International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

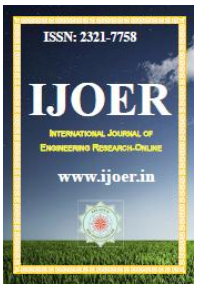
ISSN: 2321-7758

PROVIDING PRIVACY PRESERVATION FOR DATA SHARING OVER CLOUD USING ECIES

JAYANT KUMAR[1], NITIN AGARWAL[2]

[1]Department of Computer Science & Engineering, NRI Institute of Information Science & Technology, Bhopal, India

[2]Assistant Professor, Department of Computer Science & Engineering, NRI Institute of Information Science & Technology, Bhopal, India



ABSTRACT

Here in this paper a new and efficient technique for the Sharing of Data over Cloud Computing is proposed. The proposed Methodology implemented here is based on the concept of implementing Hard Logarithmic based Problem such as Elliptic Curves Cryptography. The Proposed Methodology Works in Two Phases : First Key generation using Hyper Elliptic Curve and Second by Encryption the Shared Data using these keys and Encrypted using Cipher Text Policy based Encryption. The Proposed Methodology provides Security from various Attacks and also reduces Computational Time and Cost as compared to the existing methodology.

Key Words—Cloud Computing, CP-ABE, ECIES, Public Auditing

INTRODUCTION

Nowadays, cloud computing has penetrated into every corner of Internet industry with its low-cost computing resources, easy scaling architectures, and everywhere on-demand services. Security issues is the most important issue faced by people in the use of cloud computing data storage services [1].The advantage of cloud is cost savings. The prime disadvantage is security. The security risks associated with each cloud delivery model vary and are dependent on a wide range of issues counting the understanding of data quality's, cloud architectures and safety measures organizes engaged in a exacting cloud atmosphere. With public audit capability, a trusted entity with expertise and capabilities data owners do not hold can be entrusted as an outside audit party to evaluate the possibility of outsourced information when required. Such an auditing examine not only facilitates accumulate data owners' calculation resources but also offers a visible however cost-effective technique for data owners to increase trust in the cloud. One of the most important anxiety in cloud computing is the opportunity of spread of confidentiality. As cloud computing is achieving enlarged attractiveness, anxiety is being right to be heard about the security concerns bring in all the way through the recognition of this new representation. The effectiveness and competence of usual security methods are individual think again, as the explanation of this creative exploitation representation, be unusual generally from them of straight designs. Numbers of methods have been proposed [2-3] to defend reliability of information. As well, they additional expand their method to sustain batch auditing, which can audit multiple shared data at the same time in a distinct auditing task. For now, Oruta maintains to utilize random masking [4] to support information privacy throughout public auditing and influence index hash

tables [5] to sustain entirely dynamic process on shared data. A dynamic process point outs an insert, delete or update operation on a distinct block in shared information.

Figure 1 Cloud Architecture

On cloud we can capable to store information as a group and distribute it or alter it within a group. In cloud data storage contains two entities as cloud customer i.e. group members and cloud service provider/ cloud server. Cloud consumer is a person who accumulates huge amount of information on cloud server which is deal with by the cloud service provider. Customer can upload their information on cloud and distribute it within a group. A cloud service provider will give examines to cloud consumer. The most important concern in cloud data storage is to acquire appropriateness and reliability of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of method through which customer will get the authentication that cloud data is protected or is accumulated as it is. No data loss or alteration is done by unauthenticated component. To accomplish safety measures data auditing idea is come into representation. This can be accomplished in two approaches as:

- Without trusted third party.
- With trusted third party based on who does the verification.

In cloud computing design data is stored centrally and supervision this centralized data and providing security to it is very complicated job. TPA is utilized in these circumstances and the consistency is enlarged as data is hold by TPA but data integrity is not accomplished. TPA uses encryption to encrypt the contents of the file. It confirms data integrity but there is threat of TPA itself escapes user's data. Researchers of [4] identify method to accomplish storage space accuracy without Trusted Third Party (TTP). They accomplish this by using secure key management, flexible access right supervisions and light weight reliability verification process for checking the un-authorized transform in the unique data without requesting a neighboring copy of the data.

