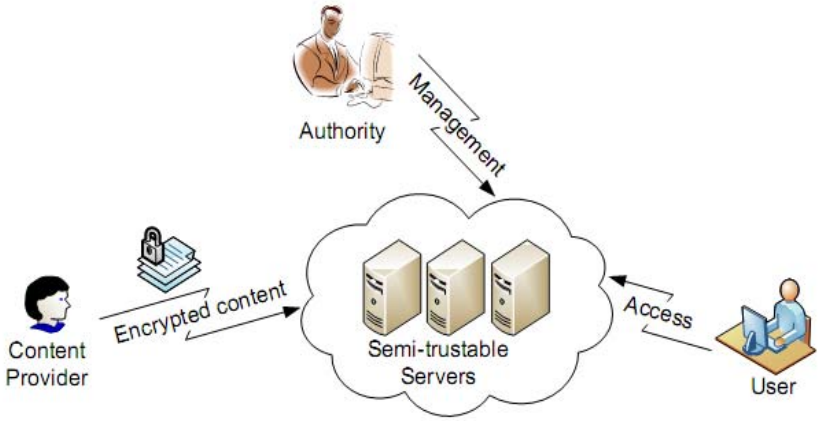

Figure 3: An example application scenario of data sharing.

Similar to preceding work [5], these servers are imagined to be interested but straightforward as an alternative of being entirely untrusted. Specifically, they will directly execute the jobs allocated by genuine parties in the scheme. On the other hand, they have the encouragement to become skilled at the substances of encrypted data as much as feasible. The authority to allocate most expanded jobs of client revocation to proxy servers without revealing any secret data to them. On each revocation occurrence, the ability just produces numerous proxy re-encryption keys and broadcasts them to proxy servers. Proxy servers will keep intimated private keys for all customers but the one to be revoked. In this mode their construction puts minimal load on the ability upon each revocation occurrence.

II. LITERATURE SURVEY

In this method author has [7] using Protected Hash function for authentication reason, Secure Hash function is the one of numerous cryptographic hash functions, most regularly used to authenticate that a file has been unchanged. The Paillier Cryptosystem is a probabilistic asymmetric technique for public key cryptography. Revoked clients cannot have the right to use data after they have been revoked. The projected technique is elastic to replay show aggressions. A writer whose characteristics and keys have been revoked cannot write back decomposed data. The protocol sustains numerous read and writes on the information collected in the cloud. The expenditures are similar to the subsisting concentrated approaches and the luxurious procedures are more often than not completed by the cloud. Proposing privacy preserving confirmed access regulated technique. According to our method a client can generate a folder and supply it progressively in the cloud. This method consists of utilize of the two protocols ABE and ABS. The cloud verifies the genuineness of the client without knowing the user's individuality before storing information. The system also has the additional characteristic of access control in which only legitimate clients are able to decode the collected information The cloud does not know the characteristics of the user who stores the information, but only confirm the user's documentations. Key allocation is done in a decentralized technique and also conceals the attributes and admittance rule of a client. One drawback is that the cloud be familiar with the access policy for each confirmation collected in the obscure. The technique circumvents repetition attacks and sustains conception, alteration and reading statistics collected in the cloud.

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters [8] initiated the idea of Attribute-Based Encoding for Fine Grained admission manage of Encoded information . He begins the new idea of cryptosystem for fine grained sharing of encoded information i.e. call Key Strategy Attribute-Based Encryption (KPABE). In cryptosystem, cipher texts are labelled with sets of characteristics and intimate solutions are connected with admission arrangements that manage which cipher texts a client is capable to decrypt. Fine-grained admittance controller systems make possible granting differential access rights to a set of consumers and permit elasticity in identifying the access rights of entity clients. Numerous methods are known for applying acceptable grained admittance control. Clandestine distribution scheme (SSS) are used to partition a underground amongst a numeral of parties.

