Privacy Preserving Audit Protocol role in Dynamic Remote Data Auditing

B Sasikumar[1], M Ramprasath[2] and Hariharan Shanmugasundaram[3]

[1]*Professor, Department of Computer Science and Engineering, Dr.V.R.K Womens College of Engg & Technology*

[2]*Associate Professor,Department of CSE, Madanappale Institute of Technology Science, INDIA*

[3]*Professor, Department of Computer Science and Engineering, Saveetha Engineering College, INDIA*

ABSTRACT:

In recent year, cloud computing provides consistent, customized and quality service to the cloud user for securing the data in cloud storage. Currently, numerous business organization generate enormous volume of insightful information for instance, employee personal data, economic related information and data related to hospital records. Subsequently, digital information related to multinational were increased. so, they avoid storing their information locally and they planned to outsource their data to cloud environment. On the other hand, the significant worry to the data owner is to deliver security and truthfulness their outsourced data. Our proposed system takes this issue as a challenging task and provide security to the out sourced data in cloud environment by using Remote Data auditing (RDA) Technique. In earlier days most auditing techniques only focused on static data and not supported for dynamic data. In this paper, we proposed a professional RDA technique using Data Privacy Preserving Protocol for cloud storage system. Our system also designs system model which support the dynamic data operation in the cloud environment. The experimental result shows that proposed model for auditing protocol is safe and extremely efficient as compare to existing auditing techniques.

Keywords: *Remote Data Auditing, cloud computing, Privacy preserving protocol, Data integrity.*

Abbreviations: *IaaS*, Infrastructure as a services; PRC, Privacy rights clearing; DAP, Dynamic Auditing Phase.

I. INTRODUCTION

In Now a days, cloud computing has capability to computing resources on demand and offer a simple pay-as-you-go services model for customers. It also emerged as a new computing standard, and has gained more attractiveness in business environment. On the other hand, the data produced by the company and managing this information in local storage [1] is difficult process. Currently, numerous big companies have moved their business service from local computing infrastructure to Amazon elastic computing cloud (EC2) or cloud storage, which is a most important public Infrastructure as a service (IaaS) in cloud computing environment [2]. To avoid data load on the local storage all the companies were chosen cloud environment to store information and dismiss maintenance in the local environment [3] and communication cost.

Storing client information in cloud environment [4] is significant enough that would help data owners. Nevertheless, the above concepts introduced new challenges to data owner for hosting data in cloud environment [5] to the user. Though the data owners gets numerous benefits such as outsourcing data to remote server, handing over the management of data to entrusted cloud service providers it can direct loss of data controls [6]. Data which were less frequently accessed were discarded by the cloud were corrected in the cloud space [7]. In 2011, some business organization reported that the data was exploited in cloud server which affects major cloud service provider and many instances of cloud services like amazon S3 break down and gmail fault detection [8].

There have been 535 data gaps happened in 2011was reported by (PRC) Privacy rights clearing house such as Sony picture and online entertainment theft of medical data record and customer information. When intruder revoke the permission for accessing data in cloud storage which lead to produce reply attack over the encoded data stored in cloud server. Due to this attack the truthfulness of the user information available in the remote server admired to internal or external attack. To Afford information integrity in cloud storage traditional integrity methods needs local copy of information stored in cloud. Even though it is not possible for mobile user to down load large amount of data from cloud storage [9] which makes complexity to the mobile operator to access the information remotely in cloud storage. [20] presented cloud storage system bear the data privacy preserving in cloud environment.

In this context, to verify integrity in cloud storage system requires more efficient techniques to validate the integrity of the data. Many researchers have proposed several techniques to address the problem using RDA method have capability to validate data in secure manner by generating challenges [10]. In general RDA can be classified into three different categories such as integrity based, recovery based [11], deduplication- based [12] methods. In existing RDA techniques focus on computational and communication cost of data owner which was the huge load for data owner. The design principal of remote data auditing is to support dynamic operation on different application process. The data owners incur various types of data structure (preferably binary tree) to support dynamic operation in cloud environment.

