A SECURE LOCKBOX TECHNIQUE FOR ENHANCED SHARED SHARING FOR USERS INFORMATION PACKETS ACCESS CONTROL IN CLOUD COMPUTING

ER. RAHUL PANTH
Department of Computer Science & Engineering
Lakshmi Narain College of Technology, Bhopal, India

PROF. SHWETA SHRIVASTAVA
Department of Computer Science & Engineering
Lakshmi Narain College of Technology, Bhopal, India

DR.VINEET RICCHARIYA
Department of Computer Science & Engineering
Lakshmi Narain College of Technology, Bhopal, India

ABSTRACT

Cloud computing [12] and its security with user's multi-label data is provided security by different module by different author. The security in terms which provided either encryption or in terms of hashing which aims to provide integrity verification. In this paper a lock box technique which aims to provide a highly secure mechanism for data sharing and its authenticity maintain is proposed. That technique uses proxy re-encryption and lazy encryption technique to provide an enhanced encrypted. That technique leads in data processing using data hiding and key sharing among the given selected user. The result were monitored in terms of computation time at server end and also security measures which claims the high level of security is provided in the proposed work. Our work is deems to be an innovative work with cloud security and its architecture.

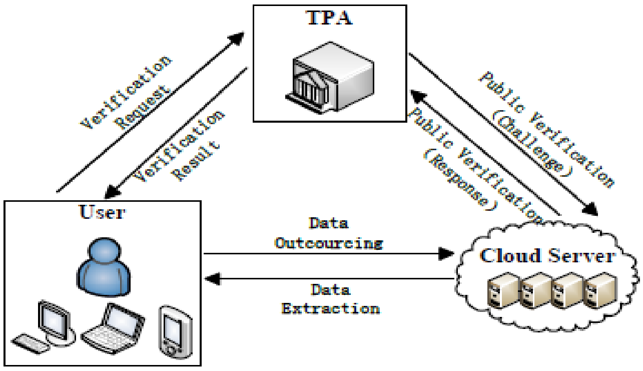
KEYWORDS: lazy encryption**,** proxy re-encryption, Attribute-Based Encryption**.**

INTRODUCTION

The Cloud computing [12] has become the collective model for grouping the different technologies which are collaborated to provide the services on Demand. Cloud computing is a model for enabling convenient and on demand accessing of the resources. This model of Cloud computing offers a shared pool of resources that are available on customer`s demand and it can accessed at anytime from anywhere. The collaboration of technologies all his schemed most talked and popular term to Cloud computing in recent times. Most of the organizations have been shifted to the Cloud computing and had a great impact on their services and efficiency. Thus the growth of the IT technologies with Cloud computing has reached to the customer in an efficient manner. As Cloud computing offers a package of services that enables a whole new way of using IT and accessed on demand. So it is a great feel to using the packaged technologies in a better way and using them from anywhere in the world.

There are various security [13] problem for Cloud computing as it encompasses many technologies including networks, Cloud users information packets bases, operating systems, virtualization, resource scheduling, transaction management, Load balancing, concurrency control and memory management. Accordingly, security problem for many of these systems and technologies are applicable to Cloud computing. The network system in Cloud computing has to be assured. Furthermore, virtualization paradigm in Cloud Computing results in several security burdens. The Cloud computing scenario proposed the three tier work & it taken TPA [14] (third party authenticator), CSP [12] (Cloud computing service provider), Cloud users& here it is the architecture proposed in this way. In this system Client may be individuals or organizations. CS is usually managed by CSP, and it has a huge storage devices and computing resources. It can also provide availability and shared services such as share Cloud users information packets on CS to an authorized visitor, beyond the Cloud users information packets storage services.

TPA [14] is used to perform Cloud user's information packets authentication and auditing tasks on behalf of the client. When doing this, the client needn't to do the auditing tasks itself, which is very important to reduce the costs of Cloud computing. What's more, the TPA [14] has the expertise and capability which a Client usually has not. So client can trust the evaluation of Cloud computing storage service and warning against security threats provided by TPA [14].Client wants to enjoy the service provided by TPA [14], but don't want their privacy Cloud users information packets leaked to TPA. By using the combination of public certification, Homomorphic certification and random conceal program, TPA [14] can audit and verify the Cloud users information packets stored in the Cloud computing without a local backup.



This system allot his schemed the client to initialize their privacy parameters and transmit the certification and Meta Cloud users information packets to TPA in the initial set-up phase and then the TPA verifies the validity of proof value generated by the server. Above all, this approach can protect the integrity and confidentiality of Cloud user's information packets in the Cloud computing server.

