Three Layer Security Model Based on Fog Computing

Abbas Mandhiri.S[1], Karthikeyan.P[2]
[1]Dept of Computer Science
[2]Professor, Dept of Computer Science
[1, 2] Prist University

Abstract- *Recent years the highly development of cloud computing technology. With the explosive growth of cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud storage servers. In traditional approach the users lose their right of control on data and face privacy leakage .Existing method of privacy protection schemes are usually based on encryption technology, but these kinds of techniques cannot effectively resist attack from the inside of cloud storage server. In order to solve this problem, we develop a three-layer security model based on fog computing. The proposed methodology can both take full benefits of cloud storage and protect the privacy of data. Besides, Hash-Solomon code algorithm is designed to divide data into three parts. Then, we can put a small part of data in local machine and fog server in order to protect the data privacy. Moreover, based on artificial intelligence, this algorithm can regulate the distribution proportion stored in cloud server, fog server, and local machine, respectively. Through the theoretical analysis the feasibility of our technique has been validated, which is really a powerful method to traditional cloud storage technique.*

Keywords- Cloud computing, cloud storage, fog computing, privacy protection.

I. INTRODUCTION

Confidentiality is a basic for strong security in all online computing sides, but confidentiality alone is not satisfies. Companies and customers are ready to use online computing only if they have the belief that their data and privacy details will stay confidential and safe. Thus to produce a trusted surrounding for users, we need to create a software, assist and works with confidentiality in mind. The location of physical assets and accessories being allowed in general doesn't known to the particular customer. It also affords services for customer to form up, use and maintain their data and privacy details in the applications on the cloud server, which maintains and manages the virtualization of assets by itself. Cloud storage memory is a method of networked online memory in which the secure data is stored in virtual group of stash that is generally being introduced by the third party. Cloud storage memory makes data stored remotely to be limitedly cached on Android phones, Personal computer or other Internet connected devices.

With the rapid development of network bandwidth, the Volume of customer's data is increasing geometrically. Data user's requirement cannot be satisfied by the capacity of local machine any more. Therefore, persons try to find new methods to store their personal data. For more powerful storage capacity, a growing number of data users select cloud server storage. Cloud server storage is a cloud computing system which provides data storage and secure management service. With a cluster of advantages, network technology and distributed data file system technology, cloud server storage makes a huge number of different storage devices work together coordinately.

Besides, depending on the property of the Hash-Solomon algorithm code, the methodology can ensure the original data cannot be recovered by partial data. On another hand, mistreatment Hash-Solomon code algorithm can turn out a little of redundant information blocks which can be normalized in decipherment procedure. Raising the number of redundant blocks can increase the reliability of the cloud storage, but it also results in additional cloud data storage. By reasonable allocation of the cloud data, our technique can really protect the privacy of user's data. The Hash-Solomon code algorithm needs complex calculation, which can be assisted with the Artificial Intelligence (AI). Paradigms of AI are with success employed in recent years to deal with varied challenges, as an example, the issues in Wireless sensor networks (WSNs) field. AI provides adaptative mechanisms that exhibit intelligent behavior in advanced environments like WSNs. Thus in our paper, we take application of AI to do some calculating works in the fog server. Compared with existing methods, our technique can provide a secure privacy protection from interior, especially from the CSPs.

II. RELATED WORK

The importance of security in cloud server has attracted a lot of attention no matter in industry. There are a large number of researches about secure cloud architectures in recent years. In order to solve the privacy leakage issue in cloud storage, use variety encryption techniques in different

positions. Solve the privacy leakage problem with the help of auditing or building their own cloud secure framework. However, there is a common defect in these articles.

Once the CSP is un-trusted, all of these techniques are invalid. They cannot resist internal attacks the CSP from selling customer's data to earn illegal profit. The private data will be decoded once malicious attackers get it no matter how advanced the encryption techniques are because customer's data was integrally stored in cloud storage. Therefore, we propose a three layer security model in this paper. By dividing file with specific code and combining with TLS framework based on fog computing architecture, we can achieve high secure privacy protection of data. It does not mean that we abandon the encryption technique. In our technique encryption also help us to protect fine-grained secure of the cloud data.

III. EXISTING SYSTEM

User uploads data to the cloud storage server directly. Subsequently, the Cloud Server Provider (CSP) will take place of customer to manage the data. In consequence, customer does not actually control the physical storage of their cloud data, which results in the separation of ownership and management of data.

In order to solve the privacy leakage issue in cloud computing, previous techniques proposed a privacy-preserving and copy- deterrence CBIR scheme using encryption techniques. This technique can protect the image content and features well from the semi-honest cloud server, and deter the image customers from illegally distributing the retrieved images.

Existing methods consider that in traditional situation, user's data is stored through cloud service provider even if CSP is trustworthy attackers can still get customer's data if they control the cloud management node. When customer requests data from cloud server, the customer sends a password to the server for identification. Taking it into consideration that the privacy password may be intercepted, the structure uses asymmetric response mode.

