Data Security Assurance in Cloud Computing

[1]Shailesh Kamble, [2]Tushar Waghmare, [3]Shilpa Gulgonda, [4]Pooja Kumbhojkar, [5]Revati Wahul

[#]Computer Dept., Pune University
Email: [1]shaileshkamble7777@gmail.com, [2]twaghmare72@yahoo.com, [3]shilpaapatil12@gmail.com,
[4]poojakumbhojkar777@gmail.com, [5]rmwahul@mescoepune.org

Abstract— Now a days, cloud computing is a technology that uses internet and central remote servers to maintain data and application. In cloud computing storage providers are responsible for keeping data available and accessible. People and organizations buy or lease storage capacity from service providers to store user, organization and application data. For storage of data relying upon a solo service provider is not very promising. Security is important factor related to the cloud computing. As the users can store his private data on cloud with the help of cloud service providers.

Data stored on a single cloud is a risk of service availability failure due to attackers enters in a single cloud. In our "Data Security Assurance in cloud computing" model in cloud computing holds an economical distribution of data among the available Service Providers which provides a cost-effective as well as secure storage to the customers.

Our proposed system aims to encourage the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. Our proposed model provides a better security for customer's data according to their available budgets from that they can choose cloud service provider.

Keywords— Cloud computing, security, customers, service provider.

I. INTRODUCTION

Idea behind this project is to build an application for cost-effective secured multi-cloud system for data storage in cloud computing. Now a days, cloud computing is a technology that uses internet and central remote servers to maintain data and application as shown in figure 1.

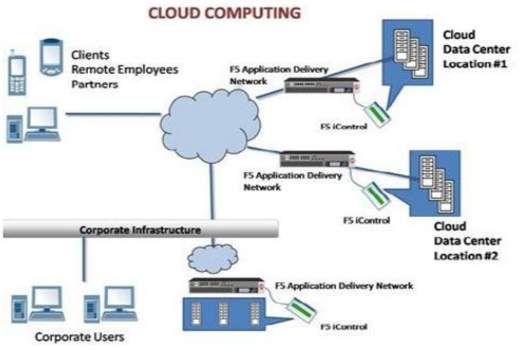
CLOUD COMPUTING
Clients
Remote Employees
Partners
F5 Application Delivery Network
Cloud Data Center Location #1
F5 iControl
F5 Application Delivery Network
F5 iControl
Cloud Data Center Location #2
Corporate Infrastructure
F5 Application Delivery Network
F5 iControl
Corporate Users

Fig. 1 Cloud Computing

Cloud data storage also redefines the security issues targeted on customer's outsourced data (data that is not stored/retrieved from the costumers own servers).

Sincecloud service providers (SP) are separate market entities, data integrity and privacy are the most critical issues that need to be addressed in cloud computing.

Even though the cloud service providers have standard regulations and powerful infrastructure to ensure customer's data privacy and provide a better availability, the reports of privacy breach and service outage have been apparent in last few years.

In addition, providing better privacy as well as ensure data availability, can be achieved by dividing the user's data block into data pieces and distributing them among the available service providers in such a way that no less than a threshold number of service providers can take part in successful retrieval of the whole data block.

Data is divided into number of data units and stored on different cloud servers, it will increase data availability and data security.

II. MODEL

In this section, we will describe about problem statement of our model and general system overview.

A. Problem Statement

To develop an application over cloud storage using multiple cloud to store data and retrieve securely where given p number of cloud service providers(SPi: 1,2…p), Each Service provider associated with a QoS factor (QoSi(0,1)) along with the cost of storing data units (Ci), Our Data Security Assurance in cloud computing model seeks a distribution of customer data pieces among the available Service Providers in such a way that, at least q number of Service Providers must take part in data retrieval, while minimizing the total cost of storing the data on Service provider as well as maximizing the quality of service provided by the Service providers.

B. System Review

We consider the cloud storage system in cloud computing that happens between Cloud Uer's (CU) and Cloud Service Providers (SP). Every service provider is having its own Quality of Service (QoS) and Cost for storing data. In our model user can analyse different

Cloud Service Providers according to their cost and QoS as per their own requirement to store data. User can use multiple cloud vendors to store data independently. User can split data and store on different Vendors.

III. ALGORITHM

Comparison between different Encryption Algorithms

- DES is the old "data encryption standard", its key size is too short for proper security. Also, DES uses 64-bit blocks, which raises some potential issues when encrypting several GB's of data with same key.
- 3DES is a other way of reusing DES implementation, by cascading three of DES (with distinct keys). 3DES is used to secure data upto at least "2^112" security. But its slow, especially in softwares.
- Blowfish is a block cipher proposed by Bruce Schneier, and developed in some softwares. Blowfish can use huge keys and is believed secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. Blowfish is efficient in software platforms (it uses key-dependent lookup tables, hence performance depends on how the platform handles memory and caches).
- AES is the successor of DES as standard symmetric encryption algorithm for US federal organizations (and as standard for pretty much everybody else, too). AES accepts keys of 128, 192 or 256 bits (128 bits is already very unbreakable), uses 128-bit blocks (so no issue there), and is efficient in both software and hardware. It was selected through an open competition involving hundreds of cryptographers during several years.

