International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 2 Issue 1 (January 2015) www.ijirae.com

Survey on Data security Issues in Cloud Environment

Vasanth.C.Bhagawat
Research Scholar/ Computer Science
Bharathiar University, Coimbatore

Dr. A.Arul L.S.Kumar
Prof & Dean, Dept. of. CSE
RGIT, Bangalore.

Abstract— Delivering Enterprise solutions have been changing from decades to decades. The computing power has evolved from parallel, Grid to Cloud now. IT services shifted from desktop to mobile, and from on premises to the cloud. Knowing the most exciting technology of today's Industry Business, Government, and even Individuals are focusing and shifting towards cloud computing. As it enhance scalability, flexibility, reduce cost by moving their applications, storage, application development environment even infrastructure to cloud. Conversely data security and privacy are the major concern for the success of cloud computing. In this paper we look into various data security issues and we see that providing cryptography by using Hash function it is more robust and securely we can protect the data in cloud.

Keywords— Survey, Data Security, Cloud, Computing, Privacy

I. INTRODUCTION

Cloud Computing is today's most inspiring technology in industry and in research. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g., network, servers, storage, applications, and services) that can rapidly provisioned and released with minimal management effort or service provider interaction.[1] Cloud computing services are quickly becoming formal and integral members of IT portfolio. Organizations are adopting cloud-based platforms which provides infrastructure and application services as a pay-per-use basic. Client organization are more concern with lack of security and it is the, most important reasons organizations are hesitating for adopting cloud services.[2] To make cloud computing adopted by users and industry, the security concerns has to be rectified.

Compared with the traditional IT model, the cloud computing has many potential advantages. It helps the users to use services from other without actually buying it for huge costs. But from the consumers' perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing. According to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues [12].

Before the data security issues are discussed we will see the functions of cloud. Cloud computing has particularly many characteristics:

- *On-demand capabilities*
- *Broad network access*
- *Resource pooling*
- *Rapid elasticity*
- *Measured service*

Here there is a cloud service provider that facilitates services and manages the services. The provider facilitates the services over the internet and end user use them for their needs and pay the service provider accordingly. Because of high performance computational services at cheaper rate cloud is growing continuously and many famous companies such as Microsoft (Azure), Amazon, Google, etc, are providing cloud services on the internet.

II CLOUD COMPUTING INFRASTRUCTURE

There are number of implementations based on services this company provides. For example, Google Apps Engines, Drop box. Depending on the access scope, cloud can be classified as : *public cloud, private cloud, hybrid cloud and Community cloud* as show in below figure 1.1

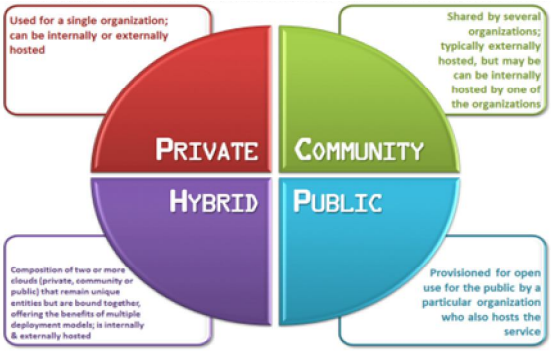

Figure 1.1 : Types of Cloud's.

- Public clouds : Are offered by service providers for general public over the internet. Like Amazon, IBM's Blue Cloud, Google AppEngine, Windows Azure etc,. The general public can use the infrastructure available via internet. It is most cost effective for users.
- Private clouds: Are dedicated to a particular organization which are managed internally or by third-party and hosted internally or externally like Amazon (EC2). It is managed by the users or by a third party within or outside the premises. It costs more than public cloud but it leads to more cost savings when compared with a datacenter as evidenced by Concur Technologies (est. savings of $7million in 3 years from 2009) [13].
- Hybrid clouds : Are which uses both private and public. Organization can host critical data in private clouds and applications in public clouds which are less secure.
- Community cloud: involves sharing infrastructure between organizations of same community like all government organizations within same state.

