ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Approach for Securing the Clients Data in Cloud Storage with Network Coding Function via Multi Authority Auditing (MAA) Scheme

Brahmini. P
M. E Scholar, Department of CSE,
SCSVMV University,
Kanchipuram-631561, India.

Ms. R. Poorva Devi
Assistant Professor, Department of CSE,
SCSVMV University,
Kanchipuram-631561, India.

Dr. S. Rajalakshmi
Director, Advanced computing center,
SCSVMV University,
Kanchipuram-631561, India.

Abstract: The data outsourced by the user to the cloud should be intact i.e., it should not be altered by the cloud for any reasons. In present days many services are being provided by the cloud. Storage is one the service cloud provides. Even it is widely accepted still end users suffer with lack of security in the storage because hackers are more intelligent hacking techniques. To protect the user's data from these kinds of hacking morality, to propose a high level of security by using secure cloud storage, networking coding and multi authority auditing phenomenon. Secure cloud storage protocol is a promising one, for enabling the user to ensure the integrity of data in the cloud. Another mechanism of network coding is a routing paradigm different from the traditional store-and-forward method. Primarily, to propose a multi authority auditing which is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities. We can demonstrate the relationship between these areas using a series of steps in cloud environment. The proposed techniques are applied into the ican cloud simulator tool to find the efficient outcome for cloud security utility.

Keywords: Secure Cloud Storage, Secure Network Coding, Multi Authority Auditing, Cloud Server, Cloud Security.

I. INTRODUCTION

In present cloud computing scenarios different users are using distinct services provided by the cloud. Whatever the service may cloud must ensure security. If any application is developed without security it will not work efficiently .In our scheme we propose Secure Cloud Storage along with Secure Network Coding with Multi Authority Auditing. **Secure Cloud Storage:** It is concerned with the problem of checking whether the data outsourced to cloud remains the same as it was before being outsourced. There are two main entities involved in this protocol: a user and a cloud storage provider (CSP). A user outsources the data to the cloud that promises to store the whole data. The user confirms to data integrity by frequently auditing the cloud through the protocol. Traditional service access can be given in the following diagram. It will enable the major services such as,

- ➢ Outsource the service ranges
- ➢ Auditing the user details
- ➢ Proving the Authenticity

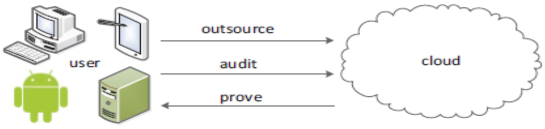

Figure 1. Service access between user and cloud server

From the above diagram we can know that the user will first outsource the data. Next he will audit the cloud by sending audit query. As a response to the audit query cloud will send a proof to the user. **Secure Network Coding:** is a routing paradigm different from the traditional store-and-forward method [6]. Instead, a router in the network sends out encoded data packets, where the encoding is a function of received data packets. Encoding can increase the network capacity.

I

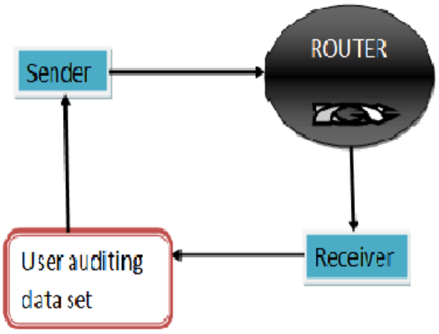

Figure 2. Secure Network Coding operation

In network coding there are 3 entities. Sender sends divided and encoded packets to the router. The router will forward the packets to the receiver acting as a sender. The receiver will combine the packets from router to form the original data [9].

A. *Implication of Multi Authority Auditing*

Multi Authority Auditing is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities. It provides the various computational facilities towards the user authorization feature and also try to improve the operational efficiency. Auditing should focus on the enhancement towards the user perspectives and enabling the service access platform to function properly. Managed service providers also be a part of this MAA based development scenarios to upgrade the user privacy and security perimeters.