In this broadside writer comprehensive exploit of CP-ABE in the background of innovativeness submissions and also protracted a cancellation method that concurrently permits high flexibility, Fine-grained admittance controller and revocation. The section allocates clients a set of characteristics within their secret key and distributes the secret key to the separate clients. Any client that assures the admission organize strategy described from the data associate can right to use the data. When a client is revoked admittance human rights the data is re-encrypted in the Cloud representation the revoked user's key useless. The method is established to be semantically protected against preferred cipher passage attacks against the CP-ABE model. On the other

hand, the method is not well-designed in the case of client revocation since the inform of cipher texts after user revocation places serious calculation in the clouds even if the load is relocated to the Cloud [9].

Lei et al. [10] then proposed the CL-PRE (Certificate Less Proxy Re-Encryption) method for protected information distribution in communal cloud backgrounds. Even though their method is based on CL-PKC to explain the key escrow difficulty and certificate management, it relies on pairing process. Even though modern progress in implementation methods, the computational expenditures need for pairing are still significantly high evaluated to the costs of normal processes such as segmental exponentiation in restricted fields. Additionally, their method only accomplishes Selected Plaintext Occurrence (CPA) security CPA security is frequently not adequate to assurance security in common protocol settings. Such as, CPA is not adequate for many requests such as encoded email forwarding and sheltered information allocation that necessitate refuge against selected Cipher text Attack (CCA).

In this paper [11], here author has concentrate on the inadequacies of such earlier approaches and recommend a new mediated Certificate Less Public Key Encryption (CL-PKE) method that does not use pairing procedures. Since most CL-PKC methods are based on bilinear pairings, they are computationally costly. Our method reduces the computational in the clouds by using a grouping free tactic. Additional, the calculation costs for decryption at the operators are reduced as a semi-trusted security mediator incompletely decoded the encoded statistics before the client's decrypt. The protection mediator acts as a guiding principle enforcement point as well and sustains immediate revocation of cooperation or malicious clients. Based on our CL-PKE method, they propose a new tactic to promise the privacy of information collected in communal clouds while enforcing access control conditions. There are five entities in our scheme: the information proprietor, users, the sanctuary Mediator (SEM), the Key making Centre (KGC), and the storage space service.

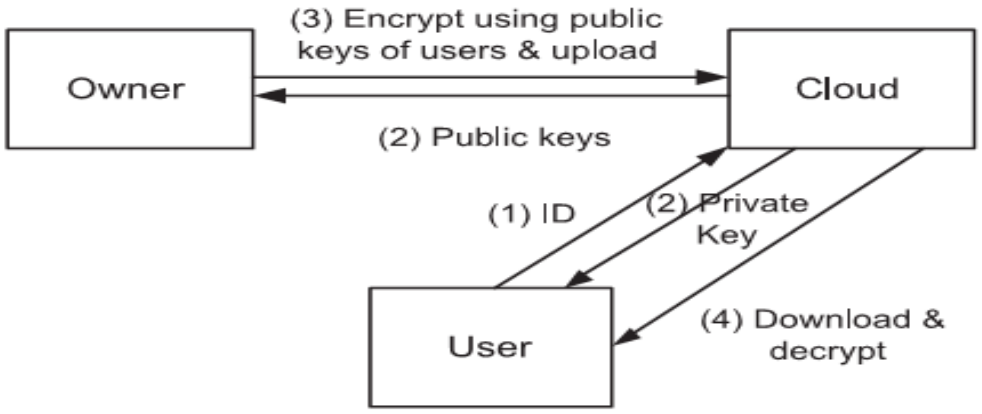

Figure-4: CL-PKE based fine-grained encryption [11].

The SEM, KGC, and the storage service are semi-trusted and be located in a public cloud. Even though they are not trusted for the privacy of the data and the keys, they are trusted for accomplish the protocols appropriately. According to the access control procedure the information proprietor encodes a symmetric information encryption key using CL-PKE method and encodes the information items using symmetric encryption algorithm. Subsequently, statistics proprietor uploads encoded information substance and the encoded information encoded key to the obscure. To become aware of that a most important benefit of our approach evaluated to traditional approaches is that the KGC, which is the thing in charge of generating the keys, exist in a public cloud.

