ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

An Identity Combined With Attribute Based Proxy Uploading and Integrity Checking in Public Cloud

Pallavi S. Kaulage[1], Prof. Dr. S. N. Kini[2]

ME Student, Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India.[1]

Asst. Professor, Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India[2]

ABSTRACT: The cloud-based outsourced stockpiling alleviates the customer's weight of capacity administration and uprightness protection by giving an identically versatile, modest, area autonomous stage. It permits the customers to check information wholeness and accuracy with no downloading the whole information on neighbourhood machine. From the security issues, we propose a novel Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking with Proxy re-encryption Scheme in Public Cloud. Intermediary re-encryption is a moderately recently formulated cryptographic primitive. The objective of intermediary re-encryption is to safely empower the re-encryption of cipher texts from OriginalClient in intermediary. That implies, in existing OriginalClient has enormous information to be transferred to PCS (Public Cloud Server) by the assigned intermediary. For security, he encodes his information in view of Identity Based Public Key then forward to the intermediary for transfer to PCS. Intermediary is approved to handle the OriginalClient's ciphertext and transfer them, is chosen and approved by OriginalClient. At the point when Proxy fulfils the warrant mω (that implies OriginalClient's ciphertext) which is marked and issued by OriginalClient, it can handle and transfer the first customer's ciphertext; else, it can't play out the strategy. This current procedure has just a single encryption in OriginalClient. So it has less security. An assailant might be hacks this information. So we extend the current way to deal with intermediary re-encryption Scheme. . We have improved role of proxy by assigning duties like ID based re-encryption, delegate uploading and delegate integrity checking. In this Scheme Proxy at the end of the day scramble that OriginalClient's ciphertext and afterward transfer to PCS.

KEYWORDS: Cloud Computing, ID –Based Encryption, Pseudonym, Attribute Based Encryption, Index Switcher.

I. Introduction

The distributed computing encourages numerous straight advantages to customers as on request benefit, area autonomy, versatility, organize based model, asset pooling et cetera. The distributed storage provisioning is one of the fundamental administrations of distributed computing. In the course of the most recent years, distributed computing fulfils the application necessities and becomes rapidly. Basically, it takes the information preparing as an administration, for example, stockpiling, processing, information security, and so forth.

By utilizing people in general cloud stage, the customers are soothed of the weight for capacity administration, widespread information access with autonomous geological areas, and so forth. Along these lines, increasingly customers might want to store and process their information by utilizing the remote distributed computing framework. Out in the open distributed computing, the customers store their gigantic information in the remote open cloud servers. Since the put away information is outside of the control of the customers, it involves the security chances regarding privacy, trustworthiness and accessibility of information and administration.

Remote information honesty checking is a primitive which can be utilized to persuade the cloud customers that their information is kept in place. In some exceptional cases, the information proprietor might be confined to get to people in general cloud server, the information proprietor will assign the undertaking of information preparing and transferring to the outsider, for instance the intermediary. On the opposite side, the remote information honesty checking convention must be proficient with a specific end goal to make it reasonable for limit constrained end

DOI: 10.15680/IJIRCCE.2017. 0506011

gadgets. Along these lines, in view of personality based open cryptography and intermediary open key cryptography; we will examine ID-PUIC convention.

Out in the open distributed computing, the customers store their monstrous information in the remote open cloud servers. Since the put away information is outside of the control of the customers, it involves the security chances regarding privacy, trustworthiness and accessibility of information and administration. Remote information uprightness checking is a primitive which can be utilized to persuade the cloud customers that their information is kept in place. In some exceptional cases, the information proprietor might be confined to get to the general population cloud server, the information proprietor will appoint the undertaking of information handling and transferring to the outsider, for instance the intermediary. On the opposite side, the remote information respectability checking convention must be proficient with a specific end goal to make it reasonable for limit constrained end gadgets. Existing System gives remote information uprightness checking yet there are security issues as just a single level of encryption is utilized. This spurred us to present Proxy re-encryption is another prefix in cryptographic thought that is presented in this venture subsequently giving two level of security. Therefore, in view of character based open cryptography and intermediary open key cryptography; we proposed ID-PUIC convention.

Cloud computing is an important technology that frees users from document / data management issues and allows them to control and access their data remotely via a connection. But it is not always possible for data owner to be present physically to upload the document thus proxy uploading was implemented that allows data owner to delegate their operation of uploading to their proxy. Existing ID-PUIC convention is likewise effective and adaptable. In view of the first customer's approval, the proposed ID-PUIC convention can understand private remote information uprightness checking, appointed remote information respectability checking and open remote information honesty checking. It has less security. Since just a single encryption (in view of id based open key) is created in OriginalClient. So Attacker can without much of a stretch hack his outsourced information. If attacker knows the information proprietor personality, he can unscramble the transferred record in light of character based decoding. Hence an improvement over following issues is needed to deal with such disadvantage.