Conversely, these data structure is not support the dynamic operation in big scale of data resourcefully because of regular update on cloud data which leads huge computational charge to on auditor. To overcome these problems in the cloud environment, our system propose Dynamic remote data auditing which support the dynamic operation by using secrecy protective auditing protocol. Major significant objective of the inspecting protocol is to protect the information privacy counter to auditor.

Major contribution of paper as follows: a) RDA methods to outsource information in cloud environment using data privacy preserving protocol. b) Design and overview of privacy preserving auditing protocol with dynamic data operation such as update, modify, insert with minimum computational cost. c) Proposed protocol implementation in real environment and the results shows protocol skill to afford improved integrity on data, safety and performance as compare to the existing techniques.

The following section will shows the reminder work of the proposed model: section 2 discussed about related work in RDA, section 3 present common system model for remote data auditing, section 4 discuss proposed system model using data privacy preserving protocol, section 5 discuss about dynamic data operation in cloud environment.

II. RELATED WORK

In recent years, outsourcing data in cloud environment is an important service which allows the user in reducing local burden for storing data [13]. Numerous user starts to accumulate the data remotely in cloud storage which make the user to concern about the data loss in cloud because of security issues. To overcome these issues researchers have presented several study related to RDA schemas [14] with integrity check and exact outsourced information in the cloud context. Several existing methods were reviewed using data integrity and discussed the advantages and disadvantages of methods. The very first provable secure schema was discussed with authentication of data integrity in cloud without download the data from it [15]. This method uses the RSA- constructed homomorphic provable tag used to produce single tag using group of tag.

This methods uses RSA based numerical methods which lead to acquire higher computational and communication cost. Proof of- Retrievability (POR) [16] in newer type of RDA methods which uses to check the information integrity and prevent from losses by using forwarded correction techniques, remotely. The computational cost for POR method is high on client side which leads to perform data recovery and encryption process. To enhance the protection and effectiveness of the POR method it uses BSL [17] homomorphic authentication techniques. This process permits auditor to combined tags which helps to reduce the computational cost. However in cloud environment it’s unfortunate to conduct dynamic remote data auditing because none of them (cloud service provider or data owner) have achieved guaranteed with balanced auditing results [21].

In several Remote auditing methods dynamic operation on information update is an essential issue in cloud computing. During this operation data owner having permission update their data present in the cloud storage without retrieving outsourced file. Enhance the scalability and efficacy of dynamic operation [10] RDA technique was projected which uses symmetric key operation to defeat problem in static RDA techniques. However the owner has to do pre-computation process for verification of data before uploading in to cloud storage, also data owner can only perform append, delete and modify operation but owner doesn't having permission to do dynamic update operation on the data which lead to re-computation of all the outstanding data and its acquire high computation charge on information owner. [18] Has discussed remote data ownership checking which allows the integrity checking or verification on the remote data in crucial information environment. [19] Present the design of dynamic provable data ownership and framework, which support to store the updated data.

In our proposed system, we introduced new method and algorithm for dynamic remote data auditing using privacy preserving protocols, which allow the data owner to perform self-motivated operation to make sure the integrity in the cloud environment. The system also discussed proof of correctness using some characteristics.

III. Proposed model for RDA protocol

Figure 1 shows general RDA model, which consider following components for instance data owner, Cloud Storage Provider (CSP), third party auditor (TPA). The following Fig 1 shows the RDA system Model.The enterprise or businessperson will be act as data owner used to upload the data into cloud storage and later he/she can able to modify or update the outsourced data. CSP is responsible for managing information in cloud space hosted by the data owner.

It also has a considerable amount storage space and calculating resources for doing operation on the stored data. Third party auditor has enough skill set for performing the audit operation on the data also aids to minimize the mathematical complexity of auditing process. Before discussing the proposed auditing protocol in details let us discuss the general notation going to used in these protocol which is shown below.

The proposed system model has the following function, such as Key production, Tag production, challenge, proof generation, Proof confirmation which helps to design a remote data integrity checking protocols.

