Secure Auditing and Storage Systems in Cloud Service

PVNSLSSR Murthy, V. Khanaa, Venkata Naga Rani Bandaru, Abirami A

Abstract---Cloud is the one of the booming technology this era; cloud technology provides various storage services for the user, which is helpful on large amount of data maintenance and management.dd in this paper, we identify the issues of integrity auditing and storage security systems on cloud. Specially, seeking to achieve both auditing and storage in cloud in secure way, we are proposing a secure system, namely secClodud+ and using the dynamic data operation with portioning method the data are stored in the server. The performance of data storage and retrieval is securely done in proposed model. Implementation of the model is based on Improved Adaptive Huffman Technique that enables the access to the user to process the secure and efficient way of data. So that this improved Adaptive Huffman technique implements to store the data with the minimized time consumption, space and computational cost.

Keyword— Cloud computing, security, Auditing, secCloud+

I. INTRODUCTION

Cloud is an emerging technology over a universe. Majorly it is based on As A Service methodology [1], in this models so many cloud service providers they are offering various services to the public in cloud environment for example Software as a service, platform as a service, Infrastructure as a service, community as a service, Network as a service, Data as a service, security as a service and finally Analytical as a service. So based on the consumer requirement the service providers offering n number of services in the market. The major challenge in cloud is resource allocation, time and auditing.

Basically auditing is very important role in cloud environment because each and every service requester requests the service to the cloud service provider. By the request given from the user the service provider will allocate the service here the role of auditing is maintain the record details on Instance, Instance type, service period, status of the instance and cost. Another aspect security is a major thing in cloud, so many security models using in internet for example basic encryption and decryption [6], AES, DES, RSA,

DSA, ECC, Digital signature etc., these all type of security algorithm the aim is protect the data in local or global storage.

The third thing is compression and Decompression technique in compression process normally data is going to reduce the size without any data loss. In Decompression technique the compressed data is becomes an original size. While data compression it is like a encoding method in this method we are using Run Length Encoding (RLE), variable length encoding (VLE) and Huffman coding, In decompression method LZW is majorly used in maximum data processing.

The proposed system ensures flexible storage and effective a system auditing and also to make sure that the data correctness and data accessibility in cloud. Also it supports dynamic data and secure public verification of the server. with the security analysis. Using DASSS data loss and storage space is minimized.

II. RELATED WORKS

a. Cloud Auditing

Cloud auditing is done by trusted third party authenticator (TPA) [3]. The role of TPA is going to verify each and every moment of the user and cloud admin in the existing models. While user uploads any data in cloud storage [4] the process is running on the following steps,

- Data or workloads are divided into multiple data blocks [8].
- Each and every data blocks will be assigned with unique security key.
- Now the secured data verified by TPA the check the data is respective cloud user.
- If user is doing any operation that is update, append and delete at the instance TPA is going to verify the data.

These are the process and steps for TPA. While auditing the role of auditor is not only for verify the workload, auditor is going to check the instance details, cost details and everything.

b. Cloud Security

Security is the major issue in cloud computing environment because the consumer always depending on the third party authenticator in cloud computing environment [2]. Some cloud user having fear on their data or workload security in the cloud, because the data in their cloud may be viewed or edited by the third party authenticator (TPA). The proposed a cloud system called secCloud+, which is used for auditing and storing the data. The performance of data storage and retrieval is securely done in proposed model. Implementation of the model is based on Improved Adaptive Huffman Technique that enables the access to the user to process the data in efficient and secured way. So this

Revised Manuscript Received on 14 August, 2019.

PVNSLSSR Murthy, Assistant professor, Department of Computer Science, Sri Krishna Engineering College,Chennai, Tamilnadu, India, Email: murthythegenius@gmail.com)

Dr.V.Khanaa, Professor, Department of Information Technology, Bharath University, Chennai, Tamilnadu, India, (Email: drvkannan62@yahoo.com)

Venkata Naga Rani Bandaru, Assistant professor, Easwari Engineering College,Chennai, Tamilnadu, India(Email:ranivenkata5@gmail.com)

Abirami A, Assistant professor, Department of Computer Science and Engineering, Easwari Engineering College, Chennai, Tamilnadu, India.-89(Email: abiavsbtech@gmail.com)

Improved Adaptive Huffman process is used to minimize the time consumption, space and computational cost to store the data. The data will be encrypted using AES, DES, RSA [5], DSA, ECC, DIGITAL SIGNATURE before getting checked by the TPA for storing it in the cloud and using the same algorithm the data will be fetched from the cloud in a decrypted format for the consumer. This makes the consumer to fell that their data and workloads are secured in the cloud.

III. PROPOSED SYSTEM

In the cloud environment security is the one of the major issue. Most of the cloud user is afraid of their data security, because the cloud computing environment uses TPA for inter facing the cloud and users, the TPA agent will authorize the users to access their data or workload through internet.

