Securing the cloud

[1]Ankit Sharma, [2]Monika Arora

[1]B.E. in CS from MIT, [2]B.E. in CS from MIT
Indore, India

***Abstract*— Till today cloud computing has become a promising business concept and still emerging to become a fastest growing segment of IT industries. Now today's main concern is "SECURITY" in the cloud computing environment. The information on individuals and companies is placed in the cloud, but how to make it secure? This paper discusses the security challenges and issues that CSP (Cloud Service Provider) face during cloud engineering and also the encryption technique to provide better security.**

***Index Terms*— Cloud Computing, Security, Encryption**

I. Introduction

Cloud Service Providers (CSP) (e.g. Microsoft, Google, Go Grid etc) are supporting virtualization technologies. In order to maximize the efficiencies of virtualization virtual machines from multiple organizations have to be co-located on the same physical server. Today day by day ente4rprise are making cloud computing services as part of their enterprises by compromising with the security to a great extent.

International Data Corporation (IDC) conducted a survey (see Fig.1) of 263 IT executive and there lines of business colleagues and concluded as security to be great threat for cloud computing.

Now a day many corporations are leading forward in order to use the services provided by the cloud but they doesn't bother about the "Security". They are moving critical and sensitive application to public and shared cloud environment but they doesn't know that they are far away from their data center network perimeters defense. To alleviate eradicate these concern, a CSP trying to manage it in some way that it can provide compliance to their auditors.

For communication to be possible between the cloud services some standardization is maintained (e.g. ISO/IEC 27001/27002, Information Technology Infrastructures Lib (ITIL), (OVF) Open Virtualization Format [2] [3] [4])

The main focus of this professional paper is "SECURITY". It also recommends OVF standards and its beneficial properties to make it compatible with virtual machines.

Corporation and individuals are concerned about how security and compliance integrity can be maintained in this new environment. Even more concerning, though, is the corporation that are jumping to cloud computing while being Oblivious to the implication of putting critical application and data in the cloud.

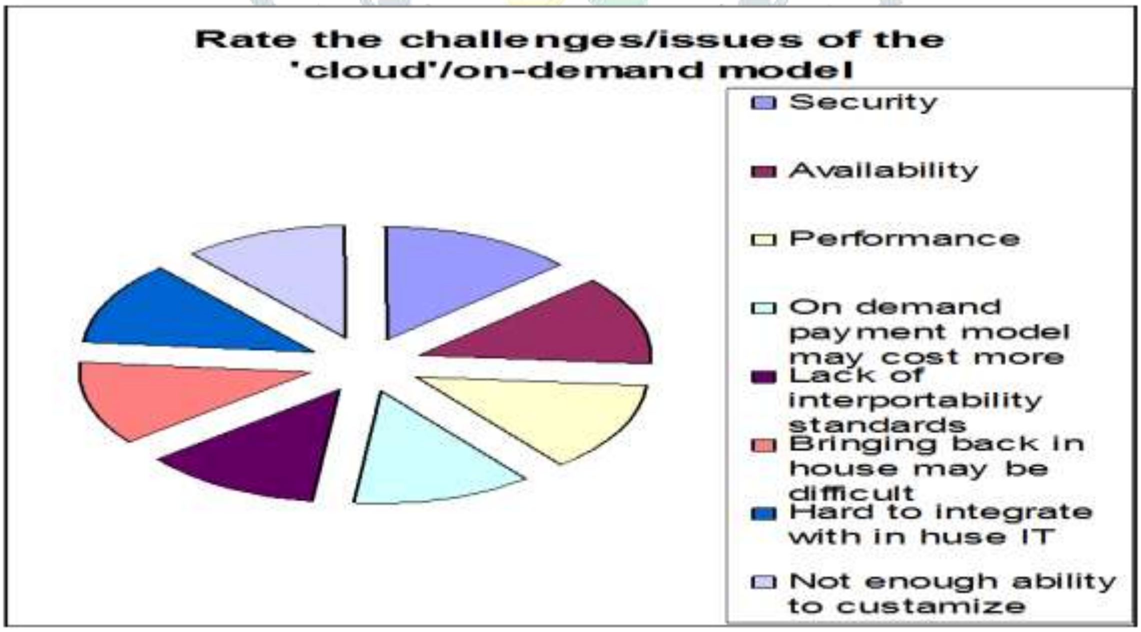

Fig. 1(Result of IDC survey of 263 IT executive about the challenges of cloud computing)

II. Cloud Security

A. Major security concern:

1. Security concern #1: Who controls the Encryption/decryption keys? Logically it should be the Customer who should control the key.

2. Security concern #2: Ensuring the integrity of the data (Transfer, storage, and retrieval) really means that it Changes only in response to authorized transactions. A Common standard to ensure data integrity does not yet exist.

3. Security concern #3: Company has violated the law (Risk of data seizure by (foreign) government).

4. Security concern #4: Some government regulations Have strict limits on what data about its citizens can be Stored and for how long, and some banking regulators require that customer's financial data remain in their home Country.