Key generation setup(μ)$\rightarrow$(St_k,Pt_k)this function takes only safety parameter as input μ it produce output as pair of undisclosed hash key and secret public key (Sh_k,Pt_k).

Tag generation(D_c ,Sh_k , St_k) $\rightarrow T_d$ The foremost goal is to verify the data integrity. It takes Data component as D_c ,secret tag key St_k and secret has key Sh_k as input and compute data component and make it publically known to everyone.

Challenge ($D_{c\ info}$)→$C_a$its takes input as abstract data component and out puts the challenge message to data owner.

Proof generation (D_c,T_d,C_a) →$S_p$its takes inputs as abstract information, data component, Auditor challenge and out put the server proof S_p.

Verification (C_a,S_p, Sh_k, Pt_k, $D_{c\ info}$) →(Accept, Reject) this verification earnings as inputs the Auditor challenge, server proof, undisclosed hash key, Communal tag key, data component and intellectual information of D_c and out auditing results as accept or reject.

During the whole auditing process auditor should be truthful and interested about acknowledged data. Server could be not truthful and may leads to attacks such as exchange, replay and forge attacks.

Replace attack: To replace the already discarded data block and data tag (D_c,T_d) the server chose **the** appropriate and unaffected data block and tag for challenge operation.

Replay attack: Without using the data owner information, server produces duplicate proof from information that exists earlier or from other informations for replay attack.

Forge attack: The information tag and block was forge by the server and mislead the auditor, when owner undisclosed tag key is reprocessed for dissimilar data version.

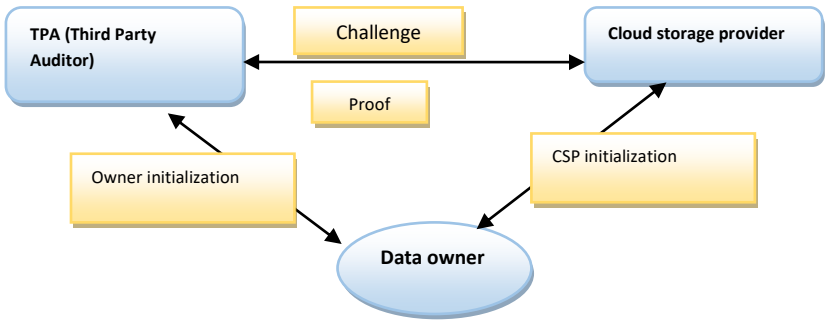


Fig 1 .RDS system Model

Table 1: Notations used in proposed system

Symbols	Meaning
St_k	Undisclosed Tag key
Pt_k	Communal Tag key
Sh_k	Undisclosed hash key
D_c	Information Component
T_d	Information tag sets
N_c	Quantity of blocks in each data section
N_s	Quantity of sector in each information block
$D_{c\ info}$	Abstract data information of D_c
C_a	Auditor task
S_p	Server proof

Privacypreserving protocol for cloud environment

In this segment, we discuss the basic methods used in our proposed project of auditing protocol after that we present the proposed procedures and structure of auditing protocol in cloud environment. In our system, privacy is the major task in design of the information storage auditing protocol. This reason behind is a) if information is publicly available means the auditor is easily attaining the data information by recovering information blocks. b) If it is encrypted data means, the auditor can obtain the encrypted key through by using some special operation and can able to decrypt the data. In the proposed system, data privacy problem could be solved by generating the encrypted

proof by challenging stamp by using linearity property where auditors can verify the perfection of the information by decrypting it.

In general, to conduct auditing service in cloud environment, auditor should have knowledge and capabilities. The computing viabilities for auditor are not as strong as cloud server. Since the performance of the system get reduced because of the huge auditing process done by the auditor. To overcome the issues, the proof of inter mediate value verification will computed by cloud

server and auditor make use of this midway value to verify the proof. As a result, the computation load is reduced by delegating work to the server.