LITERATURE REVIEW

GENETIC ALGORITHM BASED SYMMETRIC KEY CRYPTOSYSTEM [9]

In this paper author proposed a genetic algorithm based symmetric key cryptosystem for encryption and decryption , here the plain text and the user input is converted into text matrix and key matrix respectively . An additive matrix is generated by adding the text matrix and key matrix. A linear substitution function is applied on an additive matrix to produce the intermediate cipher. Then the GA functions (crossover and mutation) are applied on the intermediate cipher to produce the final cipher text. Genetic algorithm is secure since it does not utilize the natural numbers directly. In this paper author use two point crossover techniques and flipping of bits mutation technique. Author stated that symmetric key substitution algorithm is used to ensure confidentiality in networks which is combined and implemented with the help of genetic algorithm function to provide added security.

SECURITY MODEL IN CLOUD COMPUTING [2]

In this paper author proposed an efficient security model in cloud computing environment with the help of soft computing techniques. Here a strong security in cloud computing is managed with the help of reputation management system to ensure the data security. Also maintaining the transaction table that contains the info. Related to the previous transaction like the previous transaction ID of the cloud node involved, timestamp, public keys of the cloud involved, trust evaluation etc. Can be very helpful to identify the relevant cloud nodes suitable of data transmission. In this method author utilized genetic algorithm as the computing technique to identify the suitable nodes for transmission that proved to be effective method in cloud computing environment and provide security to the cloud system.

NON-LINEAR FEEDBACK SHIFT REGISTER [8]

In this paper author proposed that a new approach for encrypting real time data transmission first generate pseudorandom sequence using non-linear feedback shift register(NLFSR). NLFSR is a mechanism for generating extremely well pseudorandom binary sequence this total way of transferring secret information is highly safe &reliable. So without the knowledge of the pseudorandom sequence no one will be able to extract the message. Since NLFFSR pseudorandom binary sequence is unpredictable it is very difficult to decrypt correctly an encrypted signal by making an exhaustive search without knowing the initial value and the feedback function f and nonlinear output function g of the NLFFSR. The simulation result of the proposed work indicated that the encryption results are completely chaotic by the sense of sight and very sensitive to the parameter fluctuation. Security issues-while dealing with the cloud security we have various issues associated with the cloud data

PROBLEM FORMULATION

In order to deal with the cloud and services there are various challenges and problem formulation come across which required resolving to get solution for exact architecture in cloud computing. the challenges related to use a proper data security technique , data sharing model by exchanging data key and further using for upload and download data transmission, also integrity verification over the existing users data impact major challenges observed in recent scenario.

PROPOSED SOLUTION

In order to solve the cloud issues and challenges the further work is performed by us and a lock box technique for the key sharing among the available users and users uploaded data is being performed. The lock box technique work at the user end and the other sharing end where a hidden key sharing module is implemented by our proposed method.

Jelastic Cloud is used to perform the related lockbox technique which provides a decentralized access and wide area of functionalities. Jelastic is a cloud PaaS and CaaS for hosting providers, ISVs, DevOps and enterprises. It can be used for Public, Private, Hybrid and Multi-Cloud deployments. Jelastic is an unlimited PaaS and Container based IaaS within a single platform that provides high availability of applications, automatic vertical and horizontal scaling via containerization to software.

Our proposed work aims to provide a high security combination approach while dealing with the cloud security approach, as the general method either work with the security encryption or hashing data verification technique. Thus our proposed work implied which work on both the area as an algorithm where the data hash value is calculated at the time of implementing encryption and data storage performance into the cloud data center.

Further the SHA2 hash code is used to generate as challenge from the TPA side and then a response form generation from the cloud side. Thus the data verification process works with the help of hashing technique SHA-2 function.

