ISSN:0975-9646

An Effective & Secure Data Sharing using Elliptic Curve with MD-5 in Cloud Computing

Rahul Sharma
(Scholar)
Dept. of Information Technology
Truba Institute of Engg. & IT
Bhopal, India.

Manoj Tyagi
(Professor)
Dept. of Information Technology
Truba Institute of Engg. & IT
Bhopal, India.

Abstract— Here an efficient technique is implemented for the dynamic possession of data at the data centers. The algorithm implemented here starts with the creation of cloud and allots various users and data centers at the virtual machine to send their information in a protected manner. First of all the data from various users are set up and load is computed at each end of the records centers then setup and key generation takes place and finally encryption and decryption of the data is done. The planned tactic implemented here provides less computational time for the various Dynamic Operations to perform on Multiple Copies. The methodology also proofs to be more secure since it resolves the problem of User Revocation and Escrow Problem. It also provides less Computational time for Verification and Proof.

***Index Terms*—**Data Centers, Virtual Machines, Authentication, Multi-Copies, Brokers, Data Sharing.

I. INTRODUCTION

Outsourcing data from information owners to Data Centers requires a lot of security and computational overhead [1]. The recent advancements in technology have misused the system how electronic data is stored and retrieved. Nowadays, individuals and enterprises are increasingly utilizing remote services (such as Dropbox [2], Google Cloud Storage [3] and Amazon effortless Storage examine [4]), mainly for economical benefits. These services not only facilitate information sharing but also ensure availability of data from anywhere at any time. However, the rising use of remote services raises serious privacy issues by putting personal data at risk, particularly when the server's offering such services are untrusted. Unfortunately, servers get straight admission to the information they store and process. For protecting sensitive data from servers in untrusted environments, data could be encrypted before leaving trusted boundaries. Regardless of whether the data is encrypted or not, the server resolve want to decide who will increase admission to it. For regulating admittance to the information, access control policies could be specified. These are access control policies that will describe who can increase admittance to the data. State-of-the-art policy-based systems can ensure enforcement of these policies. However, the matter becomes complicated when sensitive policies, which may leak private information, have to be enforced in untrusted environments. While there may immobile be particular misperception as to what accurately Cloud Computing resources, and no universal accord on a definition for Cloud Computing has been reached [5, 6], for the extent of this employment we shall adopt the informal definition of Cloud Computing proposed in [7].

Recently data in the cloud server, in attendance has be a staged augment in the reputation of cloud computing systems (e.g., Amazon's EC2 and Rackspace Cloud) that lease computing possessions on command, tab on a pay-as-you-go source, and complex many clients on the equivalent corporal communications.

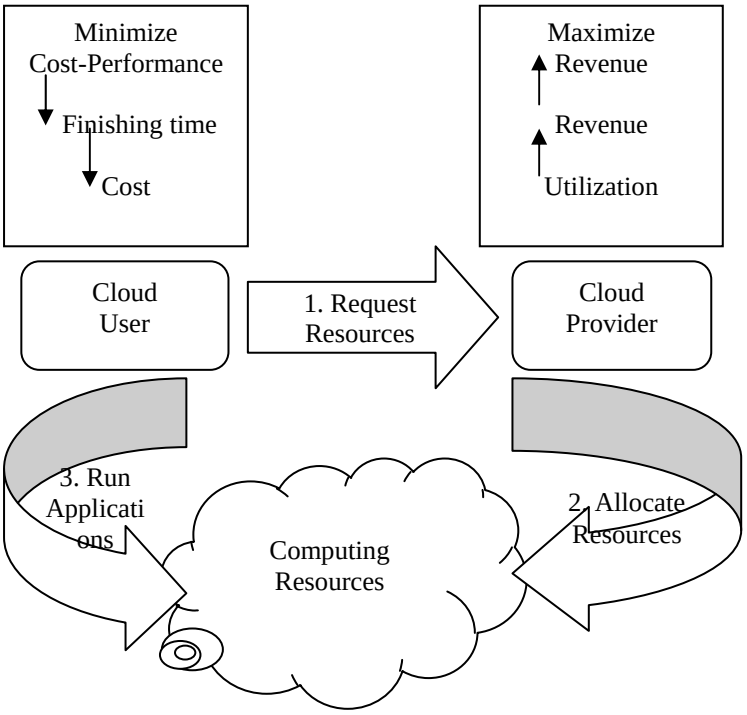

Figure 1: Cloud Usage Scenario over on cloud environment.