II. EXISTING WORK

In the existing works authors did not combine the two protocols secure cloud storage and secure network coding. Protocols have been specified for cloud storage and network coding which involves some extensions of bilinear maps and support of message authentication codes. In protocols such as POR auditing can be done only finite number of times[5]. Network Coding was implemented as a technique to improve the throughput of the network. In other work network coding is employed to repair the damaged data fast, but not to audit. The works related to Third Party Auditing (TPA) were also proposed [3], in which auditing of data is handled by single authority. Data owner will encrypt his data and put in the cloud server and TPA will perform audit action based on the data owner's request. Data owner just outsources the auditing work to the third person who can be trusted. In the earlier work ad-hoc based control is not relying on the user boundary state. Some of the major drawbacks are mentioned.

B. *Short come of Existing System*

All the above existing systems suffer with some drawbacks. They are named as:

- Lack of security argument.
- All the protocols are ad hoc in manner.
- They considered repairing the data fast.

In the traditional approaches, customer and developer conversation provides less service supportability value rather than a manual operation [4]. People found that the usage of the existing mechanism is not efficient. So, to provide an efficient result set the proposed model has been implemented for cloud security values.

III. PROPOSED WORK

The users should not suspect the cloud when they outsource the data onto the cloud platform. In our model, we try to combine both secure cloud storage, secure network coding by enhancing third party auditing with multi authority auditing [2]. Multi Authority Auditing [1] is a mechanism in which the auditor will audit the data on behalf of user there by reducing the burden and overhead on the user data storage. Multi authority auditor will have more knowledge about the data value and its data characteristics. It will check whether the data remains intact on cloud.

C. *Consequences of Multi Authority Auditing Task*

Auditing of the data is handled by multiple authorities who work in auditing department. Auditing head and attribute authority members are present inside the multi authority auditor department. **Auditing Head:** Auditing head governs the attribute authority people. Every data owner, data consumer and attribute authority people must register with the auditing head. Auditing head will give a unique id to each of them. Auditing manager will also provide a public key and a secret key to all of them. This unique id will be unique across the system. **Attribute Authority:** Attribute authority is an independent authority that is responsible for assigning attributes according to their role or identity in its domain. Every attribute is associated to each attribute authority. Each AA has many numbers of attributes. Each AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating public key and secret key for each user reflecting his attributes. Here user is data consumer. So, a data consumer, will have global identity(public key, private key) provided by authority head and private keys reflecting his attributes provided by AA. Multi Authority Auditing will be best suitable for large organizations.

D. *Architecture of Proposed System*

In the proposed model data owners need to focus on their data security in all the aspects. Basically, in the entire domain there will consider some piece of information as normal security (login) credentials system. While considering the cloud based security implication tasks at that time, users are prompting into the cloud environment based on the three factors that is, **CIA** principle.

- Confidentiality
- Integrity
- Authenticity.

The following diagram shows that, how the data owners are performing their task in cloud environment by using outsourcing technique. Lots of access data can be migrated from data owner location into the cloud vendor sites.

