A ADVANCE DATA SECURITY APPROACH OVER CLOUD COMPUTING & DATA AUDITING

Amit Tiwari1 and Raj Kumar Paul2

1 Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal (M.P.)

2 Head Of Department, Department of Computer Science and Engineering, Vedica Institute of Technology, Bhopal (M.P.)

Abstract: ***Cloud computing technique is recent trend of use which claims to the fastest computing for data and a secure storage. This algorithm also claims its low computation cost as it ask for pay as used model. Cloud computing environment give flexibility to user for the requirement fulfill for any computation on demand. According to cloud experts they say Cloud computing era is the recent trend in data storage and computing at other end in IT market where cloud provide a reliable and fast computing. Cloud are ease to access and various security encryption techniques been added to the cloud. The available architecture which contain 3 layer architecture which provide a best security model among the tradition storage technique. Security technique is recently used encryption technique where data store in encrypted form which can be unpack by the original user towards the data scheme. An efficient auditing and hashing technique such as CP-ABE been introduced by the several research article. In this paper, discuss about the various technique used in this era and the proposed dynamic auditing can be perform in cloud computing for ensuring the data integrity.***

Keywords: ***Cloud analysis, security approach, CP-ABE, Hashing algorithm, Cloud auditing, Security layer.***

INTRODUCTION:

Cloud computing is a domain for computing large data input and processing it with its available component. Cloud computing having different model of computation which help in accessing data with load balancing, data security and virtualization process among [6, 7]. Cloud computing having models which related with the software as a service, infrastructure as service and platform as a service. All these three different model exhibit different processing steps. Cloud computing models describe the process which provides the information of data flow and its execution manner. Data security is the important role in cloud which ensure user with its safe data usage and integrity.

This paper focuses on storage domain security for the data. In this a huge amount of data shared over internet. In cloud a storage mechanism is provided for the user to store their data over cloud. But there are many threats and issues are there, in which an unauthorized user want to access data which contains private information of the user. Thus security mechanisms are required for that data. In [4] a shared

authority based privacy preserving technique is resented. In this technique an encryption technique and universal composability model is used to provide security for the data during when more than one protocol merged together. In [5] a data coloring technique and software water marking technique is presented to provide security for data shared over cloud and some other techniques are presented in the literature which provide an brief overview to the security technique which are used for storage security in the cloud.

RELATED WORK:

Hong Niu, HuanshengNing, QingxuXiong[1], in this paper a share authority privacy preserving protocol is presented which resolves issues in the existing system like loss of data during process and take too much time to authenticate user and there is no provision for privacy of private data but in this system, a feature based authentication protocol is used to authenticate user and an anonymous access matching mechanism is used which not allow any un authorized user to access content and a proxy re-encryption is used in which user can further encrypt data to enhance security of the system and share data over the cloud. In this system user can independently access their data without any external interferences and can easily access cloud server to audit their personal data with shallow communication overhead and cost. In this system a universal composability model is presented which preserves the security of the data when one protocol merges or composes with other protocol.

But in this technique data is encrypted by the static symmetric key encryption which is vulnerable to guess by an unauthenticated user to resolve such problems, a random dynamic key based technique is presented for future to enhance the security of the data.

Kai Hwang, Deyi Li [2] author presents paper in which coloring technique over the document which provide the watermarking and further security enhancement over it. Cloud computing data security using the document masking using color, using document masking with its feature impact process is provided. Software generation module is applied which is document stream encryption with the presented technique by author.

L. A. Dunning and R. Kresman [3] author of this paper presented an ID allocation approach on the document which is processing by the system. Document processing which help in id allocation to the data and encrypting the data accordingly. Further data storage, processing, encrypting and accessing is taken by the process applied in it. Data security process usage is given in this approach.

N. Vaitheeka, V. Rajeshwari, D. Mahendran[13] propose an object oriented approach is for signing in mechanism is used to provide access to the intended user and thus an authorized user can access that data, and one time password (OTP) based method is used to encrypt data and provide access data in existing system there is no system for granting or invoking data access is there so enhance the security as compare to the existing system.

