A Fog-Centric Quantum Security for Cloud Storage Scheme with Enhanced Multipath routing architecture

P. Uma Devi[1], B. Manorama Devi[2]
[1]*PG SCHOLAR, Dept of CSE,KSRM College of Engineering, Kadapa*
[2]*Assistant Professor, Dept of CSE,KSRM College of Engineering, Kadapa*

Abstract - **Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. Cloud computing promises to significantly change the way to use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. Proposed system provides small part of data in local machine and fog server in order to protect the privacy. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively. But here data is divided into blocks and stored in multiple systems, access data blocks and combining is tremendous work. In order to solve this problem, Proposing a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Propose a different approach for securing data in the cloud using offensive decoy technology. Monitors data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, to protect data, launching a disinformation attack by returning large amounts of decoy information to the attacker. Proposing Enhanced A Three-Layer Privacy Preserving Cloud Storage using multi cloud servers and multi fog servers, an efficient, distributed and scalable data processing system through Multi Cloud Server Security.**

Index Terms - **Stress detection, micro-blog, social media, social interaction, Word Semantic.**

I.INTRODUCTION

With the rapid development of network bandwidth, the Volume of user's data is rising geometrically. User's requirement cannot be satisfied by the capacity of local machine any more. Therefore, people try to find new methods to store their data. For more powerful storage capacity, a growing number of users select cloud storage. Cloud storage is a cloud computing system which provides data storage and management service. With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together coordinately. Nowadays there are lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies provide large capacity of storage and various services related to other popular applications. However, cloud storage service still exists a lot of security problems. The privacy problem is particularly significant among those security issues. In history, there were some famous cloud storage privacy leakage events. User uploads data to the cloud server directly. Subsequently, the Cloud Server Provider (CSP) will take place of user to manage the data. In consequence, user do not actually control the physical storage of their data, which results in the separation of ownership and management of data.

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

Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer. Fog computing layer can perform critical data transmission to cloud server. And finally the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer.

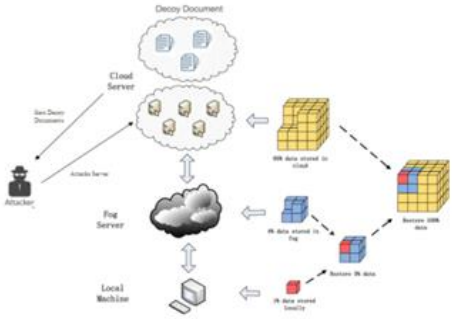


Fig 1: Three Cloud Architecture with Cloud

Confidentiality is a basic for strong confidentiality 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 will stay confidential and safe. Thus to produce a trusted surrounding for customers, 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 user. It also affords services for user to form up, use and maintain their data in the applications on the cloud, which maintains and manages the virtualization of assets by itself. Cloud memory is a method of networked online memory in which the data is stored in virtual group of stash that is generally being introduced by the third person. Cloud memory makes data stored remotely to be limitedly cached on mobiles, PC or other Internet connected devices. Confidentiality and cost are the barriers in this field, depending on the dealers. Although the first achievement and identification of the cloud model and the broad availability of producers and tools, a number of trials and prospects are intuitive to this new design of computing.

II. LITERATURE SURVEY

A. A Secure Data Privacy Preservation For On-Demand Cloud Service

This paper is focus on privacy and security of data stored in the cloud. They albeit computing is introduced to provide to increasing its efficiency, optimization and effectiveness of the cloud environment. Thus author introduce Privacy Preserving Model to Prevent Digital Data Loss in the Cloud. This proposal helps the Cloud Requester/Users to trust their proprietary information and data stored in the cloud.

B.Privacy-Preserving Security Solution For Cloud Services

This paper is based on the privacy-preserving security solution for cloud. It based on the signature scheme for the nonbilinear group providing the unidentified access to the cloud server and shared storage server. It makes Unidentified Authentication for the registered user. The user personal information can be displayed without revealing the user detail. However any illegal activity is found, the user rights in the cloud server can be revoked. Author proposed work helps to Anonymous access, unlinkability and data transmission confidentiality.

C. An Efficient Public Auditing Protocol With Novel Dynamic Structure For Cloud Data

This paper is based on the efficient method of making the structure of the data. Author proposed public auditing scheme in which dynamic operation can be performed. Hashing can be performed in this method. Using Merkle Hash Tree the dynamic data operation can be performed. Ring signature stores the information of the user.

D. On A Relation Between Verifiable Secret Sharing Schemes And A Class Of Error-Correcting Codes

This paper explains about the Verifiable Secret Sharing Schemes. Using the metric author forms a set of codes known as set of error correcting codes. Then they consider the burst error interleaving codes introduces the efficient burst error correcting scheme.

By this methods error correcting and secrete sharing of files can be performed.

E.Security And Privacy Of Ensitive Data In Cloud Computing: A Survey Of Recent Developments

This paper represents the Available technologies and a broad collection of Created and implementation of projects on cloud confidentiality and security. This paper are arranged based on the available works based on the cloud architecture ,Management of resources and cloud work management layers, along with the recollection of the developments that available in privacy preserving confidential data in cloud computing.

III. APPLICATIONS

Fog computing is an extended computing model based on cloud computing which is composed of a lot of fog nodes. These nodes have a certain storage capacity and processing capability. In our scheme, we split user's data into three parts and separately save them in the cloud server, the fog server and the user's local machine.

IV. PROPOSED SYSTEM

Objectives Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications technologies, arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Propose a completely different approach to securing the cloud using decoy information technology connected to Fog computing. Proposing Enhanced A Three-Layer Privacy Preserving Cloud Storage using multi cloud servers and multi fog servers, an efficient, distributed and scalable data processing system through Multi Cloud Server Security.

