ISSN 2320-9984
Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Preserving Cloud Storage Data Security using Identity based Encryption with Elliptic Curves

Deepika Gour
Research Scholar
Department of Computer Science and Engineering
Jai Narain College of Technology
Bhopal, (M.P.), [INDIA]
Email : deepika.gour.1990@gmail.com

Prof B.L. Rai
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA] Email: blrai_08_76Yahoo.com

Prof. Shweta Gupta
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: 6.shwetagupta@gmail.com

Dr. Mukta Bhatele
Professor and Head of Department
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P.)India
Email: mukta_bhatele@rediffmail.com

Abstract*—*Security is an important issue during the access and storage in cloud environment. Cloud computing enables various users to access and store their data through internet on data centers, but there are various security issues which needs to be solved during these transmission over cloud. The existing protocol implemented for the security of cloud over public verifiability provides security from various attacks such as man-in the middle attack [1]. But further enhancements can be done for the improvement of these resources using an efficient protocol of elliptic curve based key generation. The proposed methodology implemented here uses elliptic curves for the key generation and then cloud data can be encrypted using identity based encryption. The methodology implemented here is secure against various attacks as well as provides less auditing time.

Keywords*:—*Virtualization, Auditing Protocol, TPA, Cloud Data Storage, PAAS, SAAS.

1. INTRODUCTION

Cloud Computing is the most modern trend of today's IT industries. It is the key for the difficulty that take places due to the resources ease of use and its exploitation over the network. The attractiveness of cloud computing has enhanced due to its enormous guiding principle of pay-as-you-use or resource-on-demand but unmoving it be deficient in with confident concerns of security, confidence and effectiveness when put into practiced or organized on large activity such as in geological surveys, astrological applications, oceanography scientific applications, etc. Cloud computing is a computing representation in which hardware, software platform, and infrastructure are characterized and distributed as a service to a certain extent than a product. Cloud computing is promising [8] from modern progress in technologies such as hardware virtualization, Web services, distributed computing, utility computing and system automation.

Cloud computing acquires improvement of hardware virtualization to steadily and enthusiastically distribute physical resources

such as computational power, storage, and networks to the users. Clouds resources are distributed to the end-users through Web services. These uncomplicated model consequences in the following good-looking features:

Elasticity: Since physical resources are dynamically allocated to the consumers according to their needs, cloud services can scale on-demand.

Cost Effectiveness: Resource sharing improves utilization of physical resources and thus reduces the associated cost.

Pay-as-you-go Pricing Model: Cloud services have consumption-based metering and billing; this property makes them more affordable for small businesses and startups.

Global-scale Accessibility and Usability: Cloud consumers have access to a virtually unlimited physical resource pool through Web.

Easy Maintenance: All non-functional requirements of IT, such as maintenance of hardware and software, are addressed by cloud providers, therefore consumers can concentrate on their functional business requirements.

There exist lots of explanation in security concerns and lots of research for its effectiveness but nobody of them focuses on the both problems simultaneously. All outsourcing storage into the cloud is cost-effectively good-looking for the cost and complexity of long term large-scale data storage. At the same time, such a service is also eliminating data owners' crucial control over the providence of their data, which data owners with high service-level constraints have conventionally awaited. As owners no longer physically possess their cloud data, earlier cryptographic ancients for the rationale of storage suitability protection cannot be accepted, due to their constraint of local data copy for the integrity authentication.

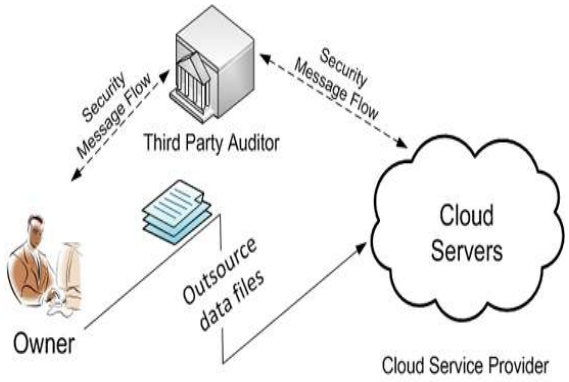

Figure 1: Architecture of cloud storage.