DATA SHARING ON THE CLOUD

Cloud Computing is a promising next-generation IT architecture which provides elastic and unlimited resources, including storage, as services to cloud users. In Computing of clouds client and cloud overhaul providers are approximately convinced to be from different faith domains. It turns out that on single offer sensitive data should be encrypted before uploading to cloud servers.

Similar to any untrusted storage case, we can resolve the issue using a cryptographic-based information admission organize mechanism. Consumer revocation is a defy matter since each attribute is conceivably shared by multiple

users. Revocation of any lone consumer would involve others who contribute to the equivalent attributes. We predominantly center on matter-of-fact function scenarios such as information storage and allocation, as given away by Figure.2.3, in which deputy servers for eternity exist for given that a mixture of types of information military.

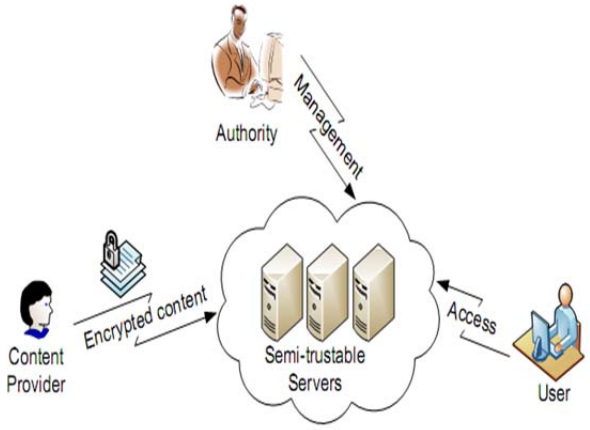

Figure 2: An example application scenario of data sharing.

II. Literature Survey

To achieve a protected and dependable cloud storage service, a secure multi-owner data sharing method is proposed [8] according to any user in the group so that they can steadily split information with others users by the un-trusted cloud. The Group manager is used for decrease of the execution time of the key production at the user end or data owner side. Public-key cryptosystem construct constant-size ciphertext as proficient assignment of decryption privileges for any position of ciphertexts are achievable. Anyone can comprehensive any set of secret keys and make them as compressed as a single key. The private key proprietor can generate a constant-size aggregate key of ciphertext set in cloud, but another encrypted files outside stay behind secret. The aggregate key strongly sent to users or keep in a smart card with limited storage. We characterize recognized investigation of security in the average model.

The Trusted Computing cluster (TCG) [9] provided the trusted computing technology. This distinguishing knowledge is debatably the amalgamation of ancestry of faith into mainframe platforms. since single of the major issues opposite computer knowledge nowadays is information refuge, and the dilemma has gotten inferior since clients are operational with receptive in sequence extra frequently, while the numeral of intimidation is mounting and hackers are increasing original types of attacks, many knowledge researchers promoter progress of trusted computing systems that incorporate information security apparatus into their hub operations, slightly than implementing it by means of add-on applications [9].

In this paper, author [10] presents a new solitude preserving safety resolution for cloud military. Here in this method transaction with user unspecified admission to cloud military and communal space servers using non-bilinear group signatures to ensure anonymous authentication of cloud service client's user. Clients use interfere unwilling strategy during the generation and storing of user keys to protect against collusion attacks. Here the resolution provides registered clients with unidentified admission to cloud military and also offers unidentified verification.

In this manuscript author [11] has try to assess how can cloud providers earn their customer's trust and provide the sanctuary, seclusion and dependability, when a third party is meting out sensitive data in a remote machine established in various countries. A thought of usefulness cloud has been characterized to provide a variety of military to the clients. Various technologies can assist to concentrate on the challenges of refuge, solitude and belief in cloud computing.