IV. PROPOSED METHOD

A. Three Layer Privacy

Now the cloud service server is divided into three different layers for enhance the security purpose and to prevent the location awareness. The three different privacy preserving layers are Cloud computing, Fog computing and local machine. A complete storage data is now divided and stored into three different layers. The ratio of the partition of storage data is major part of the data is stored in the cloud storage, neither high nor low range of storage data is stored in the fog computing and finally lower amount of local machine. When the stored cloud data required it can be combined into a single data using pattern matching techniques.

B. Encryption

While uploading the data in three layers, first it is encrypted using Hash Solomon code of encryption techniques. The data is combined with appending bit and it is encrypted. Now the encrypted stored data is stored in three layers. When the customer requires the complete data, it is decrypted first and combined with the other parts and given to the customer as a complete original data.

C. Fog Computing

Fog computing is similar with cloud computing. It consists of little latency and raising the geographical range of distribution. Fog computing can achieve the data processing and restricted storage capability. Fog computing consist of three-level structural design, the highest is a cloud computing layer, it can be used as storing data and computing data. The center layer is the fog computing layer. Fog computing layer can execute critical data spread to cloud server. And at last the third layer is wireless sensor network layer. This layer's major job is to gather data and upload it to the fog server. In accumulation, the rate of transmit flanked by the fog computing layer and other layers is faster than the rate between the cloud layer and the subordinate layer.

VI. EXPERIMENT RESULT

The structure can take full of cloud storage and defend the privacy of data. Here the cloud computing has concerned great consideration from dissimilar sector of society. The three level cloud storage stores in to the three dissimilar parts of data parts .If the one data part misplaced we lost the data in sequence. In this future structure using the bucket conception based algorithms. In our scheme we using a bucket conception so decrease the data wastages and reduce the procedure timings. We are by means of a HASH-SOLOMON code algorithm. It's High bendable. BCH code is used in a lot of communications relevance and low amount of idleness. The Bucket entrée manages reserve represents the Access Control Lists (ACLs) for buckets inside Google Cloud Storage. ACLs let you identify who has admission to your data and to what coverage. The three layer cloud storage stores into the three different parts of data parts .If the one data part

missing we lost the data information. In this proposed structure using the bucket concept based algorithms.

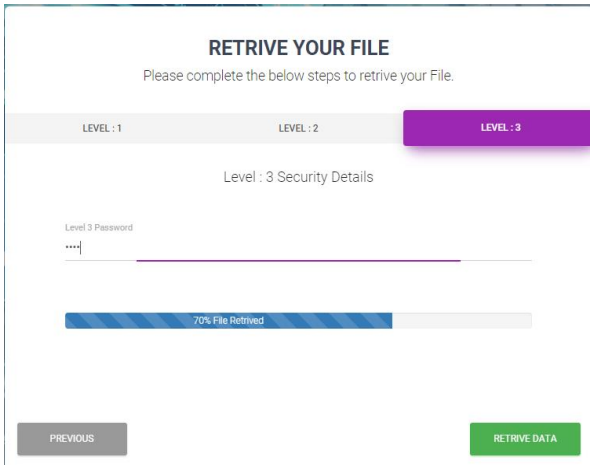

Fig. 1 Three Layer Security Model

VI. CONCLUSION

Cloud Computing makes the computer world has a wider collection of application and enhances client - friendliness by providing entrance through any type of internet connection. Even with this improved ease of use also some disadvantages. privacy is to be measured very important and is a key problem for cloud memory. Selections of techniques that can be used in order to guarantee confidentiality have been mitigated. This paper has revealed some privacy ways for avoiding the troubles in confidentiality on unsecured data stores in cloud. There are tranquil some techniques that are not addressed with in this paper. This paper makes divergence in the techniques in the text is based on encryption schemes, based on entrance control Mechanisms, keyword exploration techniques, and query reliability and compliance schemes. The work is making well-organized privacy-preserving memory.

VII. APPENDIX

As the three layer security model based on fog computing is complete by the mentioned algorithms, it can promote residential by using some other algorithms to reduce the position of code and to decrease the time convolution.

VIII. ACKNOWLEDGMENT

We are thankful to all helping hands in completion of this project. We would like to express our sincere thanks to all those who have provided us with valuable guidance towards completion of project.

REFERENCES

[1] Rajathi, N. Saravanan, A Survey on Secure Storage in Cloud Computing
[2] Ali Gholami, Erwin Laure, Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments
[3] An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data and a Class of Error-Correcting Codes
[4] Chandramohan Dhasarathan , Vengattaraman Thirumal, Dhavachelvan Ponnurangam, A secure data privacy preservation for on-demand cloud service
[5] Garima Gupta, P.R.Laxmi, Shubhanjali Sharma, A Survey on Cloud Security Issues and Techniques
[6] L. Malina, J. Hajny, P. Dzurenda, V. Zeman, Privacy-preserving security solution for cloud services
[7] Ms. B.Tejaswi, Dr. L.V.Reddy , Ms. M.Leelavathi, A Survey on Secure Storage Services in Cloud Computing
[8] Pengfei Hu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Tie Qiu, Senior Member, IEEE, Houbing Song, Senior Member, IEEE, Yanna Wang, and Xuanxia Yao