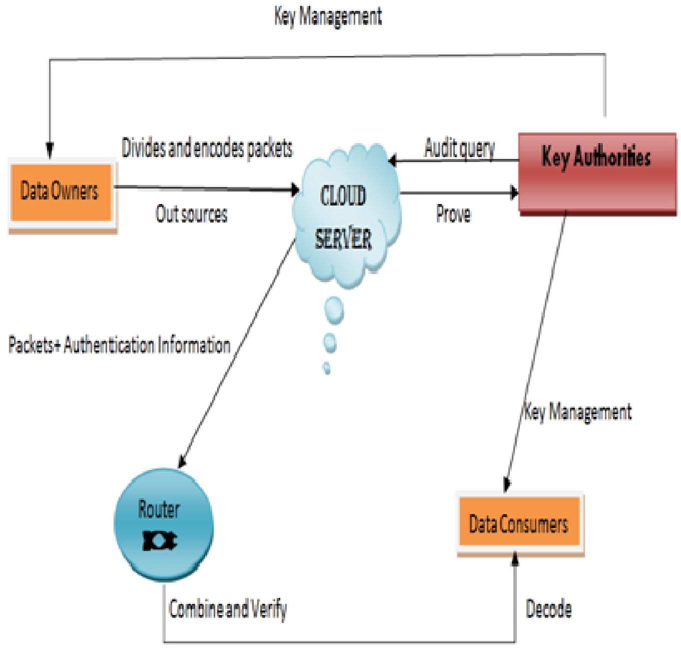

Figure 3. System Architecture

Before hosting data onto the cloud,

- Data owner will divide the data into separate components and encrypts them separately and outsources into the cloud environment.
- The multi authority auditor present in the key authority will audit the cloud to check the integrity the data.
- The cloud will send proof as a response to the audit request.
- The cloud will forward the packets to the router, in this case cloud becomes the sender so, it attaches some authentication information to the data.
- The router after receiving the data from cloud server will combine the data and verify whether it is correct or not. If it is correct he will forward to the data consumers.
- The data consumers will decrypt the data using the keys provided by key authorities.

The first 3 steps denote the procedure of cloud storage. The next 3 steps show the concept of network coding. In both the procedure we have simulated multi authority auditing.

E. The Process of data encryption by data owner is as follows:

- He divides the data M into several components {M1, M2... Mn}. For ex: personal data will be divided as {name, address…}
- He encrypts the data components with different content keys {k1, k2,…kn} by using symmetric encryption methods.
- Then, he defines the access structure S, the order in which each component needs to be encrypted.
- Content keys, access structure are also encrypted by data owner, and hosted onto the cloud.

F. The Process of data decryption by data consumer is as follows:

The process of data decryption by data consumers can make use of distinct set of input parameters and entities for securing their private data element. Some of the activities are considered as major security constraints in cloud environment which are listed below. The inputs are given as data source parameters.

- Data to be decrypted.
- User's global public key, global private key, attribute public key, user's secret key for that attribute.
- Using the above inputs content keys are decrypted by data consumer.
- Using content keys, the actual data is decrypted.

IV. IMPLEMENTATION WORK

The Implementation work can be summarized as follows:

- The user will divide the data and encrypt the packets using symmetric encryption techniques**.** **Y=E (K,X)** and then outsource the data on to the cloud. **Outsource (F; K) -> F:** On input of data F to be outsourced user runs this algorithm to get processed using secret key K.
- The auditor will audit the cloud by sending audit query q using algorithm **Audit () -> q**: The user runs this algorithm to generate an audit query q which will be sent to the cloud.
- The cloud will send proof to the auditor using **Prove (q, F) → Γ:** On input an audit query q, the cloud computes a proof Γ using the stored data F.
- Cloud server forwards the packets to router by adding authentication information with the algorithm **Auth (xi) → (xi, ti):** On input a packet xi to be sent out in the network, the sender computes an authentication information ti and sends out (xi, ti)
- On receiving packets from cloud server router will combine them by using the **algorithm Combine {ui, t i} → (w, t):** On receiving a group of packets ui and their authentication information ti's, a router runs this algorithm to generate a combined packet and the combined authentication information t.
- To forward the combined data to the data consumer router runs this algorithm to check **Verify (w, t) → δ:** On input a packet w and its authentication information t, a router or a receiver runs this algorithm to check whether a packet is modified maliciously. If the packet is correct, it outputs δ =1, else outputs δ =0
- After receiving data, the data consumer will decrypt the data using symmetric key cryptography **X=D [K, Y].**

So, these above listed functionalities are carried out in the cloud platform to sustain the security outcome and to provide an efficient output result.

V. SIMULATION WORK

In the cloud environment securing the data is very tedious task because the hackers are trying to capture the data by using very intelligent mechanisms. Moreover we are not aware of the hacker's origin. At the cloud service provider end there must be enough security [8]. When the user starts to use the service he experiences some attacks like:

- Hypervisor Hacking
- Guest OS app's hacking
- VM hacking.

In the proposed work, user is enabling the secure network coding function to optimize the user data security value. Some of the input parameters are considered for providing the information safety outcome.