The fundamental commitments of the proposed arrangement are:

1) Information driven arrangement with information assurance for the Cloud Service Provider to be notable get to
2) Apply Pseudonym Base Encryption (PEB) for greater security.
3) Security issues using symmetric encryption hence level of security provided will be same but computational complexity involved will be less.
4) Privacy issue by using Pseudonym instead of email-id as ID here Pseudonym will hide private information from directly exposing to outside world.

Apply index switcher structure to support data dynamics on cloud efficiently.

II. RELATED WORK

Garima and Naveen [1], "Triple Security of Data in Cloud Computing", proposed a framework for upgrading security in cloud by applying three calculations specifically: DSA (Digital Signature Algorithm), AES (Advanced Encryption Standard) and Steganography. For information encryption, DSA is accomplished for validation took after by AES for encryption lastly connected Steganography for disguising information inside sound document to have most extreme security. By applying the calculations in the turnaround request the beneficiary can unscramble the information however the issues found here is high many-sided quality in time since the calculations are connected in a steady progression.

In Cong Wang and Kui Ren [2] Privacy-Preserving Public Auditing for Secure Cloud Storage has for the most part a spotlight on outsider inspector (TPA) to perform reviews for various clients simultaneously and effectively. Thus to accomplish most extreme security the outsider examiner ought not to convey any extra weakness to the framework or additional weight for clients. The execution investigation of the proposed plans demonstrated that they are exceptionally secure and productive. The sharing of distributed computing assets like stockpiling, administrations and applications with different occupants is extremely hazardous as they coincidentally get different inhabitants data. Multi tenancies are considered as an imperative element in distributed computing asset use. Consequently Mohamed Al

Xuefeng Liu and Yuqing Zhang [3] have proposed a framework for element amasses in the cloud called Mona, a safe multi proprietor information sharing plan. Any client in the cloud can impart their information namelessly to others by utilizing bunch signature and element communicate encryption procedures. The calculation cost for encryption and the capacity overhead are autonomous with the quantity of disavowed clients.

Singla and Jasmeet [4], "Cloud information security utilizing verification and encryption system", It proposes the blend of two distinct calculations Extensible Authentication Protocol (EAP) - Challenge-Handshake Authentication Protocol (CHAP) and Rijndael Encryption Algorithm for empowering high security. The previous calculation is connected for verification reason and the later for information encryption. Rijndael Encryption Algorithm makes the framework more secure. In this paper Client side security has been concentrated for accomplishing high information security.

As per Neha Garg et al., [5] has examined about giving a safe Multi-tenure in the distributed computing that requires separation among client's information. In distributed computing information are put away in various nations that face different controls and legitimate frameworks. Securing of clients information is the basic figure distributed computing in light of the fact that the sharing of distributed computing assets may offer emerge to unapproved get to.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- Before requesting for Private Key owner must have generated Pseudonym.
- Pseudonym Generated is always of fixed length and has no connection with name / identity of user who generates it.
- Pseudonym is the identity of user for CSP and PKG both.
- Attributes used to decide the access policies.
- Attributes will be used to decide who can decrypt the Document.
- Decrypt the document only if access policy is satisfied with set of user attributes.

B. *Description of the Proposed Algorithm:*

Pseudonym Generation algorithm

```
Input: Character Set
Output:  p_nym i.e. Pseudonym for user U on identity I

 1) Character Set is given as initial input.
2) Then pseudo generation algorithm is applied on the identity I.
3) Initialize p_nym
4) Initialize pseudo random list
5) Initialize length = 10
for (int i=0;i<10;i++ )
{
P_ynm=P_nym+Charat(random_index);
}
6) Pseudonym is generated from step 5.
7) Output of step 6 is P_ nym
8) Return P_nym
```

Extract:
In this Algorithm first we create the 4 substances, to be specific OriginalClient, PCS (Public Cloud Server), Proxy and KGC (Key Generation Centre). In this module, when the OriginalClient's pseudonym is information; KGC produces the OriginalClient's private key. Particularly, it can create the private keys for the customer and the intermediary.

Attribute based Encryption by Owner:
Original Client encrypt data on basis of pseudonym and attributes set A= {a1, a2, …, an} appended along with the data D the transfer data to proxy for further ID based re-encryption and uploading.