Introduction of AES Algorithm

The Advanced Encryption Standard (AES) was announced by the National Institute of Standards and Technology (NIST) in November 2001. It is the successor of Data Encryption Standard (DES) which cannot be considered as safe any longer, because of its short key with a length of only 56 bits. There are three versions of AES. All of them have a block length of 128 bits, whereas the key length is allowed to be 128,192, or 256 bits.

Basic Concepts

The AES algorithm consists of ten rounds of encryption, as can be seen in figure 2. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes transformation using the corresponding cipher key to ensure the security of the encryption.

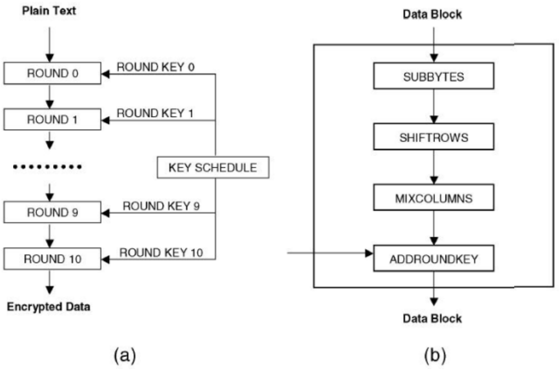

Fig 2. Example of AES algorithm

After an initial round, during which the first round key is XORed to the plain text (Add round key Operation), nine equally structured rounds follow. Each round consists of the following operations:

- Substitute bytes
- Shift rows
- Add round key

The 10th round is similar to rounds one to nine, but the Mix columns step is omitted.

IV. LITERATURE REVIEW

1. A secured cost effective multi-cloud storage model

As the uses of cloud computing increase, it is highly likely that more criminals will try to find new ways to exploit vulnerabilities in the system. To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed in order to establish trust so this model provides customers better cloud storage decision providing best quality of service.

2. Amazon S3 Availability Event: July 20, 2008

Amazon S3 were having problems communicating with each other. As background information, Amazon S3 uses a gossip protocol to quickly spread server state information throughout the system. This allows Amazon S3 to quickly route around failed or unreachable servers, among other things. Only after gossip is completed will the server send along the information related to the customer request. More specifically, we found that there were a handful of messages that had a single bit corrupted such that the message was still intelligible, but the system state information was incorrect.

3. Dropbox confirms it was hacked

Dropbox acknowledged that spam mailings afflicting users starting a few weeks ago happened when hackers used passwords obtained from third-party sites to access small number Dropbox user accounts. The investigation found

that usernames and passwords recently stolen from other websites were used to sign in to a small number of Dropbox accounts. A stolen password was also used to access an employee Dropbox account.

V. CONCLUSION

Cloud system “Data Security Assurance in cloud computing”, which seeks to provide each customer with a better cloud data storage decision, taking into consideration the user budget as well as providing him with the best quality of service i.e Security and availability of data offered by available cloud service providers. It shows ability of providing a customer with secured storage under his affordable budget. Proposed system “Data Security Assurance in cloud computing” model in cloud computing holds an economical distribution of data among the available Service Providers in the market, to provide customers with data Availability as well as storage. It provides a better decision for customers according to their available budgets.

VI. ACKNOWLEDGMENT

It gives us great pleasure and satisfaction in presenting this preliminary report on “Data Security Assurance in cloud computing”. We would like to express our deep sense of gratitude to all those who provided timely guidance and helping hand in making our preliminary report successful. We want to thank the department of Computer Engineering of Modern Education Society’s College of Engineering for giving us opportunity to do the necessary research work and to use departmental resources. We extend sincere thanks to respected guide of our project & all the teachers of the Computer Department who encouraged us for this project. We would like to thank all for their indispensable support, and suggestions.

REFERENCES

[1] A Secured Cost-effective Multi-Cloud Storage in Cloud Computing, Yashaswi Singh, Farah Kandah, Weiyi Zhang Department of Computer Science, North Dakota State University, Fargo, ND 58105

[2] Amazon.com, Amazon s3 availablity event: July 20, 2008, online at http://status.aws.amazon.com/20080720.html, 2008

[3] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. Medard, Trusted storage over untrusted networks, IEEE GLOBECOM 2010, Miami, FL. USA.

[4] W. Itani, A. Kayssi, A. Chehab, Privacy as a Service: Privacy- Aware Data Storage and Processing in Cloud Computing Architectures, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec 2009.

[5] P. S. Browne, Data privacy and integrity: an overview, In Proceeding of SIGFIDET 71 Proceedings of the ACM SIGFIDET (now SIGMOD), 1971.

[6] C. Wang, Sherman S.-M. Chow, Q. Wang, K. Ren, W. Lou, Privacypreserving public auditing for secure cloud storage, in InfoCom2010, IEEE, March 2010.

[7] Uli Kretzschmar, AES128 – A C Implementation for Encryption and DecryptioN, SLAA397A–July 2009–Revised March 2009

⟐⟐⟐