- Request type
- Recipient public and security key
- Scheme of encoding values
- Auditing Query segment
- Process of Key management
- Content Decode Techniques
- Data owner IP address

G. Environment Setup

Platform	: java JDK 1.7
IDE	: Net beans package
Simulator	: ican cloud sim
Data source:	Data owner site
Input set	: Encode & Decode form
Server	: Apache Tomcat 1.8.0 tar.gz

To execute the security task all the input packages are well defined and categorized based on its input properties. The measurement part, must be taken into the consideration work to establish the security region between encode and decode value set. Ican cloud simulator tool will provides the sufficient infrastructure to inhibit the cloud functions. It is majorly, to protect the confidential information's from the vulnerable activities. The simulated environment must perform the following task to be getting processed through the cloud platform. All the key management principles must be notified to illustrate the cloud actions which are acting upon the customer end.

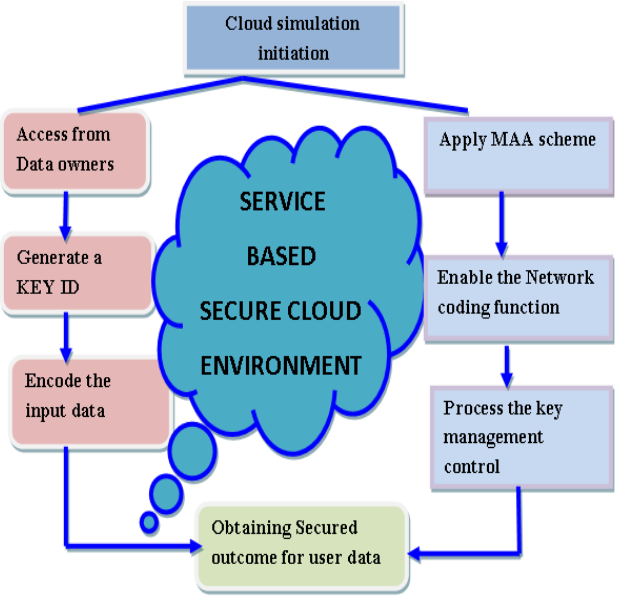
Cloud simulation initiation
Access from Data owners
Generate a KEY ID
Encode the input data
SERVICE BASED SECURE CLOUD ENVIRONMENT
Apply MAA scheme
Enable the Network coding function
Process the key management control
Obtaining Secured outcome for user data

Figure 4. Figure illustrating simulation work

From an above picture, all possible components of input elements are to be considered in the cloud environment. While establishing the setup for cloud server with the client, it needs to be processed the input elements with processing through MAA scheme along with the network coding function.

Sample code:

```
    // Network coding Function //
Init. Cloud service (WWW. Protocol)
Init. Define Global var = IP and MAC address
Access limit= VM and GUEST APP CODE
Define. Cloud resources = EXE_ 192.168.10.251
Proxy-server = APACHE TOMCAT = 0 and 1 .DLL
    // Multi authority Auditing scheme //
Init. Cloud service = Salesforce_ PACKAGE
Define. Input Key= $K_S$ [Encode, Decode values]
Access = KEY_ID {DATA ACCESS, LIMIT}
Define_REGION= [Server access privileges]
META_CONDITION = Inhibit MAA level security
Find_EXE REGION = APP / SERVICE exchangement
FINISH_SECURE_ACCESS = Ks protection
```

In this major codes only shown to observe and specify the input consideration and various activity levels of server and client validation control. Whatever the activities are processing into the cloud environment that can be satisfies the user level or client level security compromising value only. We cannot modify or change the server access and its permission level limits.