So there is a chance that the TPA agent may view or edit the confidential data of the user. To over this issue we have proposed the security system for the cloud auditing and for storage service. The data are encrypted and decrypted using one of these algorithm, AES, DES, RSA, DSA, ECC, Digital signature etc., these algorithms are used to encrypt the data before storing it in the cloud. The original data will partitioned and the partitioned data will be encrypted and compressed, so that the time consumption is less and the TPA agent cant view the exact data of the cloud user, while user fetches the data, the data will be decrypted and decompressed in to original data with the same algorithm used for encryption and the original data is shown to the user. This security system makes the data more secure in the cloud environment.

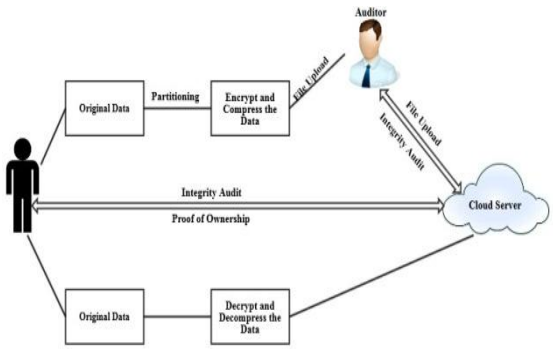

Fig 1. Secure cloud auditing architecture

A. Dynamic Auditing Secure Storage System

The Dynamic Auditing Secure Storage System (DASSS) shows the strategy of data access for enhancing the security system in the cloud environment and it helps to achieve the requirement give by the end user. The data auditing system is hosted using the TPA's data center by using the integrated checking process. If the data is larger it is complex to sort the data in the deficient data storage method. The data portioning techniques are used to reduce the provision time. For detecting the threats and give security for the cloud user dynamic remote data integrity method is implemented. This protects the data from the attacks and helps the cloud user to access the data in a secured way without any loss of data. Using the auditing technique in DASSS which helps to monitor the data which can be encrypted and used to audit the data and sent to the cloud server then data is decrypted and sent to the client. Cloud users can also get the data what they need to accessed and shared through the cloud to other users. Each and every time secured access is checked by the security system during the retrieval time of data. In DASSS compression and decompression techniques are used for storing the data in the cloud server with the time consumption, space and better performance and auditing has been done for the secure process. Auditing will provide the capability of verifying correctness of the remote stored data from the encrypted data. Two more features of integrity verification are required:

1) Public verification that allows the user to verify the stored data

2) Stateless verification which enables to eliminate the need for the state data maintenance at the verifier side between the auditing and storage of data.

In analysis of cloud and implementation of the proposed system is enhanced the storage and auditing of data in an efficient and effectiveness that is done in a secure way. An efficient data storage access in this system involves with the integrity check and storage time access control and computational cost are the parameter has been considered in this cloud environment. Implementing the DASSS in cloud environment provides secure and fast access of stored contents. As per the designed system the management and process of the cloud storage fetching system are verifying the secure access and the security for the user.

A Improved Adaptive Huffman CompressionTechnique

This technique is used to compress and decompress the secured partition data in a secure manner and easiest transaction; and secure storage process in the cloud environment is provided by this method. IAH coding is used for the better compression than the previous technique. The encoded data are compressed and stored in the cloud. This method makes the efficient storage space by compressing the encoded files so that the size of the data is minimized than the normal size. This method can be represented using tree structure.

Algorithm 1: Modified Huffman Technique

```
1: Procedure
2:  Input (A)
3:   while (A! =EOF) do
4: begin
5: if (compression mode)
6: compression (A);
7:       else decompression (A);
8: end
9: End Procedure
10: Procedure compression ()
11:       if (Input (A)) then
12:        while ((c=getc (A))! =eof)
13: begin
14: compression(c, output);
15: Update model (c);
16: end
```

17: End Procedure
18: Procedure decompression ()
19: While ((c=decompression (input))! =eof)
20: begin
21: putc (c, output);
22: Update model (c);
23: end
24: End Procedure

A Partitioning Techniques

It is complex to do the dynamic operation of storing the original data; to store the data in the cloud in an efficient way partition technique is used. The partitioned data were encrypted and compressed for storing the data in the cloud. To retrieve the original data the data in the cloud is merged decrypted and decompressed so that this method will make the system to store the data in cloud in an efficient and easy way.