In addition, the large amount of cloud data and owner's confined computing competence additional makes the job of data correctness auditing in a cloud environment exclusive and even difficult for entity cloud customers. Consequently, facilitating public auditability [1], [2], [3] for cloud storage is of critical importance so that owners can alternative to a concentrated third party auditor (TPA) to audit cloud storage services and sustain strong storage accuracy assurance, while saving their own valuable computing resources.

Considering TPA strength become skilled at unauthorized information through the auditing process, particularly from owners' unencrypted cloud data, new privacy-preserving storage auditing explanations are further required in the cloud [1], [4], [5] to abolish such new data privacy vulnerabilities. Furthermore, for realistic service deployment, secure cloud storage auditing should sustain the same level of data correctness declaration still under the circumstance that data is enthusiastically altering [2], [3], [6], [7] and/or multiple auditing apply for carry out at the same time for progressed competence [1], [2], [4], [5].

Data storage correctness or some time more usually pass on as data integrity verification is one of principal cloud security problems. Data can be altered by unauthorized entity without intimating to data owner. How would the data owner make sure that his data has not been modified by other. So detecting such kind of unlawful activities on data is an

utmost priority issue. Due to such kind of reasons, we prefer an approach where the functionalities of TPA Auditing Manager are integrated in form of client application and the application can be downloaded by cloud user from cloud server. This client application provides all the cryptographic functionalities to achieve the goals of integrity, authentication and confidentiality. As this is a software come within reach of the routine of the taken as a whole system may not be comparable to dedicated hardware kind of TPA Auditing Manager during the storage security Process.

As data in Cloud is dynamic, static auditing is not an adequate amount of cloud environment. A dynamic auditing is required to authenticate the data integrity of the dynamic data. But as data are self-motivated in cloud, it is not uncomplicated to have an auditing competently. Server can put into effect replay attack and counterfeit attack to fail the auditing procedure. The dynamic procedures consist of alteration, insertion and deletion. Whenever you like dynamic operation is achieved the owner sends to bring up to date message to the auditor characterizing the index number of that message. The auditor updates the table. The message m and the tag are reinstated by the new message and tag in message modification. The new message m and new tag are inserted in insertion operation. The message m and tag are deleted from the index table and all the entries below the deleted message move upwards. After performing updates in the table, the auditor conducts the data integrity test for the keep informed data. Auditor sends the consequence to the owner and he deletes the local copy of keep informed data.

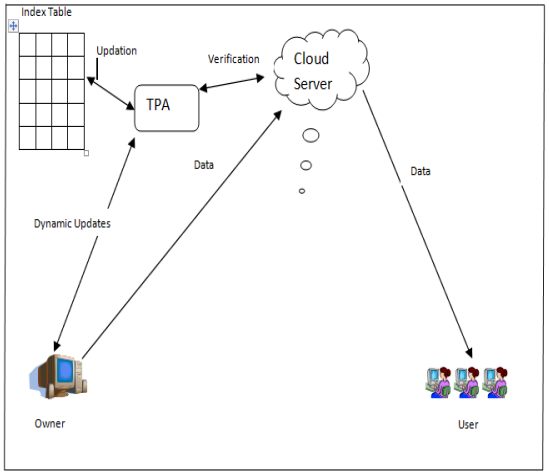

Figure.2: Dynamic TPA System

As the number of cloud provider's enlarges, deciding a trusted service became deadly. The auditing method is essential to make your mind up the cloud integrity concerns. There are different auditing structure suggested in cloud computing. But most of them are stationary in environment and they are put into practiced by cloud providers. With the intention of have dynamic examining, Dynamic Third Party Auditing System is recommend. The most important improvement of the recommended system is that the data integrity is confirmed on dynamic data by the third party auditor. As the data integrity is established by third party auditor, auditing becomes visible to the client user.

2. LITERATURE SURVEY

In the paper[9], the authors proposed a cooperative provable data possession for integrity verification in multi-cloud storage. In their method, the authors apply the mask technique to ensure the data confidentiality, such that it necessitates an extra confidences organizer to send a commitment to the auditor during the commitment phase in multi-cloud batch auditing. The TSAS be appropriate the encryption technique with the Bilinearity property of the bilinear pairing to ensure the data privacy, rather than the mask method. Consequently, the multi-cloud batch auditing protocol does not have any assurance part, such that it does not necessitate any further trusted organizer.