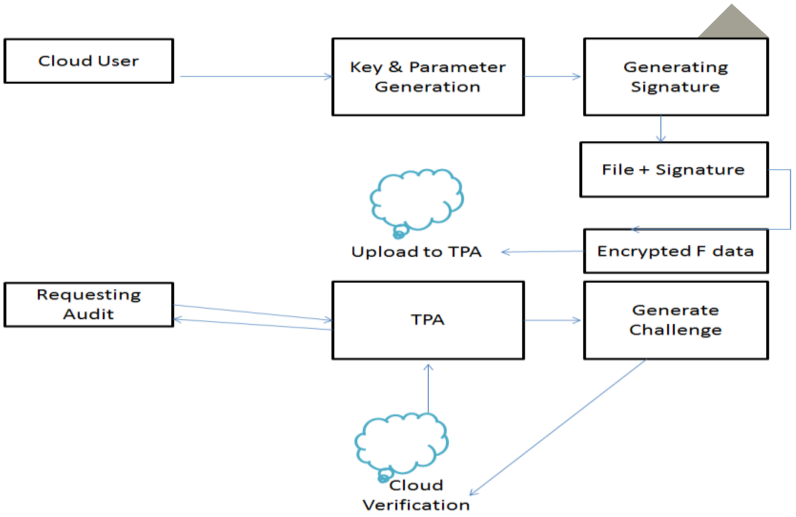


Figure1: Overview of complete Working Architecture of Proposed algorithm.

ALGORITHM

TABLE I
NOTATIONS

Symbols	Meaning
$S_k.$	K-th Session Key
f_s	S-th File to Share
l_k	K-th Lock Box Key
U_u	U-th User/Owner

USER LOGIN

1. Create an account in cloud server, if exist login.
2. Generate session key (S_k) for the user.
   If valid user than OTP (S_k is generated) is generated.
3. At the time of data uploading this OTP is required.
4. If S_k (enter by the user) = = S_k(original)
   than data is encrypted by AES encryption
   and uploaded in server.
5. Stop process.

START FILE SHARING USING LOCKBOX TECHNIQUE:

```
1. Verify user U session key ($S_k$).
2. Select file.
   For each file as $f_s$ (selected file by the user)
3. Select user.
   For each user as $U_u$.
4. Generate key $l_k$ for the user using Lockbox technique.
5. Share file.
```

ACCESSING SHARED FILE

```
1. Verify session key.
   $S_k$(Entered by the user) == $S_k$ (original)
2. Apply Lockbox to authenticate user for providing access of the shared file.
   (a) If user U enters the correct $l_k$.
   Provide access to the selected file $f_s$.
   (b) Else update login failure.
3. If login failure is more than threshold value
   then re-encryption perform using session key $S_k$.
4. Again login operation is performing.
5. End
```

RESULT ANALYSIS

In order to perform the proposed technique we use Jelastic Cloud Environment and thus used EVERDATA public cloud services. In this we used the Everdata cloud resources such as creating a fresh environment to upload the project .war files, also create a MySQL data node and configure the database services and hence deploy the project. This configuration is created with 4 GB RAM, 1 TB Hard disk, And i3 Intel core processor with 8 GB Ethernet connection to provide a stable connectivity and further using static IP the multiple clients were connected and communication performed. Upon performing this technique the following result were computed with file uploading time, file verification time, lockbox creation time and Encryption time .

5.1 COMPARISON OVER ENCRYPTION TIME

A statistical and graphical comparison of the existing and proposed technique is presented in this section. Table 5.1, shows statistical comparison of the existing and proposed technique. That shows proposed technique provides efficient results as compare to the existing technique.

Table 2.1: Comparison of Encryption time.

File size	Proposed technique	Existing technique
403 kb	8	15
68830kb	10	20
81934kb	13	28

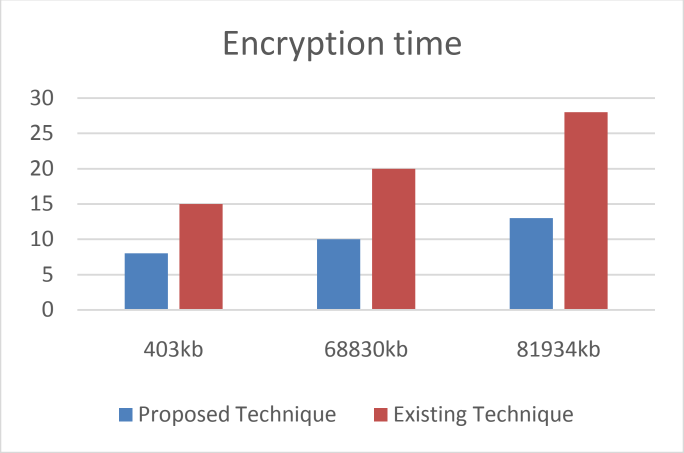


Figure 2.1: Graphical comparison over Encryption time.

A graphical comparison of the existing and proposed technique over time is presented in Figure 5.1. That shows proposed technique provides efficient mechanism to encrypt files.

5.2 COMPARISON OVER UPLOADING TIME

A statistical comparison of uploading time of existing and proposed technique is presented in this section. That comparative analysis shows, proposed technique provides better results as compare to the existing technique

Table 2.2: Comparison of Uploading Time.