In this schemes can be practical on peak of any DPDP protocol where the client has no secret key, as defined by Erway et al. [12]. Here their schemes are the only methods that can be used for authorized negotiation not public verifiability of any DPDP scheme, to the best of our knowledge. Consequently, in the performance subdivision, here they only compare two of our methods. Here they provide the first constructions of general-purpose negotiation methods that are applicable to various static and dynamic circumstances, and proficient of performing fully-automated settlement by a Judge. Here their model builds upon the DPDP model [12], and thus is applicable to a extensive variety of protocols.

III. Proposed Methodology

The Proposed work implemented here for the Data Sharing using Dynamic Multi Copies at CSP. The Algorithm implemented contains the following steps:

1. First of all create Data Owner and CSP (Server & Data Center) and Receiver and Brokers and Key Generation Center.
2. Data Owner Starts Sending Files.
3. Create Dynamic Copies of the File.
4. Encrypt each of the file and send to the Server.
5. Server and Key Generation Center creates a Master Secret key and Re-encrypts the encrypted file and store to various Data Centers.
6. Receiver request to server to access the shared data.
7. Server is authenticating receiver.
8. If authenticated server decrypts the file and send the encrypted file to the receiver.
9. Receiver finally decrypts the file.
10. Verification is done by the receiver.

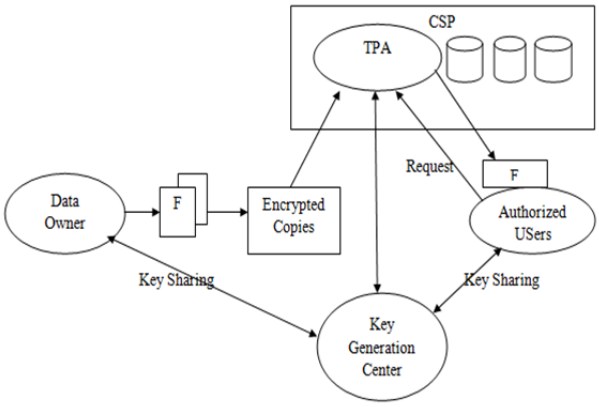

Figure 3. Flow Chart of the Working Methodology

The methodology implemented here consists of Following Functions for the operation to perform Data Sharing.
Setup: Here in the set up phase is between Data Owner and Receiver. Where Selection of Elliptic Curve Parameters are Chosen between Data Owner and Receiver.

Key Generation: Here in this phase Elliptic Curve Keys are setup and generated by the Data Owner and receiver.
SigGen: Here in this phase Generation of Signatures for Various Copies to be shared with TPA is generated.
Proxy re-encryption: This phase is used by TPA for the Re-encryption of Shared Data by the Data Owner on the basis of Shared Master Secret Key between TPA and Key Generation Center.
Dynamic Operations: This phase is used for the Data Modification by the Data Owner such as Modification and Updation and Insertion.

Verification: This Phase is used for the Verification of the Identity of receiver.

F	Shared Data File F={m_1,m_2….m_n}	CH	Challenge Values
M_i	i^{th} Data Block	H( )	One Way hash Function
N	Shared Data Block Number of i^{th} File.	V	Verification
L	Length of the shared data block	S_g	Digital Signatures
R	Root node	B	Base Point
Pk	Public key	α	Prime random integer
Sk	Secret key	Sk_{tpa}	TPA Secret Key
T_m	Tag of the Shared Data Block m	Sk_{kgc}	KGC Secret Key

Table 1: Various Annotations Used in Algorithm

Setup: Here in this phase first of all the Elliptic Curve Parameters are set and after that public and private key pairs are generated using KeyGen(.). Suppose the General Elliptic Curve Equation is defined by:

$$y^2 = ax^3 + bx + c$$

Where, $4a^3 + 27b^2 \neq 0$

Client chooses any random point over elliptic Curve E(F) that would be the chosen Secret key of the client 'Sk', using secret key and Common Base Point 'B', public key is generated.

$$Pk=Sk.B$$

SigGen: The Shared Data File F={m_1,m_2…m_n}, first of all choose a random integer ‘u’ and hence generate Tag for the Shared Data File 'F' using

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

Client Starts generating Signatures S_g for each of the block m_i,

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

The Client starts generating Linked List based on the signatures and create a First Node of the Linked List and the other Nodes are constructed using H(m_i).
Client Signs the Generated Started Linked List Root Node using secret key 'sk'

$$Sig_{sk}(H(R)) \leftarrow (H(R))^{\alpha}$$

Client Sends $\{F, T_m, S_g, Sig_{sk}(H(R))\}$ to Third Party Auditor (TPA).