Proxy-key generation:
In this stage, the first customer makes the warrant and helps the intermediary produce the intermediary key. Intermediary is approved to handle the OriginalClient's information and transfer them, is chosen and approved by OriginalClient. At the point when Proxy fulfils the warrant $m\omega$ which is marked and issued by OriginalClient, it can prepare and transfer the first customer's information; else, it can't play out the strategy.

Re-encryption & TagGen & index switcher:
In this stage, when the encoded information square is information (originating from unique client).The intermediary re-scrambles this encoded information pieces and creates the re-encoded piece's tag. Then transfer re-encoded piece label sets to PCS. An index switcher is a table used to keep a mapping between piece files and tag files.

IV. Pseudo code

```
Step 1: Generate the Pseudonym and Keys.
Step 2:  Encrypt Document using Pseudonym + Attributes (ABE).
Step 3: Download encrypted Document.
Step 3:  Check the below condition for status if access policy is satisfied or not.
              if (AP  = User_attributes)
                      Decrypt the document.
              else
                    Do not decrypt the document.
              end
Step 4: End.
```

V. Simulation Results

Our proposed system solves the problem of security of documents while uploading implementing a secure and efficient access control mechanism across cloud platform with N users. For performance measure we compare the computational overhead that is incorporated in implementing secure ID based encryption. Computational overhead is involved in process of ID based encryption which is measured in terms of time cost required to generate encrypted data for document D uploaded by N users. As input length ID increases the time required for encrypted data for document D also increases thus increasing time required for uploading and downloading process.

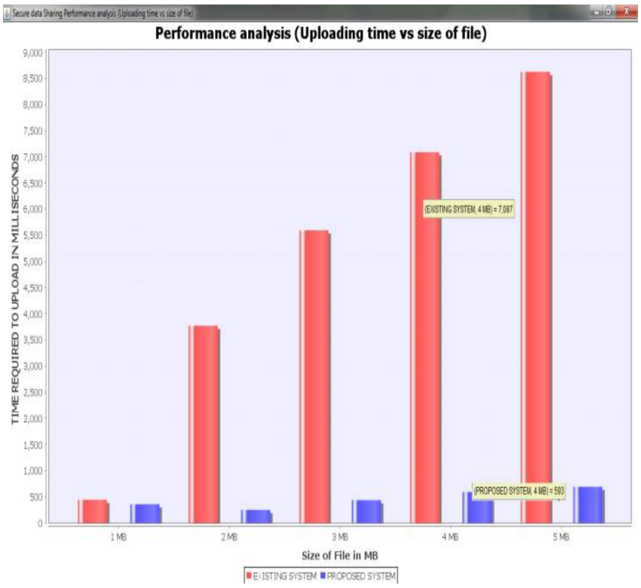

Figure 1. Performance comparison uploads Time

Figure 1 shows the execution time of existing and proposed methods. The proposed method is ID+ ABE which is used to handle big data and it works parallel in nature ad ID we are using Pseudonym which is of fixed length so that the upload time required to execute is very less than the time required to execute existing system. We have computed time by subtracting start time from end time for 5 separate file size ranging from 1 MB to 5MB.

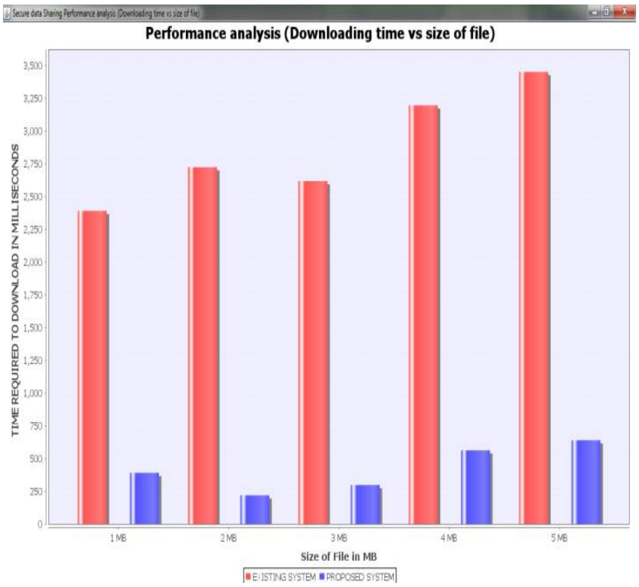

Figure 2 Performance comparison Download Time

Figure 2 shows the execution time of existing and proposed methods. The proposed method is ID+ ABE which is used to handle big data and it works parallel in nature ad ID we are using Pseudonym which is of fixed length so that the download time required to execute is very less than the time required to execute existing system. We have computed time by subtracting start time from end time for 5 separate file size ranging from 1 MB to 5MB.