Ateniese et al. proposed a Sampling ProvableData Possession (SPDP) scheme [10], which combines the RSA cryptography with Homomorphic Verifiable Tags (HVT). It divides the data into several data blocks and encrypts each data block. For each auditing query, the auditor only challenges a subset of data blocks. By using such sampling method, the integrity of entire data can be guaranteed, when sufficient numbers of such sampling auditing queries are conducted. This sampling mechanism is applied in much remote integrity checking scheme, because it could significantly reduce the workloads of the server. Although the SPDP scheme can keep the data confidentiality, it cannot sustain the dynamic auditing and the batch auditing for multiple possessors.

Erway et al. [12] also extended the PDP model to support dynamic updates on the stored data and proposed two dynamic provable data possession scheme by using a new version of authenticated dictionaries based on rank information. On the other hand, their methods may reason profound calculation trouble to the server since they relied on the PDP scheme proposed by the Ateniese.

To support the dynamic auditing, Ateniese et al. developed a dynamic provable data possession protocol [11] based on cryptographic hash function and symmetric key encryption. Their idea is to pre-compute a certain number of metadata during the arrangement phase, so that the numeral of keep informed and confronts is limited and fixed before hand. In their protocol, each update operation requires recreating all the stay behind metadata, which is challenging for huge number of files. Furthermore, their protocol cannot achieve block insertions anywhere only append-type insertions are allowed.

In this paper author [13] uses the new password at each instance which will be transferred to the mail server for each request to obtain data security and data integrity of cloud computing [13]. This protocol is secure against an untrusted server as well as third party auditor. Client as well as trusted third party verifier should be able to detect the changes done by the third party auditor. The client data should be kept private against third party verifier. It supports public verifiability without help of a third party auditor. This protocol does not leak any information to the third party verifier to obtain data protection. This proposed protocol is protected aligned with the untrusted server and private against third party verifier and support data self-motivated. In this arrangement, the password is produced and that will be transferred to email address of the client. Every time a key is used to achieve different operations such as insert, update delete on cloud data. It uses time based UUID algorithm for key making based on pseudo random numbers generation method. If an intruder tries to right of entry the users' data on a cloud, that IP address will be trapped and transferred to the user so that user will be aware of that.

In this paper, here author propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of users' data in the cloud. We rely on removal accreting code in the file distribution preparation to provide redundancies and guarantee the data dependability against Byzantine servers [14], where a storage server may fail in uninformed ways. This structure significantly decreases the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, their proposed method accomplishes the storage acceptableness assurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our method can approximately assurance the concurrent localization of data errors, i.e., the credentials of the disobedient server's. With the intention of strike a good balance between error resilience and data dynamics, here they further explore the algebraic property of our token computation and erasure-coded data, and demonstrate how

to efficiently support dynamic operation on data blocks, while sustaining the same level of storage accurateness declaration. With the intention of save the time, calculation resources, and even the communicated online burden of users, we also make available the expansion of the recommended major system to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors and are worry-free to use the cloud storage services.

3. PROPOSED METHODOLOGY

Here CP-ABE attribute based data sharing technique is used which solves key escrow problem and proxy encryption. It provides an efficient technique of attribute based encryption which prevents from various attacks. Cost ineffective and chances of security is less.

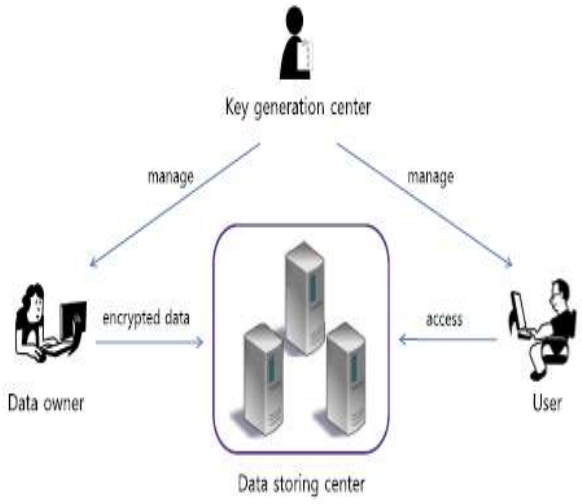

Figure 3 Cloud Data Storage & Sharing

Here in the Proposed work contains data owner, User, Data Storing center and key generation center. The data to be send is encrypted using the attribute policies to the data storing center which can be accessed by the user only after authenticated by the key generation center.