5. Security concern #5: Users must keep up to date with Application improvements to be sure they are protected.

6. Security concern #6: Storage services provided by one Cloud vendor may be incompatible with another vendor's Services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud). [5]

7. Security concern #7: Customer may be able to sue cloud service providers if their privacy rights are violated.

8. Security concern #8: The dynamic and fluid nature of Virtual machines will make it difficult to maintain the Consistency of security and ensure the audit ability of records.

B. Encryption technique:

Strong encryption technology is core technology for protecting data in transit to and from the cloud as well as data stored in the cloud. It is or will be required by law.

1. The goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage.

2. Benefits of cloud storage: reliable, shared data storage.

3. Encryption should separate stored data (data at rest) from data in transit.

4. Depending upon the particular cloud provider, you can create multiple accounts with different keys.

5. Microsoft allow up to five security accounts per client.

6. Although encryption protects our data from unauthorized access, it does nothing to prevent data loss.

7. Indeed, a common means for losing encrypted data is to lose the keys that provide access to the data.

8. One standard for interoperable cloud-based key management is the OASIS key management Interoperability Protocol. IEEE 1619.3 also covers both storage encryption and key management for shared storage.

C. Security Management Standards

Supporting standards are (ITIL) INFORMATION TECHNOLOGY INFRASTRUCTURE LIB., (OVF) OPEN VIRTUALIZATION FORMAT.

1. ITIL: Information Technology Infrastructure Library support process based approach for management of IT services. Strategies, tactical and operational levels are main concern of ITIL. Information securities are taken into consideration.

Supporting standards are (ITIL) INFORMATION TECHNOLOGY INFRASTRUCTURE LIB., (OVF) OPEN VIRTUALIZATION FORMAT.

2. ITIL: Information Technology Infrastructure Library support process based approach for management of IT services. Strategies, tactical and operational levels are main concern of ITIL. Information securities are taken into consideration.

   Benefits of ITIL are:

   - Cost is reduced.
   - IT services are improved.
   - Improved production of data.
   - Unique ideas and long term work is used.
   - Administrative tasks and technical task are separated.
   - Technical support performance is taken into consideration.
   - Many more standards are included guidance is provided.

The main concern of security management is to insure its confidentiality, integrity and availability along with related properties. The data should be protected against risks.

3. Open Virtualization Format (OVF): Enterprises data are mainly taken into account of OVF. The most enhancements are done on virtualization.

   Benefits of ITIL are:

   - Mainly supports virtualization.
   - Multi-tiered services are pre configured.
   - Virtual machines support enterprises software.
   - Perfect and error free installation are done.

Now, the cloud security is approaching towards the virtualization in order to fulfill needs and expectations. The virtual machine can be easily configured accordingly in order to provide security as it is much more similar to an XML document.

So, primarily virtualization will be the main security providing layer combined with clouds. Now prior services are combined together in a composite way, so as to provide n support virtual machines software and hardware. Along with it some models also make way towards security. These technologies will soon be emerging in a new form.

D. Layered security measure includes:

In this section we describe what all security measure we can take.

1. Operating system and virtual machine level authentication for administrator

   .

2. Inbound traffic firewall, guarding each virtual environment.
3. Signed API call.

4. SSL encryption for all traffic.

5. Every user activity is “Scrutinized” and logged for “auditing” purpose.

E. Security Management Models

This section describe requirement for cloud computing that should be provided by cloud service providers.

1. Software-as-a-service (SaaS): SaaS is one of the cloud service models where the most basic requirement for security practices will reside. The corporation or end user have to research vendors policies on data security before using there services so that data lost or unable to access data can be avoided.

2. Security Governance: There should be a security steering committee. So that the guidance about the security initiatives and agreement with IT strategies can be focused.

3. Risk management: In this security model, there are some identification related to technology issues, data link to business process, data storage and assignment of ownership are studied. It also includes implementation of confidentiality, integrity, availability and privacy controls.

4. Security awareness: There must be awareness among people about the knowledge of security issues. Proper training should be provided to people so that the social engineering attack, slower response to potential security incidents and also customer data leaks can be avoided.

5. Education and Training: There should be program which must be developed for providing knowledge about security and risk management skills.

6. Policies and Standards: Standards and policies should be developed, documented and implemented to maintain relevancy.
7. Third party risk management: Third party risk management program should be there to avoid revenue looses and damage to providers reputation.

8. Security image testing: Creation of “test image” and to reduce exposure by patching offline is also provided by virtualization based cloud computing.

9. Data security: security of data is required to move to data level so that data can be protected. Encryption is also provided at data levels and provides compliance with the payment card industries standards.

10. Application security: Security features and requirement security test result are defined in this model. The security team should provide security requirement for development of product for implementation.

11. Virtual machine security: Physical servers are connected to multiple virtual machines instances on virtualized servers. The data center security team’s advice there customer on how to prepare the machine for migration to a cloud environment.

12. Physical security: Security model may need to be reevaluated when customer lose control over physical assets. Some samples of controls mechanism are:

- 24/7/365 onsite security.

- Biometric hand geometry readers.

- Security cameras should monitor activity throughout the facility.

13. Disaster recovery: Using virtualization software virtual server can be copied, backed up, and moved just like a file.