After the consolidation of process sequences, the following output values are obtained that can be given below:

Table I. Simulated Result Set- I

Cloud vendor	Secure cloud storage value (%10)	Key Authorities (0 to 1)	Audit query segments status
Sales force	8.571	0.9	processed
MS Azure	9.014	0.82	processed
Google APP engine	9.78	0.837	Processed
AWS	8.903	0.869	processed

Table II. Simulated Result Set- II

User IP Address	Key access value / 10	Secure cloud storage	MAA value (%100)
192.168.10.89	9.03	Protected	90.32
192.168.24.81	8.08	Protected	93.29
192.168. 84.92	8.71	Protected	96.20
192.167.56.20	9.054	Protected	96.845

The result set-I and II shows that various input IP address was considered and it was executed in ican cloud simulator tool. The protocol that was processed with the encoding and decoding schemes produce a quality result set of secure cloud storage protocol. Audit query segments are executed and implemented in various user level entities. MAA (multi authority auditing) can be a vital function for this proposed phenomenon. Ensuring the user level secret information can be processed with the combination of secure cloud storage access value along with the MAA scheme.

VI. EXPERIMENTAL RESULTS

The various cloud user input values perform their functionalities based on the user level key identifier ranges. Security can be provided with high-end result set to obtain the reasonable solution for client level data protection. In this approach, we consider the major components that can be utilized in the various user level service access environments. The following input components are used in this approach:

- ✓ Key access value
- ✓ Audit Query segments
- ✓ Secure cloud storage output
- ✓ MAA resultant value

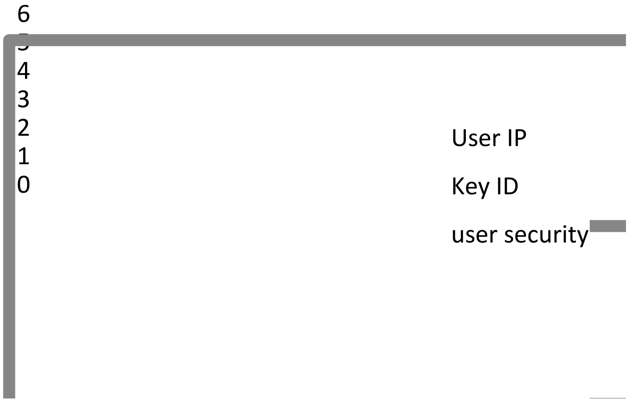

Figure 5. Illustration of the security outcome

The above result set is the outcome for this proposed model. All the input credentials are processed in the cloud environment.

VII. CONCLUSION

In the current era, all the applications must process through various security constraints and the boundary level. To secure the confidential information which is available in user end that must be notified in the client perspective. From this implemented results, security is reliable in customer end. So, from this approach we may combine the secure cloud storage protocol along with the MAA result set.

VIII. FUTURE ENHANCEMENT

In future cases all the web based applications and its services will run in to the cloud platform with the help of suitable cloud vendor. The fore coming process must be specified with the suitable algorithm like VM scheduling or load balancing algorithm to eliminate the problem of hacking.

IX. REFERENCES

[1] Chang Liu, Jinjunchen, Yang L. T, Xuyun Zhang "Authorized public auditing of Dynamic Big data storage on cloud*", IEEE transactions*, vol.9, no.2, 2014.

[2] Husain. M, Al Mourad M. B "Effective Third Party Auditing in Cloud Computing" in *Advanced Information Networks and Applications Workshop (WAINA) 28th International Conference*, 2014, May 13-16, pp 91-95.

[3] Fei Chen, Tao Xiang, Yuanyuan Yang, Chow S. S. M "Secure Cloud Storage meets with Secure Network Coding", *International Conference on Computer Communication*, 2014, April 27-May 2,pp. 673-681.

[4] A. Le and A. Markopoulos, "Nc-audit: Auditing for network coding storage," in *International Symposium on Network Coding (NetCod*), 2012, pp. 155–160.

[5] A. Juels and B. Kaliski Jr, "Pors: Proofs of retrievability for large files," *in ACM Conference on Computer and Communications Security (SP),* 2007, pp. 584–597.

[6] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[7] Y. Hu, P. P. Lee, and K. W. Shum, "Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems," IEEE *International Conference on Computer Communications (INFOCOM), 2013.*

[8] Durrani. A, "Analysis and Prevention of Vulnerabilities in Cloud applications", in *IEEE International Conference*, 2014, 12-13 June, pp. 43-46.

[9] N.CaiandR.W.Yeung,"Secure network coding," in *IEEE International Symposium on Information Theory (ISIT),* 2002, p. 323.