International Journal of Research in Advent Technology, Vol.7, No.1, January 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Multi-Cloud Secure Data storage using Cryptographic Techniques

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,
Yavatmal
G.H. Raisoni College of Engineering, Nagpur
manoj_bramhe@yahoo.com

Abstract: Cloud computing is becoming popular paradigm for storage and computing purpose for big and small organizations. Even though cloud supports pay-as-you-go model with saving on infrastructure, hardware and software cost of organizations it has disadvantages like various vulnerabilities and threats to user's information . File access mechanism is an technique to guarantee the file safety in the cloud. On the other hand, due to file farm out and untrusted cloud servers the file access mechanism develops security concerns in cloud storage systems. Malicious system administrator at cloud storage is becoming most difficult attack to stop as he has full access to the user data. In proposed system, we have implemented secure cloud storage for multi-cloud environment where instead of keeping user's data in single cloud environment it can be fragmented into different chunks and these chunks can be encrypted and stored in multiple cloud along with metadata which can be used during access of the files.

Keywords: Multi-Clouds, Cryptography, FTP

1. INTRODUCTION

Cloud computing provides on-demand and pay -per-usage access to scalable resources over the Internet. It saves operational and infrastructure based expenses for organizations.

Cloud computing as defined by NIST model is classified into three types of services as Software-as-a-Service , Platform-as-a-Service, and Infrastructure -as-a-Service. Cloud models has four categories as Private, Public, Hybrid and Community depending upon the nature of storage services. Public cloud is maintained by third party service provider which distributes their resources among clients and charge them as per their usage . Private cloud is used by big organizations for storing security critical information at private hosting place . Hybrid cloud uses both public and private cloud resources for data storage where general information is stored in public cloud whereas critical information is maintained in private cloud. Community cloud is used for specific purpose like education, insurance, healthcare services. Organizations hesitate to put their critical information on public cloud storage as most of them either maintains users data in plain text format or they may used encryption techniques on their own transparent to the user. This encryption algorithm and security keys are maintained by cloud system administrators who can use them for malicious activity so there is need of system where data must be uploaded on cloud in secured manner and user must maintain critical security information with them.

Our proposed system will provide multi-cloud based secured storage where user will split the data into multiple parts, storing each one of them on various private/ public cloud hence none of the entity will ever get complete set of the data at any time , improving trust and reliability of cloud services. Security of data in our system is improved as user will encrypt the data before uploading and will have all security related information stored in local application server thus removing the possibilities of system administrator attacks.

2. RELATED WORK

Research was carried on cloud storage system and various defense methodologies were proposed for handling cloud threats and vulnerabilities. NIST has discussed cloud security issues and challenges in their draft of cloud computing synopsis and recommendations [1]. Cloud security alliance has provided detailed guidance for focus areas in cloud as mentioned in [2]. They have discussed various security domains like identity management, encryption & key management, application level security for data security out of which encryption and identity management is widely by researchers.

Most of the cloud storage research is carried out for single cloud environment which stores complete set of data at one place thus creating vulnerabilities like system administrator attack, data integrity issues, data losses due to vendor lock-in problems so further solution was provided for multi-cloud environment as mentioned in [4] where performance is improved by distributing trust, and

security among various clouds. They have discussed many multi-cloud based systems like RACS, DepSky, HAIL with their advantages and disadvantages. Distributed file system (DFS) is used by all such systems to share and store users files in distributed network. Authors have discussed popular DFS in [5] and [6]. Paval Bozh in [7] had discussed reliability and performance improvement in DFS by distributing data and metadata parts of file separately on the server. RACS system discussed in [8] is based on creating redundant array of cloud storage which focused only on the economic failures and of the data. Our system is similar to DepSky model[10] where confidentiality, integrity cloud outage whereas HAIL system [9] works for maintaining integrity and availability parameters for maintaining security and privacy will be implemented. Authors have discussed multi cloud based system in [14] and [15] mainly for cost effectiveness and failure management.