Literature Survey

In this paper [6], here author has only think about how to audit the integrity of distributed data in the cloud with static groups. It denotes the group is pre-classified before shared data is generated in the cloud and the association of clients in the group is not transformed during data sharing. The original client is answerable for deciding who is proficient to distribute her information before outsourcing information to the cloud. Another exciting difficulty is how to review the integrity of distributed data in the cloud with self-motivated groups — a new client can be additional into the group and an accessible group member can be withdraw during information sharing — while still preserving distinctiveness confidentiality. When a client (either the original user or a group user) needs to ensure the reliability of mutual data, she first sends an auditing request to the TPA. After being paid the auditing request, the TPA produces an auditing message to the cloud server and get backs an auditing proof of mutual information from the cloud server. Then the TPA verifies the exactness of the auditing proof. As a final point, the TPA sends an auditing report to the client based on the effect of the confirmation.

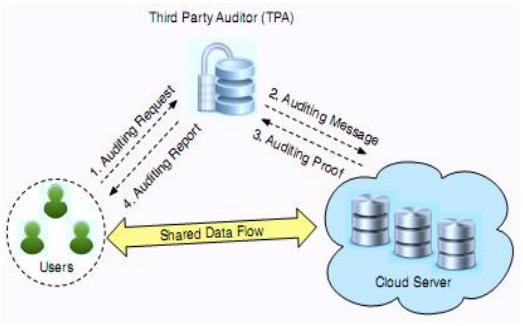


Figure 2: Architecture based on the cloud server, the third party auditor and users [6].

Wang et al. [7] designed a difficult auditing mechanism, so that for the duration of public auditing on cloud data, the content of private data be in the right placing to an individual client is not reveal to any public verifiers. Unfortunately, existing public auditing explanations talk about exceeding only focus on individual data in the cloud. They consider that sharing data among multiple clients is maybe one of the most attractive characteristics that inspire cloud storage. Consequently it is also essential to make sure the reliability of mutual data in the cloud is accurate. Existing public auditing methods can essentially be expanded to confirm shared data integrity.

In this paper [8], author has proposed a new privacy-preserving method is considered which supports public auditing on shared data stored in the cloud. In particular, aggregate signatures are utilized which calculates the verification metadata required to audit the exactness of distributed data. With this method, the distinctiveness of the owner who signs each data block in shared information is kept private from public verifiers. These public verifiers are proficient to efficiently confirm reliability of shared information without downloading the complete file. As well, this method can proficiently perform several auditing jobs at same time as an alternative of confirming them one by one.

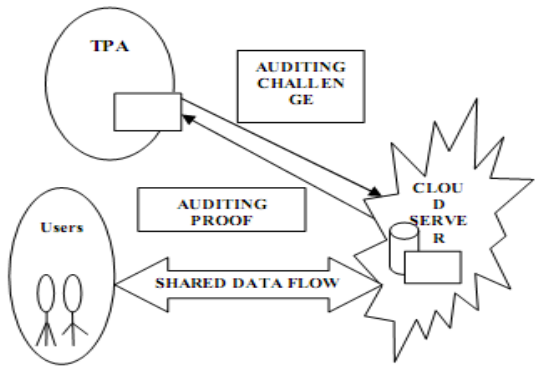


Figure 3: Group of users and a public verifier on cloud server [8].

By utilizing Aggregate Signature methods the verification and in that way privacy preservation of the data owner is being done and it is distinguish that the owner could efficiently upload the files and a client could download it using the key which is being sent to his/her mail. The performance and effectiveness of the work is evaluated.

In this paper [9], here they define and explain the difficult problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE).Here they create a set of exacting privacy conditions for such a protected cloud data utilization scheme. Among various multi-keyword semantics, they decide the proficient comparison evaluate of "coordinate matching", i.e., as many matches as feasible, to confine the significance of data documents to the search query. They additional utilize "inner product similarity" to quantitatively estimate such similarities calculate. They initial suggest a essential design for the MRSE based on protected inner produce calculation and then provide two extensively recovered MRSE methods to accomplish various strict privacy conditions in two different threat representations. Comprehensive study investigating confidentiality and effectiveness assurances of suggested methods is given. Experiments on the real-world dataset additional demonstrate proposed methods definitely initiate low transparency on calculation and communication.

