A Systematic Framework for Providing Secured Transaction of Data in Cloud Computing Environment

[1]S. Annapoorani, [2]Dr. B. Srinivasan
[1]Assistant Professor, [2]Associate Professor,
Gobi Arts & Science College, Gobichettipalayam

Abstract **- Cloud data security is concern for the client when employing the cloud services supplied by the service provider in cloud. A framework called Conditional Source Encryption based Data Transactional Security (CSEDTS) is developed in cloud environment. Initially, the request is sent from the clients and conditional attributes are needed to be evaluated for securing the clients data requirement. The conditional attributes are evaluated through client requests. The transaction request sent to cloud data storage is examined as conditional attributes. The obtained conditional attributes are encrypted by Conditional Source Encryption method. Then, mapping function is applied for conditional attributes by using unique secured identity number and then these conditional attributes gets decrypted. Experiments are conducted and the performance analysis shows that the transactional security rate on data layer and the true positive rate are improved. This technique increases security of data that can be applied to access a wide range of resources and applications through web service interface.**

Keywords **- Conditional Attribute, CSEDTS framework, Decryption, Encryption, Mapping process, Secure Data Transaction, Security.**

I. INTRODUCTION

Cloud computing is a promising technology in the field of Information Technology. Cloud Computing is the computing resources (hardware and software) which are employ of delivered as a service over an Internet. Since the cloud permits the users to store their huge volume of data into the cloud, the user's burden of maintaining the data in the local machines has been decreased. For accessing the data in the Cloud storage, Cloud users require necessary security for protecting the data. The security issues on cloud are increased with respect to privacy, integrity, availability etc. It provides unusual and challenging threats to security for the data being outsourced. It also brings new and challenging security threats to the outsourced data. Since the data outsourced to cloud are maintained by cloud service providers, the data owners control over the data is ultimately dropped out. Because of its multitenancy feature, outsourcing of private data, demanding applications and infrastructure on to the cloud, more security and privacy issues has been raised in cloud computing. Also, the companies are having strict constraints on outsourcing their private data and demanding applications on public clouds.

Even though cloud computing provides on demand accessing of computing resources, the lack of security forms a major issue. The wide spread usage of cloud computing resources will be limited unless the

cloud users begin to entirely trust the cloud providers. The legal and technical facets increase the issue of cloud security. Since, the cloud infrastructure groups the various different services and software developed by various development teams without sharing approach forms a major challenge in ensuring cloud security.

Data becomes a great concern when it is outsourced to cloud. Hence, the most active domain of research in cloud computing is concentrating on the security and privacy of cloud data. Preventing the leakage of data and protecting the sensitive data becomes essential for most of the companies moving on to cloud.

II. RELATED WORKS

In cloud computing, security is essential for protecting data in the cloud storage. Today, this new technology has received great attention by researchers and organizations. The Remote Data Auditing (RDA) method is introduced to provide remote data storage in single cloud server domain with aim of improving the retrievable rate. Cloud data transaction was performed in a capable manner by different users at various access levels, but it fails to provide optimal security framework. Stackable Secure Storage System (Shield) with the objective of improving security using Merkle Hash Tree without the need of modifying the file system. However, the cloud data storage technique in Shield has not concentrated on maximizing the security on performing the transactions over cloud servers. Therefore, both above methods mentioned have lack of security.

Multiple data owners are considered in which the entire system is divided into numerous domains. The data is encrypted using AES technique and for the purpose of broadcasting, the AES key is encrypted using Attribute Based Broadcast

Encryption (ABBE) technique which uses the limitless size on attributes. But it creates complexity in providing immediate revocation in case of multiple authorities being online. An architecture based on cloud computing is used to secure the data and retain the sensitive information regarding the location of user data. The information identified using Global Positioning System (GPS). The limitation of this technique is that it works only in GPS enabled systems.

Cloud computing has evolved as most significant pattern for the design and analysis of virtual environment over Internet. In an efficient resource allocation scheme was designed with basic quality of service using win-win effect and incentive compatibility obtained. Optimization of cloud task processing was developed to improve the execution performance through composite cloud service system. Grid computing was designed to reduce the overall completion time. This in turn improves transaction time over the three methods. To improve data storage and security in cloud, an efficient data storage auditing mechanism was introduced. However, higher level of security was not guaranteed.

The privacy preserving public auditing mechanism were presented for data storage protection using Advanced Encryption Standards (AES) encryption algorithm in cloud computing. Though the computational time is improved, but the privacy is not high. In this work, a systematic framework called Conditional Source Encryption based Data Transactional Security (CSEDTS) is designed to ensure transactional security on performing the transactions over cloud servers.