Proxy Re-encryption: When the Block is received to the TPA, then both TPA and Key Generation Center generates a Master Secret Key and Re-encrypts the Message block.

$$M_{sk} = H(Sk_{tpa}||Sk_{kgc})$$

Modification: This phase contains all the Dynamic Operations to be performed on the Data Shared on CSP. The Shared Data by the data Owner is Stored at Data Center with Separate or Same Data Centers. Each of the Copies is Stored in a Separate Linked List with a unique Signature for each of the encrypted Copy at data Center. The Operations to be performed are:

a) Insertion: If the Data Owner wants to Insert the Data Block after certain Position ‘j’. Data Owner will simply access the ‘j-1’ linked list position block and attached the newly created block after position ‘j+1’ and linked each of the ‘j+2’ block by value 1.

b) Deletion: If the Data Owner wants to Delete the Data Block at certain Position ‘j’. Data Owner will simply access the ‘j-1’ linked list position block and attached block after position ‘j+1’ and linked these two blocks.

c) Updation: If the Data Owner wants to Update the Data Block at certain Position ‘j’. Data Owner will simply access the ‘j’ linked list position block and update the data at Position ‘j’.

Verification: This phase is implemented at the Receiver end where receiver enters his details which are then send to TPA for Verification. TPA will Verifies the Details of the Receiver by the Matching the details with KGC. As soon as Verification is done TPA along with KGC Decrypted the Re-encrypted File and a Onetime Encrypted File is access by the Receiver which is then decrypted using Public key of Receiver.

IV. Result Analysis

The Table shown below is the analysis and comparison of Data Owner Computational Time in Sec for the Various Dynamic Operations on a Single Block. The Proposed Methodology implemented takes less Computational Time as Compared to the Existing Methodology implemented.

	Computational Time (Sec)	
No. of Copies	**Existing Work**	**Proposed Work**
1	0.261	0.255
5	1.304	1.047
10	2.608	2.395
15	3.913	3.661
20	5.217	4.892

Table 2. Analysis of Computational Time

The Figure shown below is the analysis and Comparison of Proof Computational Time in sec between Existing MB-MDDP work and the proposed methodology. The Proposed Methodology implemented here provides efficient and less Computation time for Verification.

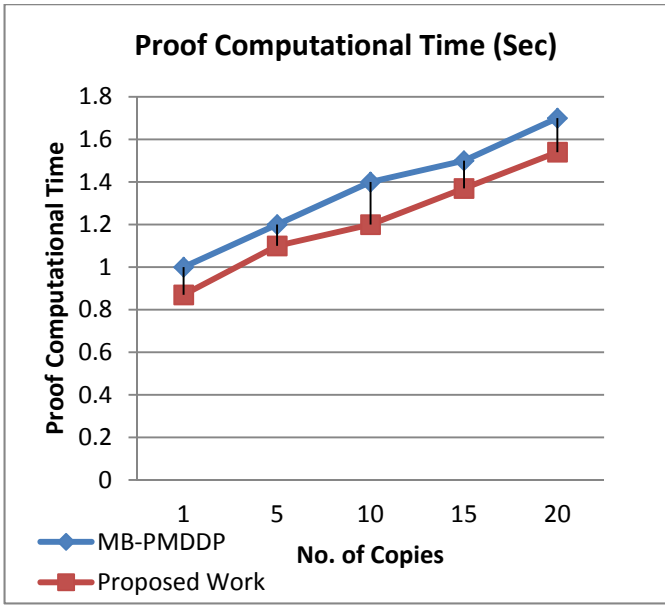

Figure 4. Proof Computational Time in Sec

The Table shown below is the analysis and Comparison of Proof Computational Time in sec between Existing MB-MDDP work and the proposed methodology. The Proposed Methodology implemented here provides efficient and less Computation time for Verification.