Existing System

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. Many Concepts are introduced in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. Traditional privacy protection schemes are usually based on encryption technology, but these kinds of methods cannot effectively resist attack from the inside of cloud server. In Traditional Methods all user related data is stored in a single cloud.

Existing system is a three-layer storage framework based on fog computing. As an extension to Traditional Method project has been extended with Enhanced security degree with combining local machine, fog server and cloud server.

Disadvantages of Existing System

- Many Concepts are introduced in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms.
- Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider.
- Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms.
- However these mechanisms have not been able to prevent data compromise and data theft is usually occurring.

Proposed System

Propose a completely different approach to securing the cloud using decoy information technology to Fog computing. Providing an enhanced layer for Cloud Server to divided the data and store in multiple clouds. Technology to launch disinformation attacks against insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. The decoys, then, serve two purposes: (1) validating whether data access is authorized When abnormal information access is detected, and (2) confusing the attacker with bogus information. The

combination of these two security features will provide a high levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security.

Advantages of Proposed System

- Cloud computing promises to significantly change the way we use computers and access and store our personal and business information.
- Enhances with Multi Clouds in Cloud Layer.
- With these new computing and communications technologies, arise new data security challenges.
- Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider.
- Propose a different approach for securing data in the cloud using offensive decoy technology.
- Propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing.

Algorithm

Begin

1: for each session separated for every user do

2: Get different HTTP requests and activities of user (DB queries q, Storage S, Services r) in this session

3: for each different r do

4: Add user Request to File with sessions(UserID,Db Query, Storage, Services)

5: if r is not in set USER login then

6: exit else

7: Encrypt File (Db Query, Storage, Services)

encipher(String s, String key)

for I = 0 to s.length() do

char encyphered = s.charAt(i) + getShift(key, i) > 90 ? (char)((s.charAt(i) + getShift(key, i)) - 26) : (char)(s.charAt(i) + getShift(key, i))

log.append(encyphered);

next

8: Append session ID with Activity

9: decrypt (String s, String key)

For I = 1 to s.length() do

char decyphered = s.charAt(i) - getShift(key, i) < 65 ? (char)((s.charAt(i) - getShift(key, i)) + 26) : (char)(s.charAt(i) - getShift(key, i));

log.append(decyphered);

10: End

Application Modules

Cloud Computing

Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It divide into three type

1.Application as a service.

2.Infrastructure as a service.

3.Platform as a service.

User Behavior Profiling

We monitor data access in the cloud and detect abnormal data access patterns User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such ‘normal user’ behavior can be continuously checked to determine whether abnormal access to a user’s information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. We monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector’s accuracy.

Decoy documents

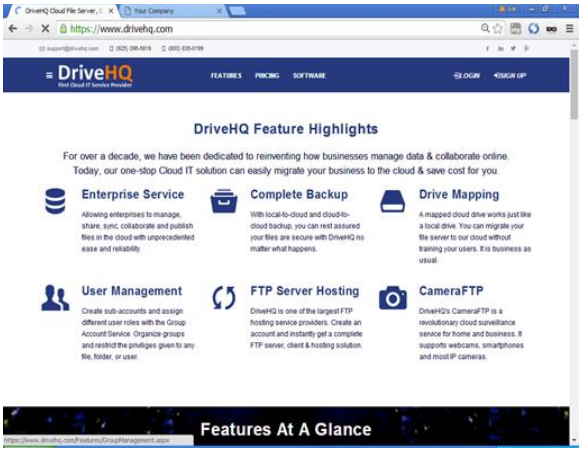
We propose a different approach for securing data in thecloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user’s real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) Confusing the attacker with bogus information.

V.RESULTS

A set of experiments carried out on stress analysis data obtained from facebook on the social media users. The performance evaluation of the system is performing using this dataset. The screenshots of various phases of stress analysis system are as follows



VI.CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to resolve the matter of privacy protection in cloud storage, we have a tendency to propose a three layer privacy protective secure cloud storage methodology framework supported fog computing model and style. By allocating the magnitude relation of knowledge blocks keep in several servers fairly, we will make sure the privacy of knowledge in every server. On another hand, cracking the encryption matrix is not possible in theory. Besides, using hash transformation will shield the fractional info. Through the experiment take a look at, this theme will efficiently complete encryption and coding while not influence of the cloud storage efficiency. Cloud Computing makes the computer world has a wider range of uses and enhances user - friendliness by providing access through any type of internet connection. Even with this increased ease of use also some drawbacks. Confidentiality is to be considered very important and is a key issue for cloud memory. A variety of techniques that can be used in order to ensure confidentiality have been mitigated. This paper has discovered some confidentiality ways for avoiding the problems in confidentiality on unsecured data stores in cloud. There are still some approaches that are not addressed with in this paper. This paper makes difference in the methodologies in the literature is based on encryption methods, based on access control Mechanisms, keyword search schemes, query integrity and Adaptability schemes. The work is making efficient confidentiality-preserving memory

REFERENCE

[1] J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud assisted urban data sharing framework for ubiquitous cities, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/ j.pmcj.2017.3.013

[2] Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z. (2018). Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2018.2793350

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[5] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014,pp. 2969–2974.
[6] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacypreserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7,pp. 1397–1409, 2014.
[7] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016,pp. 130–143.
[8] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.
[9] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.
[10] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.
[11] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts.,vol. 13, no. 1, pp. 68–96, First Quarter 2011.
[12] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp.2594–2608,Nov. 2016.
[13] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud assisted urban data sharing framework for ubiquitouscities," Pervasive Mobile Comput., vol. 41, pp. 219–230, 2017.