3. PROPOSED METHODOLOGY

System Architecture:

Architecture of our proposed system is discussed below. User application layer receives and transfer user commands to API of our distributed file system which will communicate to system modules through DFS methods. Encryption module will be used for encryption and decryption of the data for maintaining the security. De-construction module is used for splitting of files during writing data to multi-clouds whereas merging of files is done during reading the data from the clouds. File Transport module will be useful for writing and reading of files to the multi-clouds. Users data will be written to private / public clouds. System implementation is discussed below in detail.

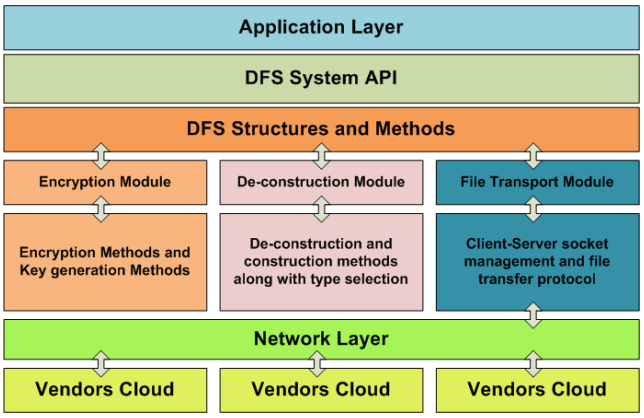


Figure 1: Proposed System Architecture

Implementation:

Our proposed system modules are explained in this section. We have user registration & login module, FTP setting module, File upload and download module, encryption and decryption module & file splitting and merging modules.

Step 1: Registration & Login Module

This module will be used for user registration and login purpose. User has to perform one time registration to the system by providing user credentials like username, password and personal details. Random verification code will be generated and forwarded to the registered mobile number which will be used for user verification during login to the system. This step will enhance user authentication. Once sign in user can use various system modules.

Step 2: FTP Management Module

This module will be used for managing FTP services used for writing and reading the data to multiple clouds. FTP service will be utilized by our distributed file system for communicating with distributed network. Our system divides and store user files among multiple clouds .Normally three clouds are used for storage and recovery purpose .First location used to store first part of our file is our local application server which is also used as storage server. Next two locations will be public clouds where second and third parts of the file will be stored. This module is used by the user application as FTP client for connecting , writing and reading various files to storage server.

Step 3: Upload and Download Module

Upload:

This module will be used by the end user to write users data into multiple clouds using web interface. User can choose any types of file from local storage. All the files uploaded by the user will be listed in user specific directory along with file details .File upload function will be used to upload file and server map function will be used to get server path for uploading data.

Download:

This module will be used by the end user for reading the required file from cloud storage. User will select file already uploaded using directory listing . System has mapping table where file parts stored are mapped with respective cloud storages. System will get first path from mapping table to get first part of the file stored on local storage Using FTP details and server path stored in mapping table system will get 2nd and 3rd parts of the file stored in public cloud storage . Merge function of the system combines all the parts of file in temporary buffer and stored it.

Step 4: File Encryption and Decryption Module

This module will be used for file security purpose. Symmetric cryptographic techniques will be used for securing files where encryption is used during upload process and decryption is used during download process. Users can perform encryption on complete file before splitting into parts or perform encryption after splitting the

file . System will provide randomly generated security key to the user which will be used for encryption and decryption. Using the key, encrypted file parts will be generated and uploaded to the
cloud storage.

Download process uses decryption module to decrypt the merged parts of the user file using the security key provided by the user. Once user credentials and security key are matched then process is executed successfully to download the requested file .