Here author has proposed the merging of Attribute-Based Encryption (ABE) with proxy re-encryption in a cloud computing function permitting Fine-grained admittance controller of resources while attempt to offload re-encryption action to the cloud wage-earner [12]. This method has many discrepancies to the cloud-based re-encryption method that will be anticipated; these differences demonstrate to be inconvenient in a mobile-based environment. The data owner, or designer, is engaged in generating a key for each novel client that joins leaves the method, rather than delegating this job to a trusted key authority below the client's manage. This is not only a excessive charge for a mobile client, but also unfeasible due to the user's mobility and consequently infrequent unavailability. Another difference is that a secret key must be renewed and re-distributed for each client in idle approach, whenever you like client revocation happens, to a certain extent than permitting clients to improve a widespread partition key based on public parameters which would decrease communication and consequence in higher competence. Also, the data re-encryption activity is combined in idle style, while in this suggestion, re-encryption occurs enthusiastically on an as-required starting point to a countless degree falling server workload for data mainly right to use by just about the same set of users over time. The re-encryption takes place due to attribute re-definition, unlike the proposal. There is also no capability for switching crucial substantial in peer-

to-peer manner, which would be beneficial amongst mobile users utilizing cheap local wireless links such as Bluetooth. Finally, the scheme is based on KP-ABE (Key-Policy Attribute-Based Encryption), not CP-ABE.

III. PROPOSED METHODOLOGY

The planned procedure implemented here works on the basis of following modules.

1. If 'N' number of users wants to share to store data at the data centers 'DC' of the cloud.
2. TTP generates 'AccPol' access policy for the users 'U' based on his identity and role.
3. User 'U' generates a Identity 'ID' and encodes the information and make a tuple containing Encrypted data and Identity and Role and MAC Code for verification.
4. TTP accepts the data and stored at the data center 'DC' based on access policy of the user 'U'.
5. The user 'U' when access the data will send the individuality and admittance policy to the TTP and TTP verifies and authenticate that user.
6. The user then receiver his stores data and decrypt using his public key and again generates a MAC code for the confirmation of the data.

The Algorithm is based on the concept of applying Elliptic Curve based Signcryption with some Access Policy rules for the Sharing of Data over public Clouds.

The Algorithm consists of certain phases for the secure sharing of data over Cloud, which includes:

Setup: Here, in this phase general Elliptic Curve Equation is selected. Elliptic Curve Cryptography is a technique, which is based on the Concept of Elliptic curve theory, which is, based Hard Logarithmic Problem that can be castoff to generate quicker, slighter and actual Cryptographic Keys. Elliptic Curve Cryptography is used for the generation of Keys by using the Elliptic Curve Equations. Elliptic Curve Cryptography yields a level of Security from 164-bits keys to 1024 bits depends on the System Requirements.

The General Equation of the Elliptic Curves is given as:

$$y^2 = x^3 + ax + b, \text{ where } 4a^3 + 27b^2 \neq 0$$

The Setup phase also includes setup of the Cloud Environment, which includes selection of number of Cloudlets and Virtual Machines and Brokers and Data Centers. The Physical Configuration for each element of the cloud is setup at this phase.

Key Generation: here in this phase each User generates a pair of Public and Secrete Key for the Secure Sharing of Data. When User of the Cloud wants to share data with other User's of the Cloud, first of all both the Parties choose random point over Elliptic Curve which is Secrete Key for the Users and also both the parties shares a common Base Point Over Elliptic Curve and by using Base Point and Secrete Keys Public Keys can be generated. Let us suppose Users 'U1' chooses a random point Over Elliptic Curve, then 'S' is the Secrete Key for User 'U1' and 'S1' be the Secrete Key for User 'U2'. Also 'B' is the Chosen Base Point for both Users 'U1' and 'U2', then

$$P = S * B \ \& \ P1 = S1 * B$$

Where, P1 & P2 are the Public Keys for User 'U1' and 'U2'.