The paper is organized as describes our CSEDTS framework, explains the experimental results and evaluates the performance of CSEDTS model by simulation.

III. SECURE DATA TRANSACTION

The detailed structure of Conditional Source Encryption based Data Transactional Security (CSEDTS) framework is constructed. The framework provides high secure transactions across different conditional attributes. Figure 1 shows data transactional security mechanism in cloud.

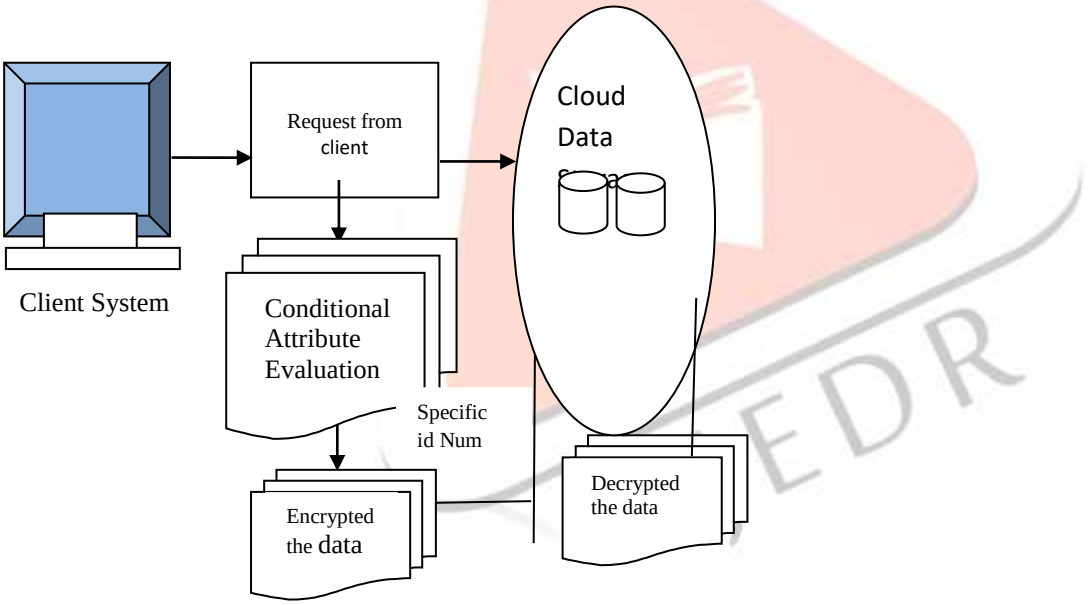


Figure 1. Architecture diagram of CSE-CDTS framework.

The client sends requests to the cloud data storage system for the purpose of transactional processing. The proposed framework is concentrated on encrypting the conditional attribute from the source root systems, to improve the security level measure. The client system sent request to cloud data storage for transactional processing. At first, the conditional attribute is evaluated by Bilinear Mapping Transformation function. Bilinear function performs one to one mapping to improve the transaction processing security. Finally, the conditional requests are updated to the decrypted conditional attribute from cloud data storage using CSEDTS framework. The concept used in CSEDTS framework increases the stochastic nature of the particle and attain maximum result with better solution.

Conditional Attribute Encryption

The first step involved is the design of Conditional Source Encryption based Data Transactional Security (CSEDTS) framework for performing cloud data transactions. The data requested from the client is evaluated as conditional attributes. The attributes are evaluated as,

(1)

CA={Attribute,Transaction(Attribute),D}->S

From equation (1), the conditional attribute evaluation is obtained by selecting the variables attributes 'A' and request to the attributes to be transacted through '*T'* on the total data storage in cloud 'D', '*S*' is the syntactic generator to the request query from the client side.

The client initiates the transaction request *T* through the cloud applications. The transaction request performed with conditional attributes to be encrypted for high secure transactional requirement. The conditional attribute information is encoded on the data layer using the bilinear mapping transformation. The data layers are transformed into a set of encrypted request from the clients used to improve the security with cipher type of message request. Then, client and server accept the request message used for transaction processing. The mapping function preserves the separate attributes from the clients to perform high effective transactions.