Jiang Wang et al. put forward an Anonymity-based technique to accomplish and preserve privacy in cloud computing [10]. The anonymity algorithm procedures the data and anonymises all or some data before releasing it in the cloud conditions. When need the cloud service provider make utilize of the conditions information it has and includes the features with the anonymous data to mine the required knowledge? This technique is different from the conventional cryptography technology for preserving user's privacy as it acquires free of key management and thus it positions easy and elastic. While anonymising is easier, the characteristic that has to be made anonymous differ and it depends on the cloud service provider. This approach will be appropriate only for inadequate number of services. Thus, the technique has to be enhanced by computerized the anonymisation.

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.

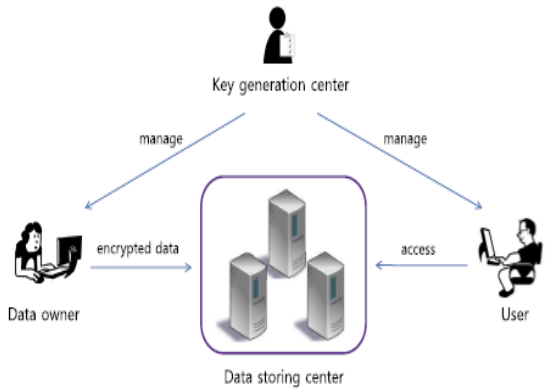


Figure 4: Cloud Data Storage & Sharing

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:

1. The sender generates an automated message and generates an identity string using message to be sending.
2. 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.
3. The owner when access the data needs to be authenticated at the storage panel using identity and password that is generated by the sender.
4. The owner after authenticates access the data based on identity and decrypts the message from the storage panel.

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.

Result Analysis

The table shown below is the attack prevention by the proposed methodology from various attacks in the cloud data storage.

Table 1 Privacy Preservation from various attacks

Attack Type	Security
Replay Attack	Yes
Identity Disclosure Attack	Yes
DOS attack	Yes
DDOS attack	Yes
Password Impersonation	Yes
Online dictionary	Yes
Offline dictionary	Yes

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 is thus omitted.

Table 2 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 3 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.

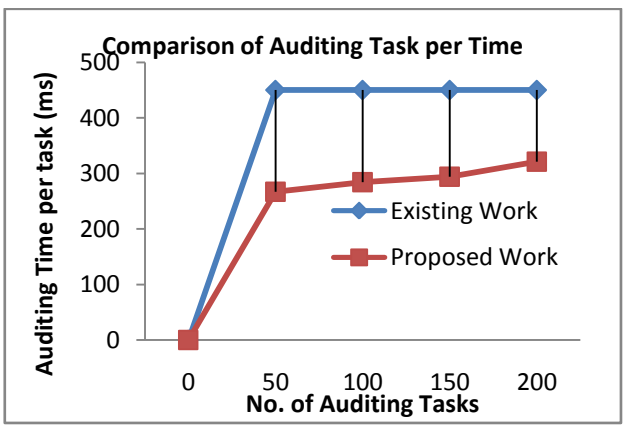


Figure 5 Comparison of Auditing Taks per Time in ms

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]. L.M. Kaufman, "Data Security in the World of Cloud Computing," IEEE Security & Privacy, July-Aug. 2009, pp.61-64.,

[2]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[3]. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.

[4]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[5]. Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[6]. Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE TRANSACTIONS, 2013.

[7]. John W. Rittinghouse James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, 2010.

[8]. Dr. J. Suganthi, Ananthi J, S. Archana, "Privacy Preservation And Public Auditing For Cloud Data Using Ass", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2014.

[9]. Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou, "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data" 2011.

[10]. Wang J, Zhao Y et al. Providing Privacy preserving in cloud computing, International Conference on Test and Measurement, vol 2, 213–216, 2009).