Signature Generation: The Message or Data to be Shared, for that random integer value 'u' is selected and from the integer value Tag value is generated.

$$Tag_m = name||n||u||Sig_{sk}$$

Sender Generates Signatures Sig_g for each of the message m_i,

$$Sig_g = (H(m_i).um_i)^{\alpha}$$

Encryption: Here in this phase Encryption is done by applying Signature and Encryption Simultaneously at the same time at the Client Side. Sender selects a random value from range [1,…p-1], Client uses the public key of Receiver and 'x' to generate hash from it which is of 128 bit String. The 128 bit string is then Split into two halves (k1,k2) key pairs.

$$(k1, k2) < -k < -hash(x, P1)$$

If 'm' is the message for Encryption, then cipher text can be computed using,

$$c = Ek1(m)$$

Also using Key Pairs K2 random integer is generated,

$$r = KHk2(m)$$

$$T = \frac{x}{(r + S) mod\ q}$$

Client sends (c, ,r, T) to the Receiver.

Decryption: Here in this phase Receiver uses the Parameter 'r' and 'T' and private key 'S1'.

(k1, k2)$< -k = hash((P1 * r)T * S1\ mod\ p)$

$$m = Dk1(c)$$
$$KHk2(m) = r$$

Verifying Access Policies

Here some of the policies have been written on the access of the user. Admin has the special access to any part of the database including no policy issues for the administrator. However, some of the policies have been made for the user so that the user can't access all the tables in the database.

Table 1. Access policy 1 for user

Access Policies for the user
if user is "user" and attempts >3 Access denied

Table 2. Access policy 2 for user

Access policies for the user
If role !=DBA Source IP is conflicting Schema belongs to admin Access denied

Access of Denial of Service

There are certain security and policy checks implemented in the module for the access of the facilities of the user. The user is not lawful to access any feature that has been denied by the administrator.

Table 3. Denial of service policy 1

Denial of service 1
Is role = user?? If user -> another user Access denied by the administrator

Table 4. Denial of service policy 2

Denial of Service 2
Is role = user?? If user -> delete, update, insert new user Access denied by administrator

Table 5. Denial of Service policy 3

Denial of Service 3
Is role = user?? If user sends packets to another user If packet -> intrusion Access denied by administrator and blocked

Table 6. Access Policy for User

Access policies for user
Is role != admin If user --→ tables not permitted by admin Access denied to access table Admin respond and block user.

IV. CONCLUSION

Data sharing is a technique of allocation data or resources on cloud so that the user can access the data in an easy manner. However, during the sharing of information user needs to be authenticated, hence various techniques are implemented to ensure the accountability of shared data in the cloud. The proposed methodology implemented here for the sharing of information using Message Verification Code and Key Generation using Signcryption provides efficient results as connected to the prevailing technique.

The projected methodology implemented here provides less computational time and security from various attacks as well as less power consumption and ability to balance load at the data centres and the virtual machines.

V. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[2] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in Proc. 29th Int. Conf. VLDB, Berlin, Germany, 2003, pp. 898–909.

[3] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Knowl. Data Eng., vol. 25, no. 11, pp. 2602–2614, Sept. 2012.

[4] N. Shang, M. Nabeel, F. Paci, and E. Bertino,"A privacy-preserving approach to policy-based content dissemination," in Proc. 2010 IEEE 26th ICDE, Long Beach, CA, USA, pp. 944–955.

[5] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB'07, Vienna, Austria, 2007.

[6] Jiadi Yu, Peng Lu, Yanmin Zhu, Guangtao Xue, "Toward Secure Multikeyword Top-k k Retrieval over Encrypted Cloud Data" IEEE Transactions On Dependable and Secure Computing, Vol. 10, No. 4, July/August 2013.

[7] M. Suriyapriya, A. Joicy, "Attribute Based Encryption with Privacy Preserving In Clouds" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 2 Issue: 2 February 2014.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006

[9] Tu S, Niu S, Li H, Xiao-ming Y, Li M, "Fine-grained access control and revocation for sharing data on clouds," IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[10] X. W. Lei Xu and X. Zhang, "CL-PKE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud," in ACM Symp. Inform. Comput. Commun. Security, 2012

[11] Seung-Hyun Seo and Xiaoyu Ding, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th conference on Information communications, ser. INFOCOM'10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 534-542.