Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 9, September -2017

A ADVANCE DATA SECURITY APPROACH OVER CLOUD COMPUTING & DATA AUDITING

[1]Akanksha Mehta, [2]Atul shriavastav

[1,2] *Department of Computer Science, Sagar Institute of research and technology-Excellence Bhopal*

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 per use model. Cloud computing environment give flexibility to user for the requirement fulfill for any computation on demand. Cloud computing concerned security is derived with proposed security framework algorithm which concentrate for secure data distribution. In this paper an approach which is Blowfish based security technique is given. SHA-2 used for the secure hash generation and thus creating hash value for the given data inputs. Proposed techniques is implemented using Apache java server and shows the efficiency in terms of comparison computation parameters.*

Keywords: *Cloud analysis, security approach, ECC, Hashing algorithm, Cloud auditing, Security layer.*

INTRODUCTION

Cloud computing is framework which provide on-demand resource and application for the user. Cloud computing offers on demand services to the user such as Software as a Service (SaaS), Platform as a Service (Paas), Infrastructure as a service (IaaS). Thus it gains huge popularity for cloud computing. But security for that data is major issue in cloud computing, in [6,7]a security framework is presented in that an on-demand security architecture for cloud computing. In this architecture three layers are there one is input layer, second is policy layer, and third layer is security mechanism layer. In input layer three checks is performed first is security level, in this only authorized user can be allowed to access the service unauthorized user doesn't have permission to access data. Second is type of service, in this, what type of service user want to access is checked because different type of service needs different security. Access network risk, in this the risk when service passes through the server is checked. Security policy in this layer data is checked and security parameters are implemented on the basis of security level, type of service, access network risk. Third layer is security mechanism layer, in this each domain provides different security mechanism, like encryption/decryption in storage domain, IP security in the network domain, honey pot in service domain.

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

@IJAERD-2017, All rights Reserved

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] presents a data data sharing and storing of the digital document using the digital encryption technique. This technique help in data security with enhanced parameter with the data integrity solutions. Data access and secure storage is given in the paper work.
They have worked with image data, its compression and conversion approach. Further a security is applied over the given scenario [3].
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 SHA-2 is using for the dynamic integrity verification process [10,11]. SHA-2 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 SHA2 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 SHA-2 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.

RESULT ANALYSIS

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.

Technique Approach	**Existing Algorithm(Computation time in ms)**	**Proposed Algorithm(Computation time in ms)**
100 KB	400	372
500 KB	1340	1121
1 MB	3920	3600
2 MB	5730	4674
5 MB	9765	8788

Table 1: Comparison analysis between existing and proposed approach

@IJAERD-2017, All rights Reserved

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.

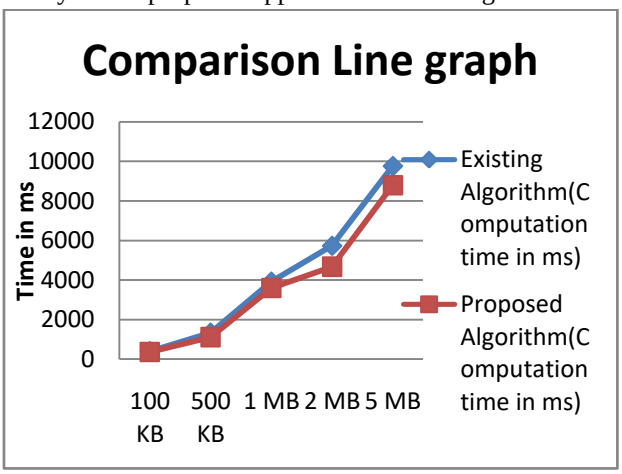

Figure 1: Comparison graph analysis between existing and proposed approach.

In the figure 1 above, an line graph is plotted between existing security algorithm and proposed algorithm. The experiment results shows the efficiency of our proposed work over existing work scenario.

Technique Approach	**Existing Algorithm(Bandwith Kbps)**	**Proposed Algorithm(BandwithKbps)**
100 KB	256	275
500 KB	226	259
1 MB	178	198
2 MB	156	173
5 MB	143	158

Table 2: Comparison analysis between existing and proposed approach

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

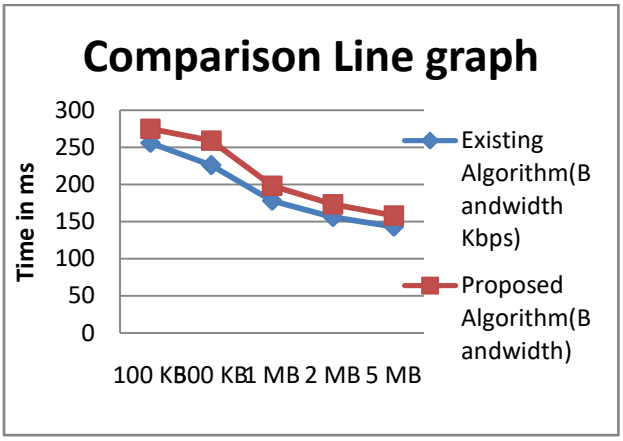

Figure 2: Comparison graph analysis between existing and proposed approach.

@IJAERD-2017, All rights Reserved

In the figure 2 above, an line graph is plotted between existing security algorithm and proposed algorithm. The experiment results shows the efficiency of our proposed work over existing work scenario.

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.

@IJAERD-2017, All rights Reserved