DOI: 10.15680/IJIRCCE.2017. 0506011

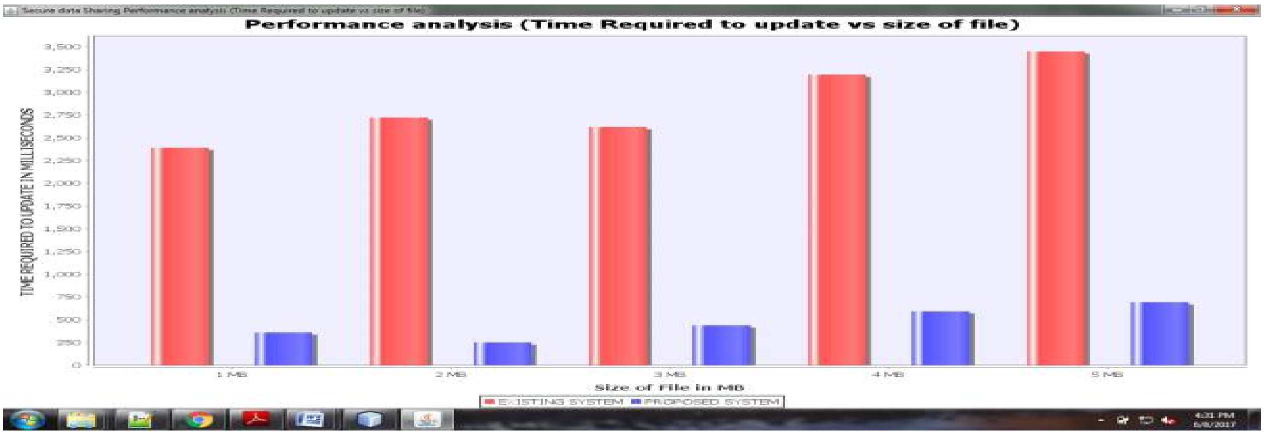

Figure 3. Update time vs File Size

Figure 3 show time computations for update operation vs. Original file size for example original file size is 1MB vs encrypted size which is to be uploaded. In figure 9.3 it is clear that using ID+ABE has reduced computational burden on update operation where proposed tend to update only added blocks and no tag re-computation is done hence is fast where as in existing system tag re-computation is occurred hence takes lot of time to update the data on cloud.

VI. Conclusion and Future Work

The proposed in this paper we have made attempt to combine ID-ABE based encryption together to extract advantages of both schemes. ID based scheme frees us from certificate management issues and further ABE based scheme allows data owner to flexibly decide attributes to documents which eases the access control system and provide another layer of security to our scheme Further ID based scheme are open for attack based on identity as scheme uses common identity as public key like emailed which can be easily mapped to a user revealing privacy of user. To overcome this we use Pseudonym of user as his identity. Pseudonym is generated using simple Pseudonym generation Algorithm which protects user's identity from being directly exposed. We have improved role of proxy by assigning duties like ID based re-encryption, delegate uploading and also this support to data dynamic operation on cloud.

We will moreover consider gathering adopter sees into more fine-grained measurement characterizations and research other probabilistic techniques for thing recommendation. In future we would consider same experiment on multi-cloud environment.

References

1. Saini, Garima and Naveen Sharma, "Triple Security of Data in Cloud Computing", International Journal of Computer Science & Information Technologies, Vol. 5(4), 5825-5827, 2014.
2. 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, vol. 62, no. 2, 2013.
3. Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”, IEEE Transactions on Parallel and Distributed System, vol. 24, no. 6, 2013.
4. Singla and Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", Global Journal of Computer Science and Technology, Volume 2, Issue 7, July 2013.
5. Thapliyal, Meenakshi, Hardwari Lal Mandoria, and Neha Garg, "Data Security Analysis in Cloud Environment: A Review", International Journal of Innovations & Advancement in Computer Science, vol. 2, no. 1, 2014.

BIOGRAPHY

Miss Pallavi Sudhir Kaulage is currently pursuing M.E. (Computer Engineering), Jaywantrao Sawant College of engineering, Pune, Maharashtra, India – 411028. She received her B.E. (Computer and science) Degree from SVERI College of engineering, Pandharpur, Maharashtra, India-413304. Her area of interest is cloud computing, network security.