Step 5: File Split and Merge Module

This module will be used for splitting the user file into various parts during upload process and merging the parts to generate original file during the download process. Meta data of all the files is stored on local application server which not only saves network transmission time but also provides greater level of security

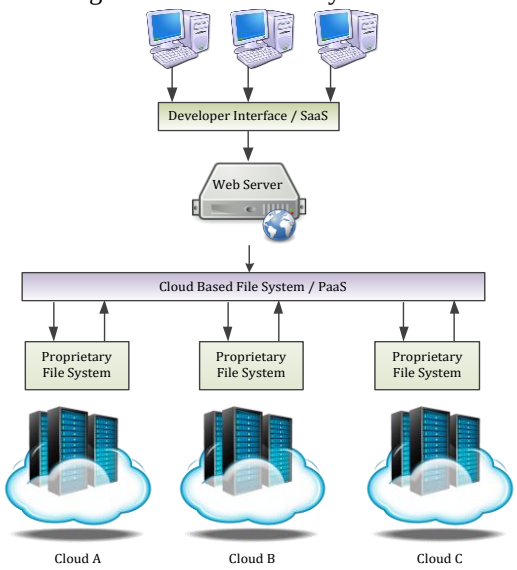


Figure 1 : Multi-Cloud Secured Storage System

4. SECURITY ANALYSIS

This section deals with analyzing security of our proposed system using various cryptographic techniques .Proposed system provides security to user's data by splitting it into multiple chunks and putting those chunks in various clouds. Confidentiality of the data is maintained using encryption techniques where symmetric or asymmetric techniques can be used

- *Cryptographic Techniques:*

Security of data is most important aspect for any cloud service provider. Most of the public cloud provider stores data in plain format or some of them may use encryption / decryption using keys stored on cloud premises. Hence there is a need of system where cryptographic techniques are in the control of the user so that data stored on cloud premises is safe from malicious inside attacker.

Cryptographic techniques are most popular for security of data has been classified as symmetric or private key cryptography and Asymmetric or public key cryptography. Symmetric algorithms are simple and easy to implement with less complexity . Some of the popular symmetric algorithms are DES, 3DES, AES, RC5, BlowFish Etc. Asymmetric cryptography is mathematically more complex than symmetric but provide more security. RSA is most popular asymmetric key algorithm.

We have tested our system for various symmetric key algorithms and results are discussed in next section. Here we discussed AES, Advanced encryption standard algorithm

AES is symmetric key block cipher uses 128 bit data size. It allows variable round and keys. It supports 10 round for 128 bit key, 12 rounds for 192 bit key and 14 rounds for 256 bit key. Each round uses 128 bit round key extracted from original key by key generator program. It is stronger and around six times faster than 3DES. It is iterative cipher using substitution & permutation network.

Each round in AES consists of four processes as Byte substitution, Shift Rows, Mix Columns and Add RoundKey

- *Security:*

In general, AES is most secured symmetric key algorithm. It is widely accepted and used in both hardware and software implementation. AES does not have any cryptanalytic attacks but has some side channel attacks detected against specific versions of AES hence programmer must take care during its implementation

5. RESULTS AND. DISCUSSIONS

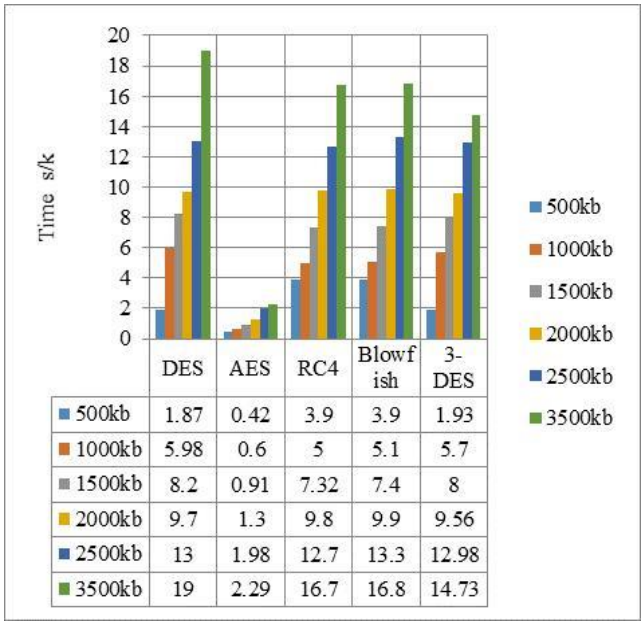
We have developed system for implementing the concept using asp.net. Our system has web interface which is used by end user for communication with the system. Registration module is used for user registration and regular signup. We have developed a multi-cloud system in which user split his file, perform encryption using symmetric key and will upload the file to multiple clouds. During downloading user will specify his file, system will read various encrypted parts from multi clouds , merge them and perform decryption to generate original file for the user.