Although the various attribute based key generation are implemented which provides security from various attacks in the network and also the chances of overhead cost reduces, but further enhancements can be done related to the security of these attribute based policies.

The algorithm contains the following phases:

- The sender generates an automated message and generates an identity string using message to be sending.
- The sender generates public key and private key from the identity and encrypts the message and makes tupple which contains identity and encrypted data and send to storage panel.
- The owner when access the data needs to be authenticated at the storage panel using identity and password that is generated by the sender.
- The owner after authenticates access the data based on identity and decrypts the message from the storage panel.

4. ECIES ALGORITHM

The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based encryption algorithm. It is a public-key encryption algorithm. It uses of domain parameters (K, E, q, h, G). It allows us to use symmetric encryption/decryption functions Ek (m) and Dk(c) by our choice which is easy to encrypt long messages. It uses elliptic curve encryption technique to choose the asymmetric public and private keys that is Y and X. The elliptic curve's equation is

$$E: y2 = x3 + ax + b$$

Step 1: Client has the data called message M and public key Y of reader and chooses a random number K from range R(1….. q-1) where q is a prime number.

Step 2: Client computes U <- [K]G, Where G is a common base point, K is selected random number.

Step 3: Client computes T <- [K]Y, where Y is a public key of reader, K is selected random number.

Step 4: Client computes keys k1 and k2 by applying key derivation function. (k1|| k2) <- KD (T, l), where T is the value computed in step 3 and l is the length of T.

Step 5: Client Encrypt the message by xor based encryption technique by using k1(step 4) as a key.

Ciphertext C<- E k1 (M)

Where E is encryption function k1 is key and M is message or data.

Step 6: Client computes a message authentication code r

r <- MAC k2 (C)

Where MAC is a hash function, k2 is key (step 4) and C is a ciyphertext (step 5)

Step 7: Client sends (U, C, r) and identity of message to the central data base (TTP).

If Receiver wants to access any data then it first have to authenticate itself to TTP by its prefix password, if password does match TTP allows reader to access the client's encrypted data then receiver can access the data.

Step 1: Receiver receives client's data (U, C, r) and apply his private key X to decrypt the data. it computes

T <- [X]U

Here U is received MAC and X is a private key of reciever.

Step 2: Compute (k1||k2) <- KD(T, l)

Here KD is key derivation function, T computed in step 1 and l is length of T.

Step 3: Receiver decrypt the cipher text and compute original message M

M <- DK k1 (C)

Here C is received cipher text DK is xor based decryption and k1 is key computed in step 2.

Step 4: Receiver computes MAC r'

r' <- MAC k2 (C)

Here MAC is hash function k2 is key computed in step 2. and C is received cipher text.

Step 5: Compare received r to computed r'

If r = r'

Then message M is correct, the receiver accept the message, otherwise discard it.

IV. Result Analysis

The table shown below is the cost introduced by the privacy preserving auditing in terms of server computation, auditor computation as well as communication overhead. Since the difference for choices on s has been discussed previously, in the following privacy-preserving cost analysis we only give the atomic operation analysis for the case s ¼ 1 for simplicity. The analysis for the case of s ¼ 10 follow similarly and are thus omitted.

Table 1 Comparison of Computational Time and Cost for s=1

s=1	Existing Work	Proposed Work
Sample Block c	460	460
Server Computational time (ms)	335.17	257.23
TPA Computational time (ms)	530.6	495.18
Computational Cost (bytes)	160	128/160

Table 2 Comparison of Computational Time and Cost for s=10

s=10	Existing Work	Proposed Work
Sample Block c	460	460
Server Computational time (ms)	361.56	280.61
TPA Computational time (ms)	547.39	503.37
Computational Cost (bytes)	1420	512/1024

The figure shown below is the analysis and comparison of various tasks to be performed during the privacy preservation of the clouds data storage security. The comparison between existing and proposed work is shown and hence the efficiency of the proposed methodology performs more auditing tasks in less time.