Algorithm

Let us consider file '*f*' having n data components as $f = (f_{dc1} \ldots\ldots f_{dcn}$ in which each file has it own meaning and it vigorously by the owner of the data. There is two cases for performing encryption operation on the file. If the file is publically available means that owner need not to encrypt the data but for remote information component, that information owner must do the encryption operation with its corresponding keys. Information components (DC_f) of each files are divided into N_{dc} data blocks as:

$f = (DB_1, DB_2 \ldots\ldots DB_n)$ (1)

Security parameter has been used to reduce the data block size for provided more production to the out sourced data by the data owner. For instance, if the security level is set to 180bit then the data block size should be 30byte. This block size reduction will help to reduce storage overhead in real time process.

Data fragment techniques could be used to divide each information block into sectors and the size of sector also have been reduced with some limitation using the security parameter. To Minimize number of information tags, its produced for each block which contain 's' sectors. The size of the data block could be varied in real time storage system; different data block contains different size sectors. For instance, the frequently read data block DC_i which contain large number of sector S_i at the same time if the data block is regularly updated means the sector size is relatively small. In general, data section, continuous number of sector for each information block can be consider for construction of auditing protocol.

Initially the data component D_c can be separated into *n* number of information blocks and each block fragmented into '*S*' sectors. The sector for each data blocks will varies based on the data components, first its selects maximum number of sector 'SE_{max}' among all sector numbers S_i . Then we consider for each D_c with S_i sector $S_i < SE_{max}$ which tell that the data block has $< SE_{max}$ sector by setting $D_{cij} = 0$ for $S_i < j \leq SE_{max}$. Since the dimension of the individual sector is continual and equivalent, security parameter '*p*' information component can computed using equation 2 :

$$n = \frac{sizeof\ (D_c)}{s.\log p} \quad (2)$$

The encoded information component is represented as $DC = \{dc_{ij}\}\ i \epsilon [1, n], j \epsilon [1, s]$. Let us consider the multiplicative group MG_1 , MG_2 …MG_t with same parameter *p* and E : $MG_1 \times MG_2 \rightarrow MG_t$ treated as bilinear map. The originatorof MG_1 and MG_2 be g1and g2 respectively and the secure hash function H :{0,1} $\rightarrow MG_1$ plots DC information to a point in MG_1. Proposed auditing RAP

contains Key generation tag generation, challenge and proof algorithm which help to build the frame work for data privacy preserving audit protocol.

Key generation randomly choose two number St_k ,$Sh_k \epsilon Z_p$as secret and hash key and produces output as communal tag key, undisclosed key and secret has key$pk_t = g^{2^{Stk}} \epsilon MG_2$.

Tag generation algorithm first chooses s as random values as V1, V2…Vs $\epsilon Z_p$and computesu_i $g^{1^{Xj}}$ for all j ϵ [1,s]. for each information block DC_i(i ϵ[1,n]), the information tag DCT_i is computed as:

$DCT_i = (h(Sh_k, W_i) .)sk_t$ (3)

where W_i indicate the concatenation operation which uses the information identifier FID and block number of data component to produces set of data tags as outputs. The owner initialization process is represented in Fig 2. Fig 3 and Fig 4 represents the audit conformation and sample auditing process in the RDA.

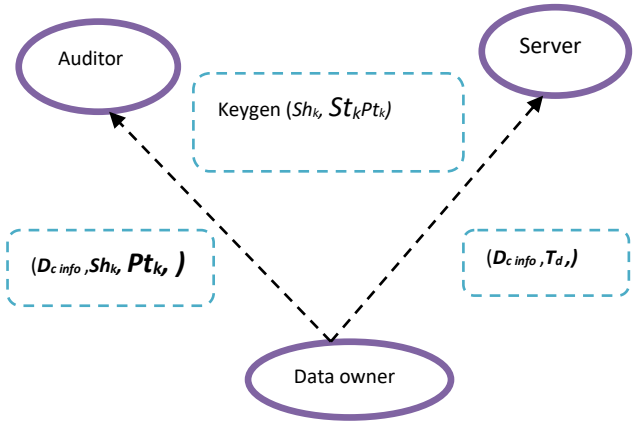
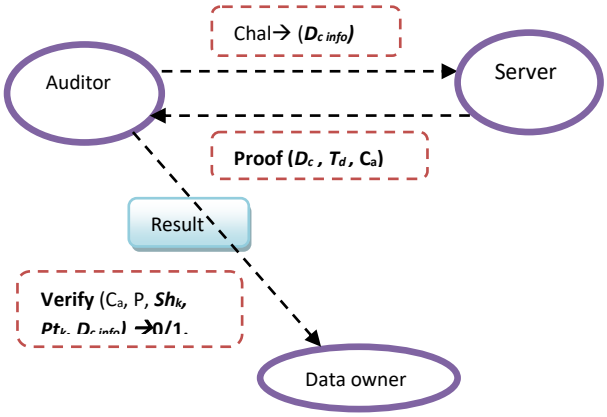