Our system is using cryptographic techniques for securing the users data. We have chosen symmetric key cryptographic technique for our system as it is simple, easy to implement as compared to asymmetric techniques.

We have tested our system for various symmetric cryptographic algorithms like DES, 3DES, AES, Blowfish and RC4. We have tested the system in cloud environment with following configuration. We have Xen (5.6 XCP) server and the client with VMware system with N- Para-virtual machine. The cloud server has Core i5 (4.8GHz) with 8GB of RAM and 500GB-HDD. The client machine has Core i3 (2.4GHz) with 2GB of RAM . We have tested

our system for encryption and decryption using various symmetric algorithms for varying file size from 500 kb to 3500 kb. We came to the conclusion that AES algorithm is fastest among all other algorithms tested hence we will be using AES symmetric key algorithm for security of our system data.

Following figure shows results of comparison of various cryptographic algorithms for varying file size.



	DES	AES	RC4	Blowfish	3-DES
500kb	1.87	0.42	3.9	3.9	1.93
1000kb	5.98	0.6	5	5.1	5.7
1500kb	8.2	0.91	7.32	7.4	8
2000kb	9.7	1.3	9.8	9.9	9.56
2500kb	13	1.98	12.7	13.3	12.98
3500kb	19	2.29	16.7	16.8	14.73

Figure 3 : Encryption with Symmetric Key

6. CONCLUSION

Cloud based storage systems are most popular among organizations due to their "pay-as-you-go" model. Big organizations are using private / public / hybrid cloud infrastructure for storage but still most of them are not deploying their critical data on cloud due to security concerns.

Our proposed system implementation is based on multiple clouds where data is fragmented and distributed among various available clouds partially so that adversary will never get complete data thus removing threats related to single cloud system. Security is enhanced in our system by using AES symmetric cipher used for encryption during writing data to the cloud and for decryption during reading data from the cloud. We have tested our system on local and public cloud environment for various symmetric key algorithm. Our system is secure and reliable.

REFERENCES

[1] Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas DRAFT Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2011

[2] Cloud Security Alliance (CSA). "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," (Released December 17, 2009), http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

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

[4] 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

[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] Satyanarayanan, M., "A Survey of Distributed FileSystems," Technical Report CMU- CS-89- 116, Departmentof Computer Science, CarnegieMellonUniversity, 1989

[7] PavalBzoch, Jiri Safarik, "Security and reliability of distributed file systems," 6th IEEE international con. on intelligent data acquisition and advanced computing systems, Sep 2011.

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

[9] 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.

[10] 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

[11] DaliborPeric, Thomas Bocek, Fabio Victora Hecht, David Hausheer, Burkhard Stiller, " The design and evaluation of a distributed reliable file system," Int. Conference of parallel and distributed computing, application and technologies, 2009

[12] Hung-Chang Haiao, Hsueh –Yi Chung, HaiyingShen, Yu-Chang Chao, "Load rebalancing for distributed file systems in clouds," IEEE transactions on parallel and distributed systems, Vol. 24, No. 5, May 2013

[13] KhengKok Mar, "Secured virtual diffused file system for the cloud," 6th International

[14] IEEE conference on internet technology and secured transactions, UAE, December 2011

[15] 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

[16] Dan Dobre, Paolo Viotti, Marko Vukolic, " Hybris: Robust Hybrid Cloud Storage", ACM Transactions on Storage, Vol . 13, Issue 3, October 2017