The algorithm for conditional attribute encryption with cipher specific id is as follows:

Algorithm 1: Conditional attribute encryption

Input:Plain Text
Output: Encrpted Data
Begin
Step 1: Divide the plain text into number of blocks and then change into binary form
Step 2: Evaluate conditional attribute splitting as CA_1+CA_2.
Step 3: Generate cipher id using

$$G=\frac{CA1S+c1}{CA2S+c2}$$

G is the cipher specific id generation.'c1' and 'c2' are the constants while generating the Id and 'S' is the syntactic combined with conditional attributes 'CA_1 ' and 'CA_2'
Step 4: Generate specific key id generation based on cipher text using set Key () function.
Step 5: Converted cipher text and Specific id is sent to cloud storage server.
Step 6: Repeat step 1 to 5 for entire request from client systems.
End

Mapping Process for Transaction Processing

The mapping function designed for improving transaction efficiency. It is used to perform the mapping process for transaction processing security in CSEDTS frame work.

Algorithm 2: Hash Function Mapping

Input:
Specific key id's: k1, k2, …. kn and Cipher text
Output: Mapping of data into corresponding users in Cloud.
Begin
Step 1: For all client requests
Step 2: CSP get specific key id's obtained from Transformation Encrption Algorithm
Step 3: CSP allocate data location for the corresponding data users.
Step 4: Pre-stored keys are generated for the data user location id to perform mapping process
Step 5: Pre-stored keys are mapped to the Specific Key id's for providing data to the user
End

Conditional Attributes Decryption

Finally, the conditional attribute decryption is significantly performed in the design of CSEDTS framework. In the server side, the conditional attribute is decrypted in order to provide transaction time for whole transaction process in CSEDTS framework. The decryption procedure on the cloud server side is employed to obtain the The decryption procedure on the cloud server side is formalized as given below,

Algorithm 2: Conditional Attribute Decryption

Input: Ciper Text
Output: Original Data
Begin
Step 1: Convert cipher message into decimal factor
Step 2: Find mapping transformation by using

$$M=\frac{C1-GC2}{GCA2-CA1}$$

'CA1' and 'CA2' represents the conditional attributes for original specific id using two constants 'C_1' and 'C_2' with

'G' representing the cipher specific id.

Step 3: Original Specific id makes the original request message from the binary form.
Step 4: Now, the binary form is changed to text form.
Step 5: Repeat the step 1 to 3 for the entire specific request id.
End

IV. EXPERIMENTAL EVALUATION

The Conditional Source Encryption based Data Transactional Security framework uses the CloudSim simulator to work under the simulation environment. The experimental work is carried out for evaluating the security level on the transactions between different cloud environments. With the simulation speed is 8 GB of RAM and 1 TB of storage space. Amazon Access Samples data set information is used on the transaction processing between clients and server systems. The Amazon Access Samples dataset includes four categories of attributes including Person_Attribute, Resource_ID, Group_ID and System_Support_ID.

V. DISCUSSION

The proposed CSEDTS framework is compared against with the Remote Data Auditing (RDA) method and Stackable Secure Storage System (Shield).

Impact of Transactional Security Rate

The impact of transactional security rate for CSEDTS framework is elaborated and comparison is made with two other methods RDA and Shield respectively. Table 1 represents the security level obtained using CloudSim simulator. Figure 2 explains the transactional security rate obtained with respect to number of request. The transactional security rate using the proposed CSEDTS framework is higher when compared to two other existing methods namely, Remote Data Auditing (RDA) method and Stackable Secure Storage System (Shield). This is because of the application of Conditional Attribute Encryption and Conditional Attribute Decryption algorithm that efficiently uses the mapping function therefore increased the transactional security rate on data layer. In addition, the cipher specific id generation is obtained through bilinear function based on different client requests. This in turn helps to increase transactional security rate by 7.5 % when compared with the RDA and 11.8 % when compared to Shield respectively.

Impact of True Positive Rate

The impact of true positive rate for CSEDTS framework is presented in Table 2. Figure 3 explains the true positive rate with respect to the number of attributes. The true positive rate is higher for the proposed CSEDTS framework when compared to two other existing methods namely, Remote Data Auditing (RDA) method and Stackable Secure Storage System (Shield). This in turn increases the true positive rate when compared with the RDA and Shield respectively.