Fig 2. Owner initializations

Challenge ($D_{c\ info}$) : the input for this process is abstract information of data $D_{c\ info}$ and select some data block construct test set *q* and generate arbitrary number for all **Proof (D_c , T_d , C_a) →*P*** this process uses the challenge from the previous step and data component used a information block. It output the challenge stamp C_s = $Pt_k$by randomly choosing number from data block

P = (tp ,dp).inputs. It contain tag proof *tp*and data proof *dp* and output as



.

Fig 3. Audit conformation

Verify (C_a, P, Sh_k, Pt_k, $D_{c\ info}$) **→0/1.** It initially computes identifier $I_{challenge}$ value and of all challenge data block and calculate challenge has value $H_{challenge}$as follows :

$$H_{challenge} = \prod i\varepsilon q(\mathbf{Shk,wi}) \qquad (4)$$

The equation is used to confirm the data resistant from the server.

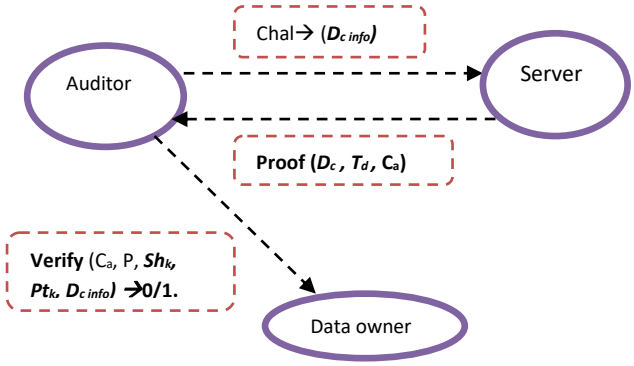


Fig 4. Sample auditing

Audit protocol construction

Figure 4 contains three phases for audit protocol construction such as initialization of the data owner or owner construction, Audit conformation and Trial auditing. In the begin or initial phase, data owner generates key and tags for data. Next the data must be Figure 4 contains three phases for audit protocol construction such as initialization of the data owner or owner

construction, Audit conformation and Trial auditing. In the begin or initial phase, data owner generates key and tags for data. Next the data has to be store in the server after wards the data holder enquires the auditor to contact audit conformation to make sure that information properly stored on cloud server. After conformation received from the auditor the owner has rights to remove information stored locally. To verify or check the data truthfulness the auditor can periodically contact the trail auditing on the data.

Data owner initialization component initially run the key production algorithm to generate underground-public tag key (**St_k**,**Pt_k)** and confidential has key ***Sh_k*** **,** then it compute the data tag by running tag generation algorithm. Then making information tags, data holder send information components ***D_c*** and its corresponding tags to server in concert with set of parameter. Finally, the data owner send the abstract information of data component, secret hash key and public tag key (***D_c***,***Sh_k***,**Pt_k)** to the auditor for initialization process.

The next phase of the audit construction is conformation auditing which involves only two way communication such as challenge and proof. The main goal in this phase auditor to checked whether information is appropriately stored in the server or not. The working process of the conformation audit as follows:

First, auditor run challenge procedure '**C_a**'**(*CH_a*)** to produce challenge for information blocks in data components '***D_c***'and auditor send response message to server. After getting challenge response from auditor server run the prove algorithm to generate proof '**S_p**' and send back to auditor. After receiving the proof by the auditor from the server run verification algorithm to verify accuracy of challenge message and extract audit result. Next, audit result should be send to the data holder and he will check whether the result is correct of not. If its correct then data holder influenced that information is properly stored in the server and data editing is possible.

