Scientific Journal of Impact Factor (SJIF): 5.71

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

International Journal of Advance Engineering and Research Development

Volume 5, Issue 02, February -2018

AN Optimal Matrix Approach for virtual load allocation and data sharing

Lavleet Kaur, Atul Shrivastava

[1]Department of Computer Science and Engineering , SIRTE, Bhopal, India
[2]Department of Computer Science and Engineering, SIRTE, Bhopal, India

Abstract: *Distributed technology which means to the cloud is commonly used service today for many industries as well as personal level. Users are utilizing the cloud service, its model for reliable and secure storage for their data. All the cloud service provider gives inbuild algorithms, which help in providing data security, integrity verification as well as ease of access utility. Different level of security and accessing mechanism for the range of user is provided. Cloud computing having an architecture which gives an advantage than the tradition approach. Previous approach of security over the cloud face challenging issues such as high computation time, low level of encryption key in use. This approach lacks in modern attack defense which usually occurs over the network. In order to prevent these attack and data misuse an efficient storage, security and accessing mechanism over the data storage is required. In this paper a proposed for the data security algorithm and access mechanism for the user data is given. This paper also depicts the implementation of algorithm, its proper working model as well as the efficiency of algorithm. The proposed algorithm is implemented and compared with traditional security techniques. Results were observed by giving multiple user input files. Monitored results shows the low computation time, cost as well as high resistance over the input file attacks.*
Our further work is going to run towards finding its real time application usage and providing an open source platform for the user for public use.

Keywords:*Cloud distributed technique, Security technique, accessing mechanism, cloud application, data monitoring & verification.*

I. INTRODUCTION

Cloud computing is an emerging platform which replace the current data storage standards [1]. Cloud help in proper configuration of server related component such as data center, virtual machine, processing unit, RAM and other sub unit which participate in communication. In order to identify the utilities and usage of cloud, there are some different models according to user need is given in the system. Cloud computing having the different model according to industry and type. Cloud environment model is differentiated in terms of providing service as infrastructure, software platform for end user, providing some set of configuration for end users [2-4].

Cloud is having different models:
In any basic level there are three models are given which is IaaS – vendors providing infrastructure to business owners, SaaS –software providing company for N users and public use, PaaS- platform software providing for business owner to run their software services.

SAAS (Software as a service): These are the platform such as slack, Google, mail platform and other software units which are directly involve to provide services to the user. Software services for the public problem solution are best practice here. Software as a service is a common model today, where anyone can find using it [5].

IAAS (Infra as a service model): There are vendors which provide infrastructure facility for the data storage or accessing system. They provide the hosting service, virtual machine, system configuration on demand. These configured services further can be used by the end user business or individual entity.

PAAS (Platform as a service model): These are the vendors who are providing a set of installed software for the other software owner's use. Platform provides the software such as apache or some data base which can be used by the third party users to install and deploy their software.

The more common types of services include:

Security: Data security and usage of security component for the cloud is an important aspect. Here a security algorithm is applied on the users data to provide them security. A encryption approach and dynamic security system is implemented over the cloud, which help in getting user trust for cloud use [6].

Data Accessing: Accessing mechanism for the user data is technique which builds for fast and reliable access. A access mechanism for users data in fast, index and efficient manner is always applied on the cloud. This is the approach which also differentiates cloud from the normal server [7].

A Cloud computing platform is an openly entity unit, which can be use according to industry and personal need. A self configuration environment makes it enable for N user to use with high productivity [8].

II. RELATED WORK

This section discuss about the related work in the field of cloud computing. Cloud component communication, security mechanism and access control provided by the previous approach is discussed in this section.

The author of the paper [2] proposed technique in which they have described about the technique for cloud and data security and majorly they have highlighted the big data storage capacity in a cloud computing environment, they have proposed a secure k-means data mining approach assuming the data to be distributed among different hosts preserving the privacy of the data. The approach is able to maintain the correctness and validity of the existing k-means to generate the final results even in the distributed environment. An approach to mine the data securely using k-means algorithm from the cloud even in the presence of adversaries. Their approach assumes that the data is not stored in a centralized location but is distributed to various hosts. This proposed approach prevents any intermediate data leakage in the process of computation while maintaining the correctness and validity of the data mining process and the end results.

They have measure the results and shown the effectiveness of their system by correctness and security terms of their proposed scheme and concluded by their scheme system can be more effective in security and correct data storage scheme compare to other available techniques in cloud computing.
There are existing approach which find several challenges and units which focused on the cloud security , access mechanism for internal component communication[9-11].
Few challenges which focused on the security, as well as the phases involved in the encryption system is discussed. Majorly observed challenges are depicted here:

They perform access sharing technique for large data and hence following problem formulation is found in the past work.

