International Journal of Research in Advent Technology, Vol.7, No.2, February 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Secure Cloud Data Storage: From Single to Multi-Cloud Environment

Manoj V. Bramhe, Dr. Milind V. Sarode, Dr. Meenakshi S. Arya
Phd Research Scholar, Professor and Head, Associate Prof. & Head
Department of Computer Science & Engineering, Department of Computer Engineering ,
G.H. Raisoni College of Engineering, Nagpur
Government Polytechnic, Yeotmal
manoj_bramhe@yahoo.com

Abstract: Cloud based storage services are most popular among organizations due to its high computing power at low cost with saving in IT infrastructure. Major threat found by organizations before storing data in public cloud storage is security of the information stored. Even after strong provision of various security mechanism at various cloud service level, still full security is not achieved yet. Malicious system administrator can access data of any organization . Our proposed solution deals with the cloud storage security issues by distributing trust and security of user's data among multiple clouds by distributing fragmented data among them. Since no entity will get complete set of data at any instance of time hence system is secure and reliable.

Keywords: Cloud Computing, DFS, API

1. INTRODUCTION

Cloud Computing saves operational and infrastructure cost for organizations as it provides networking, hardware and software resources as per their usage but major problem with public cloud storage systems is various security challenges because whole user's data is available to service provider. Various methodologies were proposed by many researchers for cloud security and privacy like cryptographic techniques, replication of data, trusted cloud computing, isolation of virtual machines etc but most of them were implemented in single cloud based system . Single cloud storages stores data at one place hence it faces many problems like failure of service availability, malicious system user, data integrity and data intrusion problems. Further research was carried into multi-cloud or cloud-of-clouds where user's data is fragmented into multiple slices and distributed among various clouds. This improves overall security, trust and reliability of storage services as none of the entities get complete information at a time. Distributed file system (DFS) are used for managing files from multiple hosts.

We have implemented multi cloud based storage service which not only provides security and privacy to user's data but also provide reliability. User's files are divided into multiple chunks, encrypted and then stored in multiple public/ private cloud in secured environment. Data is retrieved with integrity check and merged to generate original user file. Failure management is implemented through replication of data in multiple clouds .

2. RELATED WORK

Cloud computing security research was carried out in two phases. In initial days solutions were proposed for single cloud based system where as mentioned in [1] and [2]. They have used security approaches like trusted system, erasure coding, secret sharing, VM isolation and cryptographic techniques for data storage. Main issues with such approaches is that data is available fully with public cloud provider where we cannot have trust on inside system user as they can utilize data for malicious purpose breaking security measures at IaaS level. Secondly some solutions were proposed for multi-cloud based system where security and trust is divided into multiple cloud hence dependency is less as compared to single cloud systems. Authors in [6],[8],[9] has discussed approaches where data is divided into various parts and partial data parts are stored in various clouds. Various architecture for data and application processing for multi-cloud environment is discussed in [4]. Authors in [7] have used open source distributed file system named Tahoe-LAFS for reliability purpose. They have used secret sharing scheme and private key encryption methodologies. In [13] researchers have proposed cost effective schema for storage in multi-clouds. Bessani et.al. have proposed dependable storage clouds in [14] where they stores the users data partitioned in three clouds. They have used RAID techniques for recovery of the data. All of these approaches have focused on some specific security parameters but our proposed system works on all security parameters.

3. PROPOSED SYSTEM

We have studied solutions proposed by various researchers for single and multi cloud environment and concluded that multi-cloud systems are better options for storage systems. Multi-Clouds systems are more secure as they not only removes threats for single cloud systems like vendor-lock-in but also makes the data safe from malicious system user . Malicious activity is not possible for storage system user as he never have full copy of data available with him and he cannot do anything with partial data.

Our proposed system takes dynamic decision as per end-user request, divide data followed by encryption to ensure security. This encrypted blocks of data are stored in various cloud storage. The proposed system uses RAID similar techniques to regenerate original file from partial chunks in the event of failure of some cloud storages.

Figure 1 describes the architecture of proposed system. System is designed for multi-cloud environment where application layer is developed as end user interface used by user for data and query provision. User requests are processed by API developed for our system. We have used distributed file system mechanism for cloud storage . DFS command are useful for writing and reading data in cloud based system using its distributed characteristics. DFS methods are developed for processing the files using three main components of our systems as Encryption, De-Construction and File transport.

1) Encryption Component: It is designed for using cryptographic techniques to ensure security of data before storing in clouds. Encryption is used for partitioned file chunks before writing them into clouds and decryption is used for getting original file along with merging operation during reading the files from clouds. We have used private key algorithms like AES and BlowFish for testing purpose.