Algorithm 2: File Partitioning

1: Procedure
2: Let threshold = "A-Size"
3: Compute srcsize = sizeOf (A)
4: if (srcsize<= threshold) then
5: Compute Px: = SrcSize div TargetSize;
6: if SrcSize mod TargetSize> 0 then
7: Inc (DestFileCount);
8: PX(A); – Splitting Files
9: store "PX"
10: exit (0);
11: close (A);
12: else if (srcsize>threshold) then
13: Write "File size is greater than file size"
14: exit (1);
15: end if
16: end if
17: End Procedure

B. Sec Cloud+

The public and private keys were initialized in the Sec Cloud by the auditor. The key server picks the random key for the security of the file in the cloud, further the file encryption key is generated and the cloud user is assigned with the generated key for the encapsulating the file in the unique way. The three protocols used in the Sec Cloud+ were described using the initialized parameters. This is been analyzed in a sec cloud and sec cloud+ which is used to tell about the secure and safety in the cloud server. It is worthwhile noting that,

- We take advantage of the idea of convergent encryption to make the deterministic and "content identified" encryption. In this way, different "contents" would result in different cipher texts, and reduplication works.
- Convergent encryption suffers from dictionary attack, which allows the adversary to recover the whole content with a number of guesses. A "seed" (i.e., convergent key seed) is used for controlling and generating all the convergent keys to avoid the fact that adversary could guess or derive the convergent key it is just from the content itself.
- We generate convergent keys on sector-level for the security process (i.e., generate convergent keys for each sector in file F), to enable integrity auditing system. Specifically, since convergent encryption is deterministic, it allows computing homomorphic signatures of the encrypted data as with on plain data, and thus the sector-level integrity auditing is preserved from the cloud network. The convergent keys are encapsulated by client's secret key ckand directly stored at the cloud servers.

IV. IMPLEMENTATION AND RESULT

The implementation of DASSS is based on cluster system is based on 4 node and master node is act as a private cloud another slave systems are act as a client in the working environment. For private cloud we use Open stack private cloud environment and the system configuration is master node 8GB RAM, i7 processor. Salve node 4GB RAM with i5 processor. Based on the complexity effectiveness and efficiency the input for the proposed system was evaluated. DASSS uses splitting file system for storing and auditing the data, for security purpose the data uses partitioning file system for storage and auditing the data, security and IAH technique coding is used for compressing the files and storing the data in cloud environment with the RSA double encryption algorithmFig.2 shows the working model of proposed system.

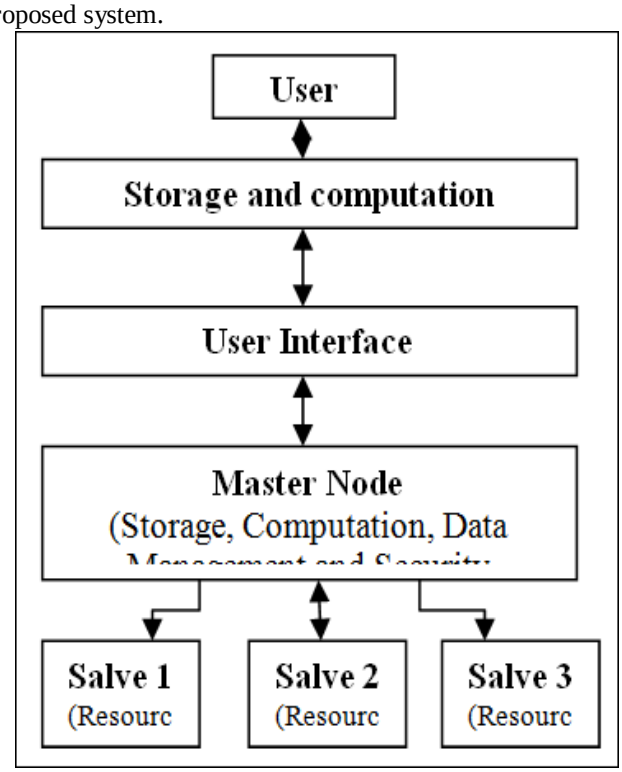

Fig 2. Working model for proposed system

A. Improved adaptive huffman technique analysis

The improved adaptive Huffman technique is used to compress and store the data in the cloud, a secured process is provided by this technique for data manipulation. Time consumption is minimized for retrieving the data from the cloud and manipulation on data is easier.

B. Partitioning technique analysis

This portioning technique makes the cloud storage very efficient and the compression is performed based on the existing system provides efficient data storage in cloud with improved performance which makes in a less time and cost effectively. User client data is partitioning into multiple data blocks based on proposed algorithm.

C. File Auditing

The time taken for file auditing in the cloud should be analysed first to identify the issues in our integrity auditing protocol which makes to data store in an easiest and orderly manner. If some of the files correpted in the cloud using the verifiedr we can easily detect thed misdbehavior of the cloud data. The file auditing system demonstratdes that to achive the high medium and low confidence of detecting the corrution in the cloud data.

The result for the proposed algorithm we compared with the existing aldgorithm based on File size , uploadeing speed and uploading time.table 1 is showing the comparison of whaile user upload a workloads based on with security guarantee and without security garentee. If the file size increases the uploading speed of the secured data will increase periodically, the uploading speed of the unsecured data is increased unperiodically if the file size increases.