1. The existing work exhibit only single level of data encryption.
2. Single level of data encryption can reveal by single level decryption mechanism.
3. Data access and performing access rights is also need a privacy preserving approach.
4. The multi-level encryption technique makes use of proposed architecture which is lacking in existing any of the security approach.
5. Data auditing mechanism is low and having single level of process.
6. Batch auditing concept is not introduced along with matrix encryption solution.

III. PROPOSED METHODOLOGY

As the previous approach , their security model steps and further alternate over the previous security approach is given by our system. The proposed system algorithm is discussed here, which shows the steps behind our proposed work and its use. Our flow diagram and other component mechanism show the execution process.

Proposed methodology architecture:

The proposed method architecture is shown below in figure 2, which shows the component and their interaction communication platform.

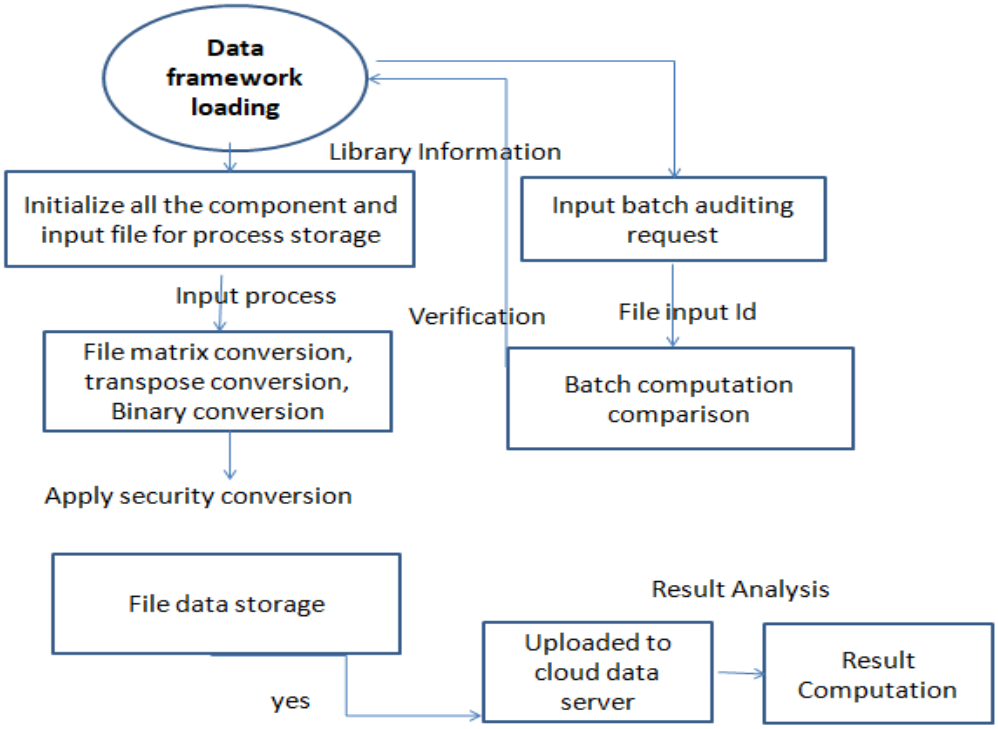

Figure 2: Proposed methodology architecture

The proposed methodology architecture shows the components and their interaction flow. It shows the efficiency of proposed architecture communication.

Algorithm Pseudo Code: Algorithm for advance matrix based security approach is performed with following Pseudo code architecture. A detail Pseudo code architecture is presented here.

MatSHA Approach-

Dynamic Matrix SHA-2 Approach:
Input: File f, Data centre DS, Matrix init, Plain text, Key.
Output: Matrix process, Cipher text, Computation time.
Steps:
Load Matrix initials;
For Each file(i-n)
{
File Load inputs();
Cipher Text Return();
}
Send VerReq(FileID);
Sha2= SHA2(CipherText);
ProofGen(sha2);
If(Match==true)
{
File verified return 1;
}
Else

{
Return 0;
}
Group key sharing();
File access();
Return Computation time;
}
End.

A proposed algorithm and presented architecture shows the proposed perform approach which is presented by our research work algorithm.

An effective and flexible scheme is proposed in our paper. And with the proposed scheme we have fallowing advantage:

- Eliminates the burden of extra computation required by previous scheme.
- Uses cryptographic Hash Function SHA-2 which is more secure than the mapping hash function used in previous paper.

Efficient Encryption approach

IV. EXPERIMENTAL SETUP

In order to perform experiment and setup analysis a framework is designed using the Jsp pages. An apache local server is configured with the file storage and data storage system. Here different component setup and simulation is performed with the given among proposed system architecture.

A further setup is performed using Java API, Apache configuration over the machine of i3 processor, 4 GB of RAM and 1 TB of HDD which gives an efficient processing.

V. RESULT ANALYSIS

As the experiment setup is performed with Java API framework using Apache Server API. The existing and proposed algorithm is experimented and results over the experiment are observed. Dataset process is performed and following parameter results were observed.