14. Data privacy: It insures that the organization is prepared to meet the data privacy demands of its customers and regulators.

15. Data governance: The framework should describe who can take what action with what information, and when, under what circumstances, and using what method.

III. Conclusion

We have argued about the security in the cloud. In this paper we have cover the challenges and the issue while using the cloud services and also encryption technique, security standards, layered security measures, security management models.

- Security issue indicate problem which may arise.

- Encryption encrypts and secures the data.

- Security standards provide type of security template which CSP could obey.

- Layered security measures indicate what security measure we can take to secure the cloud.

- Security management models recommendation based on best practice and standards.

We have also find out result to provide better encryption technique. Here (see Fig.2) we are using the merging of two security algorithm so that more security can be achieved. Algorithm which we are using, one is the most secure algorithm and one is minimum time complexity algorithm. This makes the encryption algorithm more efficient.

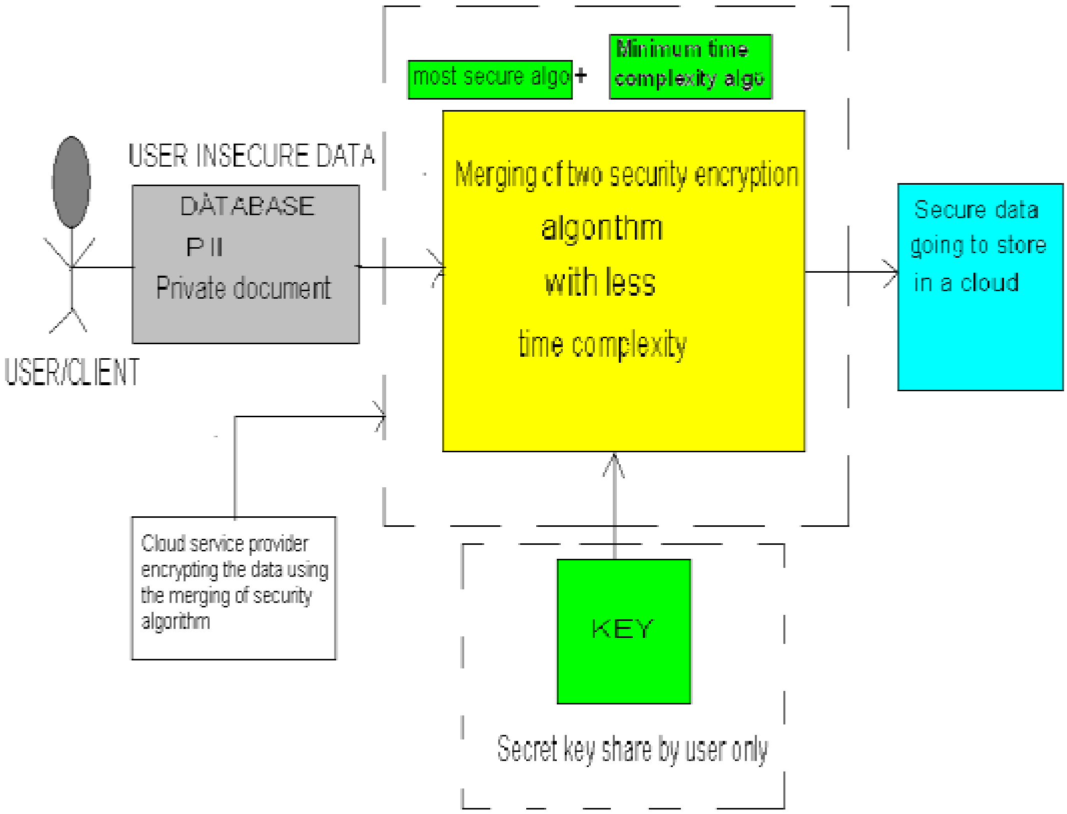
most secure algo
+
Minimum time complexity algo
USER INSECURE DATA
DATABASE
P II
Private document
USER/CLIENT
Merging of two security encryption algorithm with less time complexity
Secure data going to store in a cloud
Cloud service provider encrypting the data using the merging of security algorithm
KEY
Secret key share by user only

Fig. 2(merging of two algorithms in which one is most secured algorithm and one is minimum time complexity algorithm and generating the key which will be only shared n control by client).

We have also find out one more result that the key which is been generated will be only shared by the user/client. Client will control encryption and decryption key. Also we need to approach key management seriously. Keys should have a defined lifecycle. There should be automated key store backup and recovery techniques.

These are all very important topics which will be discussed in upcoming year of cloud computing. Product that fall within the security and vulnerability management market will remain in high demand security and vulnerability management market will remain in high demand.

REFERENCES

[1] International Data Corporation, http://blogs.idc.com/ie/wp-content/up loads/2009/12/idc_cloud_challenges_2009.jpg

[2] Information Technology Infrastructure Library, http://www.itil-officialsite.com/home/home.asp

[3] International Organization for Standardization, http://www.iso.org/iso/home.htm

[4] Distributed Management Task Force, http://www.dmtf.org

[5] Cloud computing bible by Willey publication.

[6] NIIT cloud computing student guide.

[7] Wikipedia.