Methods	Transactional Security rate (%)
CSEDTS	93
RDA	86
Shield	82

Table 1. Tabulation for transactional security rate

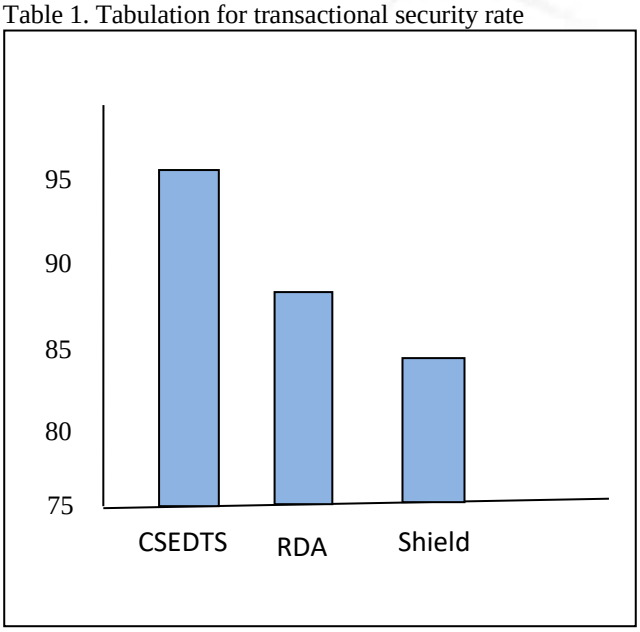
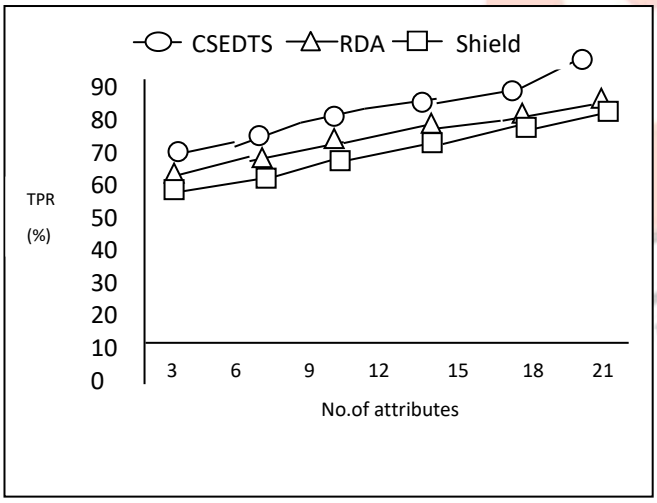


Figure 2. Measure of transactional security rate.

No.ofattributes	Truepositiverate(%)		
	CSEDTS	RDA	Shield
3	62.35	54.38	58.21
6	68.65	56.62	61.35
9	71.24	58.23	63.29
12	73.42	60.24	64.37
15	75.14	63.25	67.12
18	76.89	67.68	69.39
21	81.36	68.74	71.28

Table 2. Tabulation for true positive rate



VI.CONCLUSION

In this work, an effective framework called Conditional Source Encryption Data Transactional Security (CSEDTS) is presented. This framework increases the performance of transaction security for different user conditional request using mapping function using the specific id number. The transaction request is evaluated in an efficient manner and as a result, the proposed framework improves the transactional security rate on data layer for each client requests resulting in improved transaction processing. The results show that the CSEDTS framework offers better performance when compared to the state-of-the-art methods.

VI. REFERENCES

1. Purushothaman D, Abburu S. An approach for data storage security in cloud computing. International Journal of Computer Science Issues. 2012 Mar; 9(2):100-5.
2. Vairagade RS, Vairagade NA. Cloud computing data storage and security enhancement. IJARCET. 2012 Aug;1(6):145-9.
3. Bhisikar P, Sahu A. Security in data storage and transmission in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Mar; 3(3):410-5.
4. BrindhaT, ShajiRS, RajeshGP. A survey on the architectures of data security in cloud storage infrastructure. International Journal of Engineering and Technology. 2013 Apr-May;5(2):1108-14.
5. Divya SV, Shaji RS, Venkadesh P. A comprehensive data forwarding technique under cloud with dynamic notification.

Research Journal of Applied Sciences, Engineering and Technology. 2013 Jul; 7(14):2946-53.
6. Pandey A, Gond S. Secure communication over cloud computing network using OTP (one time transaction) method. Int J Computer Technology and Applications. 2014 Sep; 5(5):1707-10.
7. JadhavSP, NandwalkarBR. Efficient cloud computing with secure data storage using AES. International Journal of Advanced Research in Computer and Communication Engineering. 2015Jun;4(6):377-81.
8. Shaikha R, Sasikumar M. Data classification for achieving security in cloud computing. Procedia Computer Science. 2015; 45:493–8.
9. Sugumar R, Imam SBS. Symmetric encryption algorithm to secure outsourced data in public cloud storage. Indian Journal of Science and Technology. 2015 Sep; 8(23):1-5.
10. Mohamed SPM, Shaji RS. An efficient framework to handle integrated VM workloads in heterogeneous cloud infra structure. Soft Computing. 2016 Jan; 1-10.