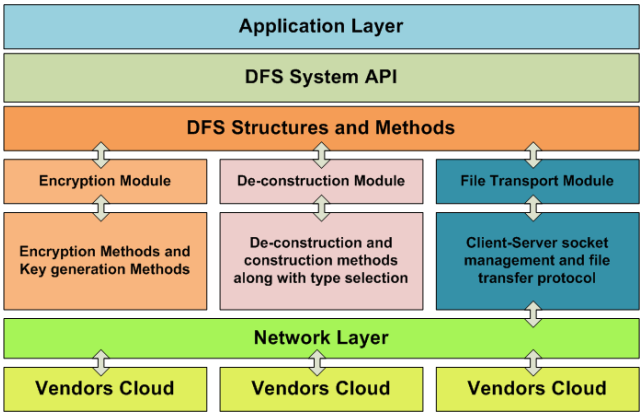

Figure 1: System Architecture

2)De-Construction Component: It is used for splitting the original file into multiple parts and storing them among various public cloud storages. System divides whole file and stores first 1/3rd part as chunk 1 in local server. this is used to store number of cloud storage server required for the system. Further system divides remaining parts in two chunks and stored them as chunk 2, chunk 3 in two different public cloud storage.

3)File Transfer Component: It is used for writing and reading file chunks over cloud environment using TCP/IP framework. It uses socket programming and network protocols like FTP. We have choose to use FTP over HTTP as it is easy, fast and simple to implement. File Transport Protocol uses port no 20 and 21 to write and reads file to cloud storage server. Standard FTP client and server management systems can be used for implementation .

4. IMPLEMENTATION

We have developed system API for three main components of the system for making it reusable in various applications. Independent dynamic linking libraries were developed for various methods as per the design of our DFS structure.

KeyGenaration, EncMethod, Encrypt, Decrypt are the functions written for encryption modules which are used for processes required for maintaining security of files. SetFileCount and SetMode function are developed for De-construction module used for deciding no of fragments and mode of fragmentation. File Transport module uses functions developed like SetTransferMode, Connect, Disconnect, SendFileChunk, ReciveFilechunk for doing network operation related to file writing and reading. These API sets allow end user to connect, configure and utilize the storage system using FTP.

5. EXPERIMENTAL RESULTS

We have tested our implementation for single and multi cloud based systems. We have used system configuration as Intel P5 2,8GHZ processor with 2 GB RAM as local server . We have used different types and different size of files for performance evaluation. System is tested for three private key algorithms AES, DES and 3DES for verification of their performances. We have considered excel, doc, jpeg, html and pdf files of various size and following graphs shows uploading time required for various files in single and multi-cloud environment. Figure 2 shows time required for uploading various files using AES encryption algorithm for single and multi-cloud environment. Figure 3 and figure 4 shows uploading time required for uploading various files using DES and 3DES algorithm.

Our experimental results shows that DES algorithm is slowest in performance and 3DES performs better than DES whereas AES algorithm is best in class . We conclude that AES is most suitable and fast private key algorithm in cloud environment for encryption purpose