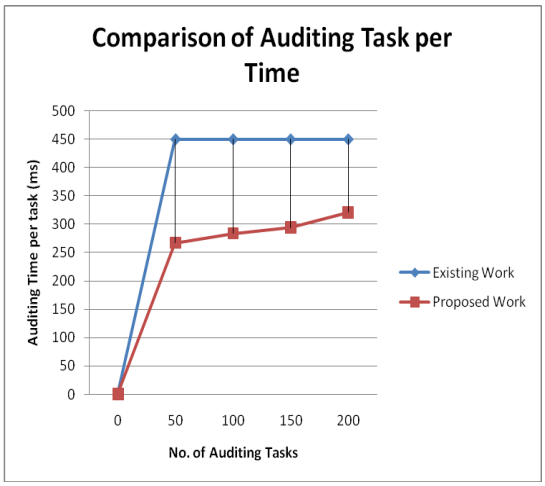

Figure 4 : Comparison of Auditing Taks per Time in ms

V. Conclusion

Cloud computing enables various users to share or access resources over internet, but during the data sharing or storage in cloud security plays a vital role and hence various auditing protocols are implemented for the security of these cloud data and also provides privacy preservation between users.

The proposed auditing protocol implemented here for the privacy preservation using hybrid combinatorial method of Identity based encryption with elliptic curve based cryptography for the encryption of data. The proposed methodology implemented here provides efficient results as compared to the existing auditing protocol implemented for the cloud data storage security. The proposed protocol implemented here for the cloud data storage security prevents from various attacks such as identity disclosure attacks, password impersonation and public verifiability. The proposed protocol also provides less cost for the privacy preservation in cloud as well as provides more number of auditing batch task in less time.

REFERENCES:

[1] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers (TC), 2011 (A preliminary version of this paper appeared at the 29th IEEE Conference on Computer Communications (INFOCOM'10)).

[2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", To appear, IEEE Transactions on Parallel and Distributed Systems (TPDS), Vol. 22, No. 5, pp. 847-859, May, 2011.

[3] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," To appear, IEEE Transactions on Service Computing (TSC). (A preliminary version of this paper appeared at the 17th IEEE International Workshop on Quality of Service (IWQoS'09)).

[4] Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Towards Publicly Auditable Secure Cloud Data Storage Services", IEEE Network Magazine, Vol. 24, No. 4, pp. 19-24, July/ August 2010.

[5] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-preserving Public Auditing for Data Storage Security in Cloud Computing", The 29th IEEE Conference on Computer Communications (INFOCOM'10), San Diego, CA, March 15-19, 2010.

[6] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", The 14th European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, September 21-23, 2009.

[7] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", The 17th IEEE International Workshop on Quality of Service (IWQoS'09), Charleston, South Carolina, July 13-15, 2009.

[8] NIST. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[9] Zhu,Y., Hu, H., Ahn, G., Yu, M.: Cooperative provable data possession for integrity verification in multi-cloud storage. IEEE Trans. Parallel Distrib. Syst. 23(12) 2231–2244 (2012)

[10] Ateniese, G., Burns, R.C., Curtmola, R., Herring, J., Kissner, L., Peterson, Z.N.J., Song, D.X.: Provable data possession at untrusted stores. In: Proceedings of the 14th ACM conference on computer and communications security (CCS'07), pp. 598–609. ACM (2007)

[11] Ateniese, G., Di Pietro, R., Mancini, L.V., Tsudik, G.: Scalable and efficient provable data possession. In: Proceedings of the 4th international conference on Security and privacy in communication networks (SecureComm'08), pp. 1–10. ACM (2008)

[12] Erway, C.C., Küpçü, A., Papamanthou, C., Tamassia, R.: Dynamic provable data possession. In: Proceedings of the 16th ACM conference on computer and communications security (CCS'09), pp. 213–222. ACM (2009)

[13] Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, "Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security", International Journal of Scientific and Engineering Research, vo. 4,no. 2, ISSN 2229-5518, Feb 2013.

[14] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," ACM Transaction on Computer Systems, vol. 20, no. 4, pp. 398–461, 2002.