Sample audit is important phase in audit protocol construction, which could be contacted periodically by modifying test set of data blocks. This audits process depends service conformity among the documents owner and server and how much data owner having trust on the server. During the sample auditing process if any data corruption is happen that could be calculated as follows by using probability function. For instance, each sector in the data block is corrupted every so often with probability ***'P'*** on the server. The probability of detection of 't' challenged data blocks in sample auditing is calculated as

$$P(t,s) = 1- (1-\rho)^{t-s} \qquad \textbf{(6)}$$

The equation 6 is used to detect any corrupted data block in sample auditing process. Correctness of the proof for privacy preserving auditing protocol can uses the standard following principal: which state that, the server only pass the audit challenge – response protocol if all the data blocks and tags or correctly stored. The proof verification equation can be written as follows:

$$\text{DP}.(e^{H}{}_{chalenge}\ pt_k) \qquad \textbf{(7)}$$

if any information block or tags is dishonored server cannot pass the audit.

SECURE DYNAMIC AUDITING AND SOLUTION

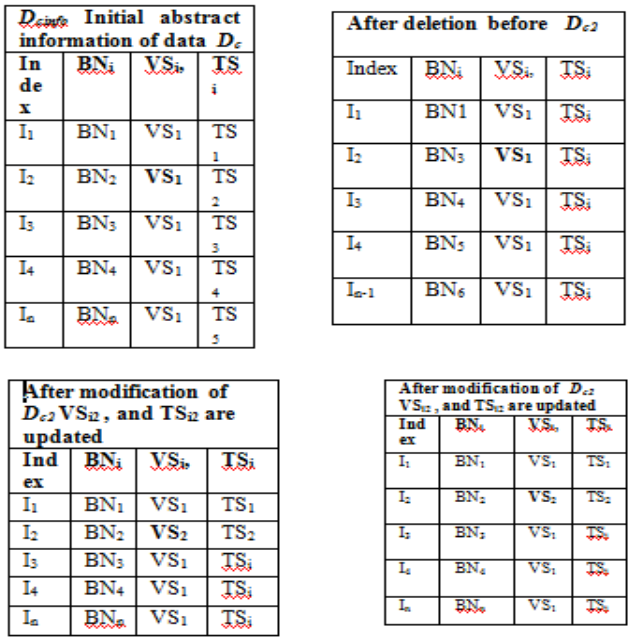
Data owner can dynamically update their data in cloud environment. In our proposed system the auditing protocol designs to support the static and dynamic archive data. Even though, the dynamic operation will formulate the auditing protocol insecure by conducting the *reply* and *forge* attack by the server. During the reply attack, the server fails to update owner data and he will use oldest version of the information to contact auditing. In case of *forge* attack the owner update the data to the current version and server may receive the information about forge data tag from dynamic operation by using this data tag he can pass auditing.

The solution for reply attack could be provided by introducing I Table which is used to record the abstract information about information tag. The I Table contains four major components such as, *index* component used to denote the current block number of the data clock DB_iin data components. BN_i it implies the unique block number of file content blocks and VS_i indicate the version number TS_idenotes the time stamp used to generate the data tag.

During the owner initialization Index table is created and managed by auditor. After completion dynamic operation, the data owner sends the update message to auditor for updating the I Table. Subsequent to the conformation meeting the auditor can send the result to data owner to ensure that owner data and abstract information on the auditor are both up to date. The above information completes the dynamic operation. In the case of forge attack, specially focus on modify the tag generation algorithm while generating the data tag $\boldsymbol{T_d}$ for each data blockB_t the data owner has to insert abstract information $\boldsymbol{D_{c\ info}}$in to data tag. These operations help server in getting sufficient information for to forge data tag for dynamic operation.