File Size	Proposed Technique	Existing Technique
403kb	55	66
68830kb	59	71
81934kb	94	109

.

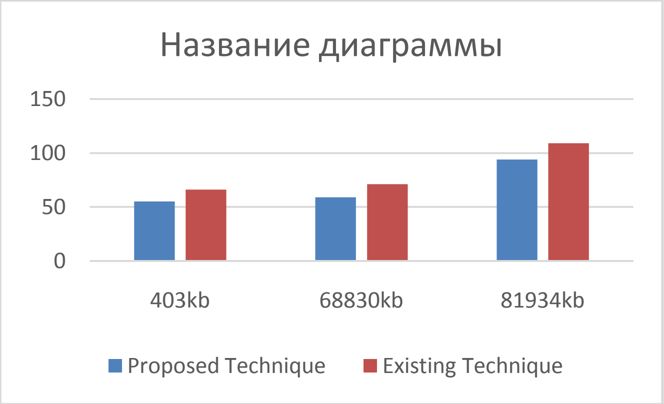


Figure 2.2: Graphical comparison over uploading time.

A graphical comparison of the existing and proposed technique over uploading time is presented in Figure 2.2. That shows proposed technique provide efficient mechanism to upload files.

5.3 LOCKBOX SECURITY

Lockbox technique provides enhanced secured sharing of files for the cloud users and also provides high level of security mechanism to access those files.

In Lockbox technique we generate an OTP (One Time Session Key) which is only generated at the time of successful logged in of user. All the files which to be uploaded for sharing is done when we provide the correct one time session key this will added a new security mechanism to the lockbox technique. This will help to verify that only authorized users to share those files over cloud.

A lockbox is a group of privileges for a single or a group of users to access a single or a group of files uploaded for the cloud users. Whenever a file is uploaded with correct session key, a unique lockbox ID is generated which is associated with a group of users and files, the privileges to access those files is provided by the user of that uploaded file. The users who want to access the lockbox having valid pair of public & private key pairs which is authenticated by cloud in real time scenario.

When a user want to access a lockbox it must first authenticated from the cloud having correct credentials and is able to access the dashboard after that user can access the lockbox which is shared to him, so lockbox is a secured way to share and access the files over cloud.

CONCLUSION

The Cloud technique using the different available scenario and available paradigm were presented in the system configuration. This paper presents an innovative approach and also the previous algorithm drawback of providing low security and low level architecture. The algorithm proposed by us is lock box approach. Where a data sharing and privileges sharing approach is presented. The proposed work proved as best in its field and further work can be done using high level encryption technique with real time scenario. A comparative analysis over time for the existing and proposed technique is presented result analysis section. That shows proposed technique provides an efficient mechanism to upload files in the cloud storage.

REFERENCES

1) Awsnaserjabber, Mohammadfadli bin zolkipli"*use of cryptography in cloud computing" 2013.*

2) Vijay .g.r, a. Rama Mohanreddy"*an efficient security model in cloud computing based on soft computing techniques"2012.*

3) Sashankdada"a new technique of data integrity for analysis of the cloud computing security" 2013.

4) M. Sugumaran, balamurugan. , D. Kamalraj, "*an architecture for data security in cloud computing" 2014.*

5) Lianfu yin“*the analysis of critical technology on cloud storage security” 2014*.

6) Pranita p. Khairnar, vs.Ubale“*cloud computing security issues and challenge” 2013.*

7) Tonydurgadasjagyasi,“*cloud computing using encryption and intrusion detection” 2013,.*

8) Abdel Salamalmarimi, anilKumar, Ibrahimalmerhag, nasreddinelzoghbi“*a new approach for data encryption using genetic algorithms” 2014.*

9) Sindhuja k, pramelaDevi s,“*a symmetric key encryption technique using genetic algorithm key” international journal of computer science and information technologies, vol. 5 (1), 2014.*

10) Cloud Security Alliance, *“Top Threats to Cloud Computing,”* http://www. Cloud *security alliance.org, 2010.*

11) Rachna Arora,AnshuParashar,” *Secure User Data in Cloud Computing Using Encryption Algorithms”, IJERA Vol. 3, Issue 4, Jul-Aug 2013.*

12) *http://searchcloudcomputing.techtarget.com/definition/cloud-computing.*

13) *https://cloudsecurityalliance.org/.*

14) Miss. Nupoor M. Yawale, Prof. V. B. Gadichha “*Third Party Auditing (TPA) for Data Storage Security in Cloud with RC5 Algorithm” IJARCSSE, 20103.*