Data security and access control mechanism using Data security algorithms

Lavleet Kaur[#1], Atul Shrivastava[*2]

[#]*CSE Department, SIRTE, RGPV University*
Bhopal, India
[1]lavleetkaur@gmail.com

[*]*Assistant Professor, SIRTE, RGPV University*
Bhopal, India

Abstract: Data sharing platform find its unique concept of keeping the same copy and sync operation in between the files data. Cloud computing environment make it usable which work towards the data sharing with security. Access based control and providing security over the data is being performed by different research author. Algorithm such security improves the data complexity but still it out performed with single step encryption with single data key. A further study is performed here is survey of previous technique and our proposed multi-step approach to deal with large data storage and multi-phases security over it. Matrix defined steps to encrypt the data in multiple stage is defined here along with access based control over the cloud data. Our further investigation is going to perform research to apply technique over cloud environment and data sharing.

Keywords: Cloud Computing, Data sharing, cloudsim computation, Multi-level encryption.

INTRODUCTION

Cloud is the word comes to its large accessibility and scalability. Cloud computing is a solution to the existing server problems which are being associated. Cloud help in large data computation with its scalable and long computation in nature. Cloud is having its architecture which contains several component which combine to form a cloud input and user processing criteria. Cloud computing enable to use it service with different available platform, such as private cloud, public cloud, community cloud and hybrid structure cloud. User can have the usage selection as per their business needs.

Cloud computing use a Virtual machine, data center and its controlling structure to process the user request. It can have on demand user services such as algorithm, storage criteria and other helping entity which can contribute in usage support. Although cloud is pay as peruse which is a special feature make it differ from the existing competitive server provider.

Challenging issues in single level data encryption Approach:

At this level of encryption either its symmetric key encryption or asymmetric key of encryption. The complete data is encrypted at single level. This type of encryption make produce cipher with complex one time security but still there is only one level of decryption or key is required. Here there are challenges associated with same in cloud where the single phase won't work to provide effective security over data.

Challenges being derived while data sharing and providing access through it. Thus a proper access control is required for proper data security.

LITERATURE REVIEW

Deepti Mittal, Damandeep Kaur, Ashish Aggarwal

The author of the paper entitled "**Secure Data Mining in Cloud using Homomorphic Encryption**" 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, author used a mining algorithm to predict a low usage component and host to transmit the algorithm. The given proposed approach is reliable over the given previous solutions. This is a provided secure approach which deals in data selection using the K-mean clustering approach make use of data mining efficiently. Their approach assumes that the data is not stored in a centralized location but is distributed to various hosts [11]. This proposed approach prevents any intermediate data leak in between and also a data integrity level of the proposed technique is efficient than the provided previous algorithms.

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.

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.

In this paper [3] An HLA, BLS based technique which uses bilinear pairing approach and computation for encryption approach. They have given an concept of TPA of integrity computation. TPA takes a challenge from the user input and process the challenge to compute its integrity from the available dataset. The challenge computation use the user file ID and other parameter which help in generating challenge proof. Challenge proof gives a output results to the input values. Further the output challenge response help in deciding the data integrity.

HLA MAC based computation help in equation computation. It is a signature based scheme which constructs a ring structure to formulate the encryption. A random masking over the values and linear homo-

orphic encryption is performed by the author of this research.

In this paper [4] A different range of security encryption technique is introduced by the paper. They have discussed the encryption algorithms such as AES, DES, Blowfish and other given symmetric and asymmetric approach for data encryption and then storage in the cloud computing environment.

There are algorithm which uses different key length and different internal operation to process the input text. RSA approach is also describe in their paper which uses two key one as public and one as private key to perform the encryption and decryption over the given simulation. The comparison analysis of their work shows that, a technique need to be long length key for encryption / decryption. Also , it should be collision free key and able to work oppose to different attack such as brute force attack etc.

In this paper [5] a short signature BLS approach is used for the data security purpose. They have used SHA-1 hashing algorithm for the hash generation and further performing integrity analysis using the hash values. SHA-1 use the 160 byte length of hash value which is generated by the use of user input and help in matching the hash value for the integrity proof generation. A short signature scheme which is BLS used in cloud for all type of input files which contributed by the data owners.

PROBLEM DEFINITION

In the previous algorithm which are dealing with either security or dealing with data access control. 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.

PROPOSED SOLUTION

In order to perform limitation overcome solution, the proposed technique make use of multiple phase matrix computation and hence multiple level of security is given in our proposed work , the work is summarized here:

1. Enhanced Dynamic matrix based encryption along with SHA-2 hashing scheme is proposed in the system which make it effective presentation of our proposed work.

2. Our algorithm also checks for proper access control using more secure and reliable parameters.

3. Access control mechanism based on identity of user is performed.

4. Matrix based technique make use of various conversion such as matrix binary conversion, Matrix transpose, key generation, XOR operation.

5. Further the security over data is implemented.

6. Batch auditing of previous stored user data is also performed in proposed work given by the work.

7. In this work some RSU concept is also introduced, where the work distribution over the centralized unit is performed.

CONCLUSION

Cloud computing and its data processing environment found its huge advantage over the storage and processing. The different algorithms make use of encryption technique model and keep data secure. File accessing over a large data is also a challenging task which need to be investigate. In this paper different security mechanism over the cloud data performed were discussed. Security algorithms make use of encrypted steps and keep data secure. A proposed technique which is multi-phases and data security oriented with sharing approach is given. The algorithm proposed is assumed to be best and going to perform over the implementation in next phase.

REFERENCE

[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.