PROBLEM FORMULATION & PROPOSED WORK

In order to prove our best among the available recent algorithm taken combination is of recent encryption technique for data security storage and further hashing function technique CP-ABE is using for the dynamic integrity verification process [10,11].

CP-ABE contains the key length of 256 bit which is not breakable with the brute force attack system which is the key main point of the hashing scheme, also the MAC security provided in case of encryption where the highest number of security is being transformed. Our proposed work aims to provide a high security combination approach while dealing with the cloud security approach, as the general method either work with the security encryption or hashing data verification technique. Thus our proposed work implied which work on both the area as a algorithm where the data hash value is calculated at the time of implementing encryption and data storage performance into the cloud data center.

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

EXPERIMENT SETUP & RESULT ANALYSIS

In order to perform simulation experiment evaluation, An apache JSP framework along with Wamp Server is setup on Ubuntu 16.x Machine [9]. This setup having 8 GB RAM and 1 TB of Hard disk with i7 processor. The experiment carried out with different data statistics and different size of file with different experiment user. Below are the results which are executed and observed during the scenario of experiment.

Algorithm PsudoCode :

Input: Data packet, receiver address.

Output: encryption evaluation, access management, result evaluation.

Algorithm Begins:

Receiving user input packets();

If(data packet received)

{

Packet transmission ();

Permission access();

Datasecurity ();

SigCP-ABE();

EndIf;

}

If(Access==Allowed)

{

Data permission access;

Rightsmanagement();

Fileshare();

}

EndIf;

}

The figure below represent the complete flow of the proposed scenario which represent our work and computes parameters efficiently.

RESULT ANALYSIS:

Inputs: There are different data file formats which used for input processing and data storage over the cloud component designed by us. Input data files for storage which is of large size file ranging 200 MB to 3 GB.

Outputs: Data outputs of secured encrypted manner, effective data management, auditing and accessing mechanism is applied. Further computation time, computation cost is computed over the processed data system.

Computation Time (parameter name): A computation time of a data processing in Java is computed with the help of start and end time class, difference between both the time.

File Upload Size(in MB)	Computation time (in ms) Existing algorithm	Computation time (in ms) Proposed algorithm
File 1- 250 MB	359	238
File 2- 750 MB	887	529
File 3- 1000 MB	816	504

Table 1: Comparison analysis between existing and proposed approach

In the table 1 above, it shows the computation time uploading different data and time taken to process them. The proposed algorithm executed shows the efficiency of our proposed approach over existing scenario.

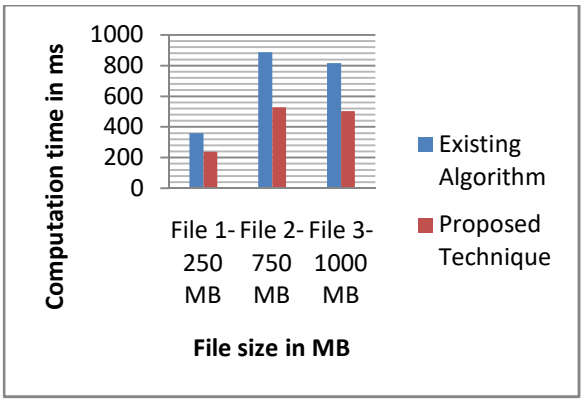

Figure 1: Comparison graph analysis between existing and proposed approach.

In the figure 1 above, an line graph is plotted between existing security algorithm and proposed algorithm.

The experiment result shows the efficiency of our proposed work over existing work scenario.

File Upload Size(in MB)	Computation cost (in INR) Existing algorithm	Computation time (in INR) Proposed algorithm
File 1- 250 MB	652	252
File 2- 750 MB	1104	987
File 3- 1000 MB	1430	1121

Table 2: Comparison analysis between existing and proposed approach

In the table 2 above, it shows the Computation Cost uploading different data and time taken to process them. The proposed algorithm executed shows the efficiency of our proposed approach over existing scenario.