Dynamic Operation

In general the dynamic audit construction protocol having for phase such as owner initialization, conformation auditing, sample auditing and dynamic auditing. The major difference in this auditing protocol is *tag generation* and *index table* creation during the first phase (OI). In the following phase we discuss the DAP (Dynamic auditing Phase) which consist *Data update*, *Index update* and *Update conformation*.



D_{cinfo} Initial abstract information of data D_c

Index	BN_i	VS_i	TS_i
I_1	BN_1	VS_1	TS_1
I_2	BN_2	VS_1	TS_2
I_3	BN_3	VS_1	TS_3
I_4	BN_4	VS_1	TS_4
I_n	BN_6	VS_1	TS_5

After deletion before D_{c2}

Index	BN_i	VS_i	TS_i
I_1	BN1	VS_1	TS_i
I_2	BN_3	VS_1	TS_i
I_3	BN_4	VS_1	TS_i
I_4	BN_5	VS_1	TS_i
I_{n-1}	BN_6	VS_1	TS_i

After modification of D_{c2} VS_{i2}, and TS_{i2} are updated

Index	BN_i	VS_i	TS_i
I_1	BN_1	VS_1	TS_1
I_2	BN_2	VS_2	TS_2
I_3	BN_3	VS_1	TS_i
I_4	BN_4	VS_1	TS_i
I_n	BN_6	VS_1	TS_i

After modification of D_{c2} VS_{i2}, and TS_{i2} are updated

Index	BN_i	VS_i	TS_i
I_1	BN_1	VS_1	TS_1
I_2	BN_2	VS_2	TS_2
I_3	BN_3	VS_1	TS_i
I_4	BN_4	VS_1	TS_i
I_n	BN_6	VS_1	TS_i

Figure 5. Secure Process and representation

Data update

Data owner can perform three different way of operations such as Modification, Insertion and deletion. For every revise operation the corresponding process in dynamic auditing process which helps for future auditing phase to perform easy operations.

B. Modification $(DB_i, St_k Sh_k) \rightarrow (MG_{modify}, TS_i)$ the input to the algorithm is all latest version of information block DB_i, tag key St_k, and secret has key Sh_k and generate the new version number VN_i, new time stamp TS_i and new data tag DT_i for data cell DB_i which was generated using tag generation algorithm. This algorithm give the updated output as follows: MG_{modify} = (I, BN_i, VS_i,TS_i). Final its send the updated message to auditor and new set of data cell and tag should send to server.

C.Insert $(DB_i, St_k Sh_k) \rightarrow (MG_{modify}, TS_i)$it also take same parameter as input as same as modification algorithm. Then insert new DB_idata block before the i^{th} position and generate original data block DB_i, new version number VN_i , and Time Stamp TS_i. Next it uses tag generation algorithm to generate new tag DT_i for new data block $DB_i$and output the updated message as MG_{insert} = (I, BN_i, VS_i,TS_i). Now it can insert new data cell and tag as (DB_i, DT_i) on server and send the updated message to the auditor.

D. Delete (DB_i**)** $\rightarrow MG_{delete}$ This algorithm takes input as data block $DB_i$and output the updated message as : $MG_{delete} \rightarrow$(I, BN_i, VS_i,TS_i) after it delete the pair of data clock and tag (DB_i, DT_i) form the server and send the updated message to auditor.

D. Delete (DB_i**)** $\rightarrow MG_{delete}$ This algorithm takes input as data block $DB_i$and output the updated message as : $MG_{delete} \rightarrow$(I, BN_i, VS_i,TS_i) after it delete the pair of data clock and tag (DB_i, DT_i) form the server and send the updated message to auditor.

V. SECURITY ANALYSIS FOR PRIVACY PRESERVING PROTOCOL

Safety Analysis is significant process in cloud environment operation. In our proposed system we are prove that our auditing protocol can provide guarantee for data privacy under the security model. During the protocol design data privacy will be the important need in the cloud storage system. This could state as following theorem: In our proposed auditing protocol, during the auditing process neither server or auditor will obtain the evidence about data and secret has key.