Computational Cost: Computational cost is the total cost obtained by the computational resources. Computational time shows the total cost take to process the data request.

Computational Time: Computation time is the process execution time which taken by the server to execute dataset. A difference between time finished and time request initialized is computed as computational time.
Ct = finalize processing time – initializing processing time.
Statically Results: Here a result observed in experiment shows the computation performed. In the table 1 below, an observation is made over the given dataset with the existing greedy based technique, also the proposed technique MatSHA is observed in table 2 and following results are observed.

Algorithm computation	**Existing Computation time (ms)**	**Proposed computation time (ms)**	**Existing technique Decryption time (ms)**	**Proposed Technique Decryption time(ms)**
File 1	**13**	**11**	**11**	**9**
File 2	**12**	**10**	**10**	**8**
File 3	**8**	**6**	**6**	**4**

Table 1: Computational parameter result observed with existing algorithm

In the table 1 above, it shows the experiment and result observed from the performed greedy approach. It shows the experiment result in 4 parameters.

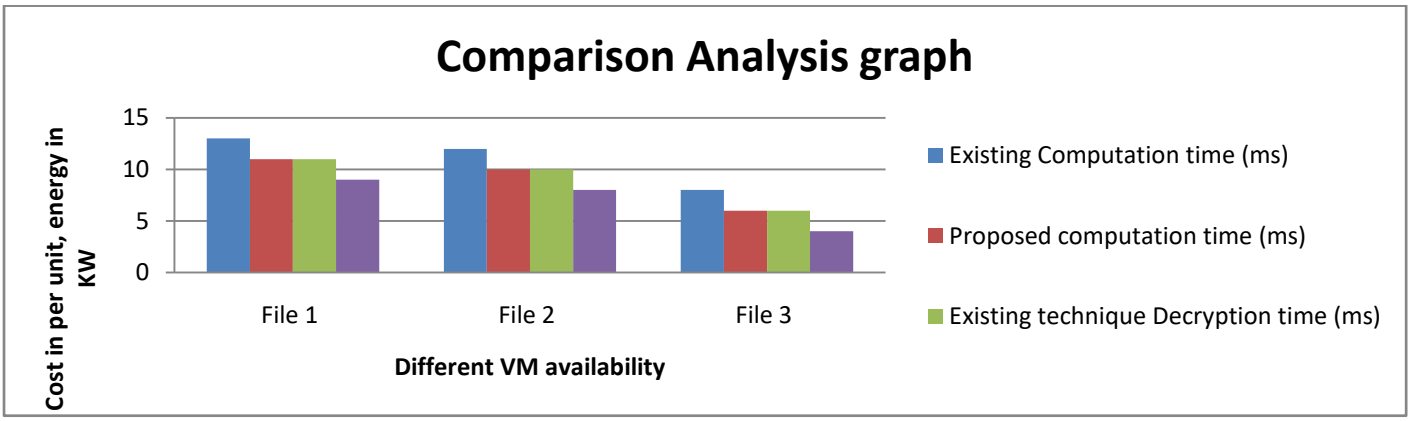

Figure 3: A comparison graph between the given parameters.

In the figure 3 above, a comparison graphical analysis is performed which shows the efficiency on computational cost of our proposed technique over existing greedy approach.

VI. CONCLUSION & FUTURE WORK

Cloud computing and security parameters over the cloud are important aspect in communication. Data storage, data accessing is the key usage of any cloud or server. Cloud computing provides the process architecture which include virtual machine and data center , as well as communication algorithm in between them. A security technique which uses the encryption key and conversion to a secure form is also a important process. In this paper our proposed MatHash approach is described. This technique help in data processing through a security platform, processing the data with its secure usage, proper access mechanism is given. Our further work is going to apply the proposed technique in which help in applying it over real time usage and over the mobile application network.

VII. REFERENCES

[1]. Deepti Mittal, Damandeep Kaur, Ashish Aggarwal The author of the paper entitled “Secure Data Mining in Cloud using Homomorphic Encryption”, IEEE conference 2014.

[2]. Xingliang Yuan, Xinyu Wang, Cong Wang, “Enabling Secure and Fast Indexing for Privacy-assured Healthcare Monitoring via Compressive Sensing”, IEEE 2016.

[3]. Feng Zhao , Chao Li , Chun Feng Liu, “A cloud computing security solution based on fully homomorphic encryption, IEEE conference 2014.

[4]. Deepti Mittal, DamandeepKaur, AshishAggarwal The author of the paper entitled “Secure Data Mining in Cloud using Homomorphic Encryption”, IEEE conference 2014.

[5]. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73,2012.

[6]. Qian Wang, Cong Wang, KuiRen, Wenjing Lou, Jin Li,” Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011

[7]. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10,2008.

[8]. C. Wang, B. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

[9]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), 2009.

[10]. K.D. Bowers, A. Juels, and A. Oprea, "Hail: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), pp. 187-198, 2009.

[11]. D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from theWeil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), pp. 514-532.