No. of Copies	MB-PMDDP	Proposed Work
1	0.90	0.87
5	1.2	1.1
10	1.4	1.2
15	1.47	1.37
20	1.51	1.54

Table 3. Analysis of Proof Computational Time in Sec

The Figure Shown below is the Analysis and Comparison of Verification Time in Sec Between MB-PDDP and the proposed Work. The Proposed Work has verification time less than that of MB-PDDP scheme. For 20 Copies, the verification times for MB-PDDP and Proposed work is 1.58 and 1.51 respectively.

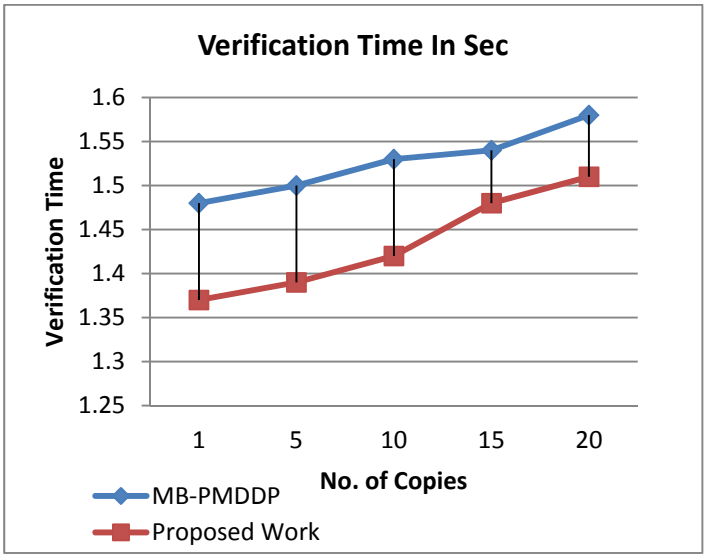

Figure 5. Verification Time in Sec

The Table Shown below is the Analysis and Comparison of Verification Time in Sec Between MB-PDDP and the proposed Work. The Proposed Work has verification time less than that of MB-PDDP scheme. For 20 Copies, the verification times for MB-PDDP and proposed work is 1.58 and 1.51 respectively.

No. of Copies	MB-PMDDP	Proposed Work
1	1.48	1.37
5	1.5	1.39
10	1.53	1.42
15	1.54	1.48
20	1.58	1.51

Table 4. Comparison of Verification Time in Sec

V. Conclusion

Data Sharing is a way of sharing data or resources in the cloud so that the user can access the data in an easy manner. But During the sharing of data users 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 data using Message Authentication Code and Key Generation using Elliptic Curve Cryptography provides efficient results as compared to the existing technique.

The proposed methodology implemented here provides less computational time and security from various attacks as well as perform Efficient Dynamic Operations on various Copies to be shared. It also provides Efficient User revocation and Security from Escrow Problem.

REFERENCES

[1] Ayad F. Barsoum and M. Anwar Hasan," Provable MultiCopy Dynamic Data Possession in Cloud Computing Systems", IEEE Transaction on Information Forensics and Security, Vol. 10, No. 3, March 2015.

[2] "Dropbox." https://www.dropbox.com/. October 30, 2013.

[3] Google, "Google cloud storage pricing." https://cloud.google.com/pricing/cloud-storage, February 2013.

[4] Amazon, "Amazon simple storage service (Amazon S3)." http://aws.amazon.com/s3/#pricing, February 2013.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53:50–58, April 2010.

[6] Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1:7–18, 2010. 10.1007/s13174-010-0007-6.

[7] P. Mell and T. Grance. The NIST Definition of Cloud Computing (Draft)–Recommendations of the National Institute of Standards and Technology. Special publication 800-145 (draft), Gaithersburg (MD), Jan. 2011.

[8] Gade Swati,Prof.Prashant Kumbharkar, "CRYPTOSYSTEM FOR SECURE DATA SHARING IN CLOUD STORAGE" IJIRT Volume 1 Issue 6 2014.

[9] N. Leavitt, "Is Cloud Computing Really Ready for Prime Time?," Computing Now, pp. 15-20, 2009.

[10] Lukas Malina and Jan Hajny, "Efficient Security Solution for Privacy-Preserving Cloud Services" 6th INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013.

[11] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing "JCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[12] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia. Dynamic provable data possession. In ACM CCS, 2009