IV.CONCLUSION AND FUTURE ENHANCEMENTS

Here we converse dynamic remote data auditing using privacy preserving protocol, which is used to perform the dynamic operation such as update, modify, insert and delete also provide the security over the data. We also tested our protocol with real data set in the cloud environment, result gives data integrity, and protect it from auditor. Next the security system model presented.

Safety Analysis is significant process in cloud environment operation. In our proposed system we are prove that our auditing protocol can provide guarantee for data privacy under the security model. During the protocol design data privacy will be the important need in the cloud storage system. This could state as following theorem: In our proposed auditing protocol, during the auditing process neither server or auditor will obtain the evidence about data and secret has key.

REFERENCES

[1]. M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: opportunities and challenges, Inf. Sci. 305 (2015) 357–383.

[2].Amazon.com, Amazon elastic compute cloud(Amazon EC2). [Online]. Available: http:// aws.amazon.com/ec2/

[3]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, Above the clouds: a view of cloud computing,Commun. ACM 53 (2010) 50–58.

[4]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," technical report, Nat'l Inst. of Standards and Technology, 2009.

[5]. T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010

[6]. W. Cong, R. Kui, L. Wenjing, L. Jin, Toward publicly auditable secure cloud data storage services, IEEE Netw. 24 (2010) 19–24.

[7]. S. Shamshirband, N.B. Anuar, M.L.M. Kiah, A. Patel, An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique, Eng. Appl. Artif. Intell. 26 (2013) 2105–2127.

[8]. T. Armerding, The 15 Worst Data Security Breaches of the 21st Century, in: COS Security and Risk, csoonline, 2012.

[9]. M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li, A.Y. Zomaya, SeDaSC: secure data sharing in clouds, IEEE Syst. J. PP (2015) 1–10.

[10]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, D. Song, Remote data checking using provable data possession, ACM Trans. Inf.Syst. Secur. 14 (2011) 1–34.

[11]. J.S. Plank, T1: erasure codes for storage applications, in: Proceedings of the Fourth USENIX Conference on File and Storage Technologies, San Francisco, 2005,pp. 1–74.

[12]. M. Sookhak, H. Talebian, E. Ahmed, A. Gani, M.K. Khan, A review on remote data auditing in single cloud server: taxonomy and open issues, J. Netw. Comput.Appl. 43 (2014) 121–141

[13]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing,"technical report, Nat'l Inst. of Standards and Technology,2009.

[14]. Q.A. Wang, C. Wang, K. Ren, W.J. Lou, J. Li, Enabling public audit ability and data dynamics for storage security in cloud computing, IEEE Trans. Parallel Distr. 22 (2011) 847–859.

[15]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, Provable data possession at untrusted stores, in: Proceedings of the fourteenth ACM Conference on Computer and Communications Security, ACM, Alexandria, Virginia, USA, 2007, pp. 598–609.

[16]. A. Juels, J. Burton, S. Kaliski, PORs: proofs of retrievability for large files, in: Proceedings of the Fourteenth ACM Conference on Computer and Communications Security, ACM, Alexandria, Virginia, USA, 2007, pp. 584–597.

[17]. D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures frombilinear maps, Advances in Cryptology (EUROCRYPT), Springer,Berlin Heidelberg, 2003, pp. 416–43

[18]. F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[19]. C. Erway, A. Kupc¸u, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[20]. C. Wang, S.S.-M.Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Cryptology ePrint Archive, Report 2009/579, http://eprint.iacr.org/, 2009.

[21]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Cooperative Provable Data Possession," Cryptology ePrint Archive, Report 2010/234, http://eprint.iacr.org/, 2010.

[22]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," IEEE Transl. J. Magn.Jpn., vol. 2, Aug. 1987, pp. 740–741 [Dig. 9th Annu. Conf. Magnetics Japan, 1982, p. 301].

[23]. M. Young, The Techincal Writers Handbook. Mill Valley, CA: University Science, 1989.

[24]. J. K. Author. (year, month, day).Basic Book/Monograph Online Sources) Title (edition) [Type of medium]. Volume(issue)Available: http://www.(URL)

[25]. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com

[26]. (Journal Online Sources style) K. Author. (year, month). Title. Journal [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)