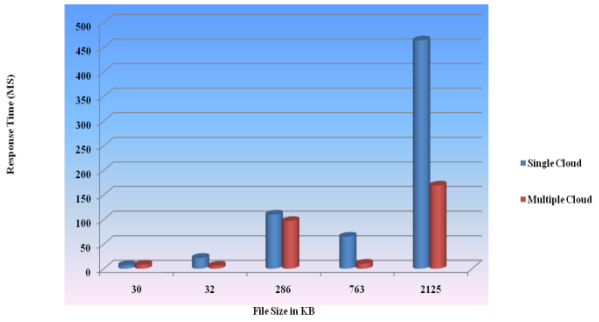

Figure 2: File processing using AES

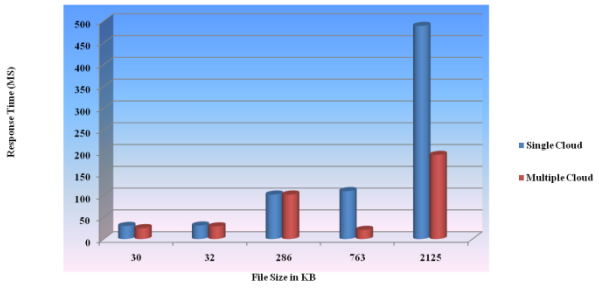

Figure 3: File processing using DES

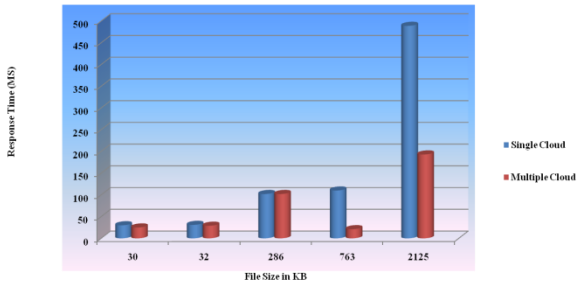

Figure 3: File processing using 3DES

Comparing the results of various algorithms in single and multi-cloud environment we conclude that small size files have similar uploading time for single and multi-cloud environment whereas as the file size increases multi-cloud based system gives better performance over single cloud based system and required less time to upload data in storage server. Thus Multi-cloud based system are better than single cloud based system.

6. CONCLUSION

We have implemented system for secure data storage and evaluated its performance for single and multi-cloud environment. Our system enhances security features in multi-cloud environment by distributing multiple file chunks in various public clouds thus adversary never have complete information about user's data. We have evaluated working of system using AES, DES and 3DES cryptographic algorithms. Our experimental results shows that AES is most suitable and fast security algorithm for cryptographic operations. We also conclude that multi-cloud based system gives better performance than single cloud based system for file processing.

REFERENCES

[1]]Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, March 2012

[2]MohammedA. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE 45th Hawaii International Conference on System Sciences, 2012

[3] Singhal M., Chandrasekhar S., TingjianGe., Sandhu R., Krishnan R., Gail-JoonAhn., Bertino E., "Collaboration in Multicloud Computing Environments: Framework and Security Issues", IEEE computer society journal, Vol. 46, Issue 2, pp. 76-84, Feb 2013

[4] Bohli J., Gruschka N., Jensen M., Lo Iacono L., Marnau N, "Security and Privacy Enhancing Multi-Cloud Architectures," IEEE Transaction on Dependable and secure computing, Vol PP, Issue 99, 2013

[5]Tran Doan Thanh, Subaji Mohan, EunmiChoil, SangBum Kim, Pilsung Kim "A Taxonomy and Survey on Distributed File Systems," IEEE Fourth International Conference on Networked Computing and Advanced Information Management, 2008

[6] Su Chen, Yi Chen, Hai Jiang, Laurence T Yang, Kuan-Ching Li, " A secure distributed file system based on revised Blakely's secret sharing scheme," 11th IEEE international conference on trust, security and privacy in computing and communications, 2012

[7] Fan-Hsun Tseng, Chi-Yuan Chen, Li-Der Chou, Han-Chieh Chao, "Implement a reliable and secure cloud distributed file system," IEEE international symposium on intelligent signal processing and communication systems, November 2012

[8] ShushantShrivastava, Vikas Gupta, Rajesh Yadav, Krishna Kant, "Enhanced Distributed storage on the cloud," IEEE 3rd international conference on computer and Communication technology, 2012

[9] KhengKok Mar, "Secured virtual diffused file system for the cloud," 6th International IEEE conference on internet technology and secured transactions, UAE, December 2011

[10]RajkumarBuyya, Introduction to the IEEE Transactions on Cloud Computing, IEEE Transactions on Cloud Computing, Vol. No. 1, January –June 2013

[11] NirnayGhosh, SoumyaGhosh, Sajal Das, "SelCSP: A framework to facilitate selection of cloud service providers," IEEE Transactions on Cloud Computing, Vol. 3, No. 1, January-March 2015

[12] Chien-An Chen, Myounggyu Won, RaduStoleru, GeofferyXie, "Energy-Efficient fault-tolerant data storage and processing in mobile cloud," IEEE Transactions on Cloud Computing, Vol. 3, No. 1, January 2014

[13] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, Yafei Dai, " CHARM: A Cost-efficient multi cloud data hosting scheme with high availability," IEEE Transactions on Cloud Computing, Vol. 3, Issue 3, July-September 2015

[14] Alysson Bessani Miguel Correia Bruno Quaresma Fernando Andre Paulo Sousa, " DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", ACM Transaction on Storage, Vol. 9,No. 4, Article 12. November 2013

[15] Sancha Pereira, Andre Alves, Nuno Santos, Ricardo Chaves , "Storekeeper: A Security-Enhanced Cloud

Storage Aggregation Service", IEEE 35th Symposium on Reliable Distributed Systems, 2016

[16] Hussam Abu-Libdeh, Lonnie Princehouse, Hakim Weatherspoon, " RACS: A Case for Cloud Storage Diversity", International conference for Internet technology and Secured Transaction, December 2012

[17] Kevin D. Bowers, Ari Juels, Alina Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage", 16th ACM conference on Computer and communications security, November 2009.