Table 1. System Performance in Data processing

File size(MB)	Uploading speeed (Mb/s)with security	Uploading speeed (Mb/s)without security
50	10	13
75	15	18
100	20	28
125	25	18

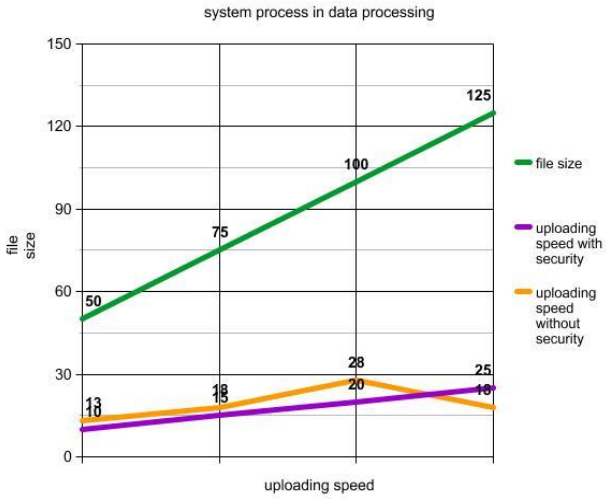

Fig.3 Performance of with and without security in cloud

Fig 3 Shows The Output Performance For File Uploading In A Cloud Environment While Uploading A File With Security And Auditing Process For Example 50MB File Is Going To Upload In Cloud It Was Take 10MB/S If It Is Without Auditing And Security It Will Take Around 13 Mb/S So Here The Proposed Methodology Comparatively Very Efficient Performance In Existing Methodology.

V. CONCLUSION

We have proposed a method for secure encoding auditing method in cloud environment in this paper. This work is collaboratively considered as data storage, data partitioning and secure cloud processing. We have define a new approach based on secure auditing it is comparatively improve the performance of data uploading, downloading, resource sharing in the proposed methodology. Without any data loss the secured access performance control, efficiency, minimized storage space and minimum time access without any data loss are provided by overall performance of the DASSS work. The proposed system reduces the complexity of the storage process in the cloud and flexible access is provided t the end user. In future we are plane d to improve the security level of the cloud environment and efficient retrieval of data from the cloud server is improved. Also reduce the compression ratio for the efficient storage space provision.

REFERENCES

1. Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A New Approach for Privacy Preserving Data Publishing," Knowledge and Data Engineering, IEEE Transactions on, vol.24, no.3, pp.561-574, March2012.
2. Wang Cong, Wang Qian, RenKui, Cao Ning and Lou Wenjing, "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220-232, April-June 2012.
3. Jingwei Li, Jin Li, DongqingXie and Zhang CAI,"Secure Auditing and Deduplicating Data".10.1109/TC.2015.2389960, IEEE Transactions on Computers.
4. G. JeevaRathanam, M.R. Sumalatha,"Dynamic secure Storage system."978-1-4799-4989, 2014 IEEE
5. Nagar, S.A.; Alshamma, S., "High speed implementation of RSA algorithm with modified keys exchange," Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on , vol., no., pp.639,642, 21-24 March 2012.
6. Wang, Suli; Liu, Ganlai, "File Encryption and Decryption System Based on RSA Algorithm," Computational and Information Sciences (ICCIS), 2011 International Conference on, vol., no., pp.797, 800, 21-23 Oct2011.
7. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and CommunicationsSecurity, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.
8. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 12:1–12:34,2011.
9. J. Douceur, A. Adya, W. Bolosky, P. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file ystem,"in22nd International Conference on Distributed Computing Systems,2002, pp. 617–624.
10. M. Bellare, S. Keelveedhi, and T. Ristenpart, Message-locked encryptionand secure deduplication," in Advances in Cryptology – EUROCRYPT2013, ser. Lecture Notes

in Computer Science, T. Johanssonand P. Nguyen, Eds. Springer Berlin Heidelberg, 2013, vol. 7881, pp.296–312.

AUTHORS PROFILE

1.PVNSLSSRMurthy,,M.E,(PhD), Assistant professor Department of Computer Science,Sri Krishna Engineering College.Papers published :12 International Conferences,20 National Conferences,5 International Journals published.

Author-2 Photo

2.Dr.V.Khanaa,,,M.E,PhD, Department of Information Technology ,Bharath University.

3.Mrs.Venkata Naga Rani Bandaru ,M.E, Assistant professor, Department of Computer Science and Engineering, Easwari Engineering College, Chennai-89, Papers published :12 International Conferences,20 National Conferences,5 International Journals published.

.4. Mrs.A.Abirami,M.EAssistant professor, Department of Computer Science and Engineering, Easwari Engineering College, Chennai-89, abiavsbtech@gmail.com