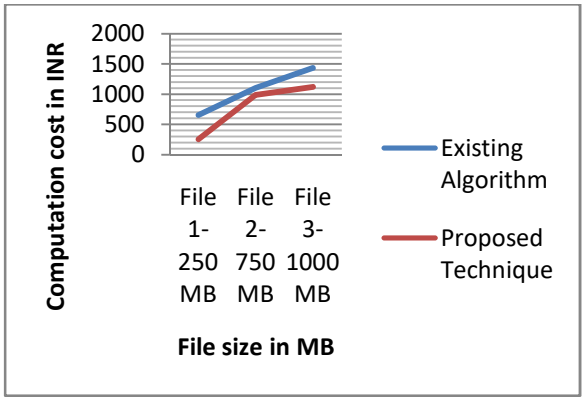

Figure 2: Line graph of computation cost in INR between existing and proposed technique.

The figure 2 above shows the line graph comparison to understand the cost estimation between both the presented approach.

CONCLUSION & FUTURE WORK

In this work, we have discussed about the different work been done in order to share data in between multiple authority and data authentication. Our contribution is to investigate different encryption protocol and again to work on the symmetric key based algorithm which is more privacy preserving. Also as the data is being shared in multiple users, a batch auditing process using signature or hashing based mechanism may introduce in order to maintain authenticity of data. Our further work will be in order to find a enhance privacy preserving symmetric key algorithm for the authentication scheme, whereas the existing technique use single authentication scheme which can further enhance using a key based authentication, proxy based re-encryption can further enhance to verify the loss of data and to resist anonymous access or attack and to perform batch auditing in user data. A further work to apply similar approach over mobile computing can be performed.

REFERENCES

[1] Hong liu, HuanshengNing, QingxuXiong, Laurence T. yang " Shared Authority Based Privacy Preserving Authentication protocol in cloud " IEEE Transactions on Parallel and distributed system Vol. PP NO:99, 2014.

[2] Kai Hwang, Deyi Li "Trusted cloud computing with secure resource and Data Coloring" IEEE 2010.

[3] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[4] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi Owner Data Sharing for Dynamic group in the cloud" IEEE Transactions on parallel and distributed system, 2012.

[5] SlawomirGrzonkwoski, Peter M. Corcoran "Sharing cloud service: User Authentication for social Enhancement of Home networking" IEEE Transaction on consumer electronics, Vol. 57, No. 3, August 2011.

[6] Kan yang, XiaohuaJia "An efficient and secure dynamic auditing protocol for data storage in cloud computing" IEEE transactions on parallel and distributed system, Vol. 24 No. 9, September 2013.

[7] Quin Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li "Enabling public auditability and data dynamics for storage data in cloud computing" IEEE Transactions on Parallel and distributed system, Vol. 22 No. 5, May 2011.

[8] C. Wang, Q Wang, K. Ren, N. Cao and W.Lou "Towards Secure and dependable storage service in cloud computing" IEEE Transactions on service computing Vol. 5, No. 2, 2012.

[9] Huaqun Wang "Proxy provavle data possession in public clouds" IEEE Transactions on service computing, Vol. 6 No.4, October-December, 2013.

[10] T. Nalini, K Mnivannan, VaishnaviMoorty "Efficient Data possession checking in critical information structure Ensuring Data Storage security in cloud" IJIRCCE, March, 2013.

[11] Xiaosong Lou, Kai Hwang "Collusive Piracy Prevention P2P content delivery network" IEEE, July 2009.

[12] Madhumita S Patil, Santosh Kumar" Study for Enhancement in privacy preserving authentication

protocol using third party in cloud" IJEEM, Vol 3 Issue 1, 2013.

[13] N. Vaitheeka, V. Rajeshwari, D. Mahendran "Privacy Preserving By Enhancing security In Cloud" IJIRCCE, Vol. 3 Issue 3 March 2015.

science of engineering department of Vedica Institute of Technology Bhopal, India. He received his Master degree in computer science from the MCU Bhopal, India in 2014. His research include in advance security in cloud computing and data auditing

Raj Kumar Paul is working as Head Of Department in CSE department at Vedica Institute of Technology, RKDF University, Bhopal, India. His areas of research interest include localization, in advance security in cloud computing and data auditing