Based on the services provided cloud is classified as follows:

- Software as a Service (SaaS) where the providers offers various applications on a cloud infrastructure. Users can access software application hosted by cloud vendor through a thin client interface such as web browser. Like Salesforce.com offers online CRM space, Google's Gmail, Google docs, Microsoft's online version of office BPOS (Business Productivity Online Standard Suite).
- Platform as a Service (PaaS) involves offering a development platform for customers on cloud where he can deploy his own applications without installing any platform or tools on their machines. Few PaaS providers are Google's Application Engine, Microsoft's Azure, etc.
- Infrastructure as a Service (IaaS) involves offering hardware recourses like storage, network and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include OS and applications. IaaS are provided by Amazon Ec2, Amazon S3, Rackspace Cloud Servers etc.[5,6]

In spite of advantages of cloud computing, trusting the system is more important as the real asset of any organization is the data which is available on cloud. This trust depends on the data security and privacy issues which will be discussed in this paper. The meaning of security here we consider is the combination of confidentiality that is how to prevent an unauthorized disclosure of information, integrity, prevention of unauthorized amendment or deletion of information and availability, the prevention of unauthorized withholding of information.[4]

III DATA SECURITY ISSUES

As many are moving to cloud storages, there are many potential attacks attempted few of them are :

a. Denial of Service(DoS) attacks: As cloud is shared by many users, DoS attacks much more damaging.
b. Side Channel attacks: By placing a malicious virtual machine to a target cloud server an attacker can launch a side channels attack.
c. Authentication attacks: There are many different ways to authenticate users, and methods used are a frequent target of attackers.
d. Man-in-the-middle cryptographic attacks: It is carried out when an attacker places himself between two users.
e. Inside-job: Here person, employee or staffs who have the knowledge of system can attack the cloud system.

The content of data security and privacy protection in cloud computing is similar to traditional data security and privacy protection. The content of data security and privacy protection in cloud has its particularities. In this paper we will see the different security techniques of data security and privacy protections in cloud computing. Security aspects can be classified as data integrity, confidentiality, availability and privacy as show in figure 3.1.

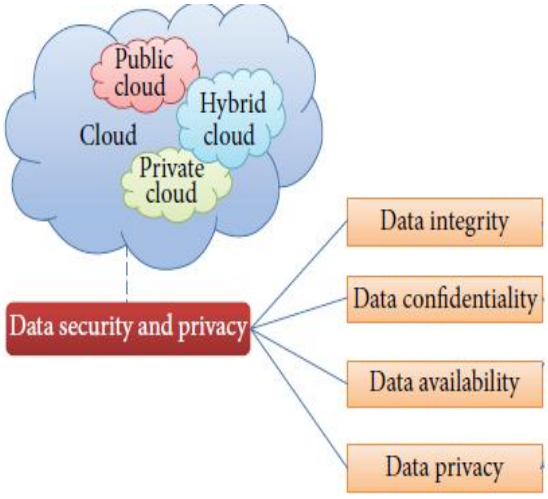

Figure 3.1: Various Data Security

Data Integrity:

Generally data integrity means securing the data from unauthorized detection, fabrication or modification. It is one of the critical aspects in security. Data integrity in the cloud system means preserving information integrity. It is the basic to provide cloud computing service such as SaaS, PaaS and IaaS. [8]In cloud the data stored in data ware house must be secure enough from the intrusion and other damages. The loosing of data can be from inside or outside. While providing the security of data, cloud provider should implement mechanisms to ensure data integrity. He should make the client aware of what particular data is hosted on the cloud. There could e a malicious inside attack or from outside it could be hackers, attackers. Like Google docs got attacked in 2009, Amazon S3 was also attacked recently.[7] In standalone system integrity is maintained via database constraints transactions. Access of data can be controlled by authorization.

Data Availability:

It means the recovery of user's data when an accident such as hard disk crash, damage or any other network failures happens. The issue of storing data over servers is a main concern of user's as cloud vendors are governed by local laws and the cloud clients should be cognizant of those laws.

Data Confidentiality:

User's privacy and confidentiality risks vary significantly with the terms of service and privacy policy governed by service providers. Data confidentiality is important for users who store their data private or confident data in the cloud. To ensure confidentiality in cloud data control strategies and Authentication are used. These issues can be addressed by increasing the cloud reliability and trustworthiness [9]. Encryption is usually used to provide confidentiality for data.

IV CRYPTOGRAPHY METHOD

To secure the data which is uploaded by users into cloud, it has to be encrypted. Information in cloud data centers is encrypted by the users using many cryptography techniques.

Cryptography is the art and science of achieving security by encoding messages to make them non-readable". The plain text message is in simple English language that can be understood by any. The message is codified using cryptographies techniques called as cipher text message [10].

We have three type of techniques 1) Symmetric Key Cryptography 2) Asymmetric Key cryptography 3) Hash function Cryptography as show in Figure 4.1

- *Symmetric Key Cryptography*: Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.
- Asymmetric Cryptography: The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys-a key pair.

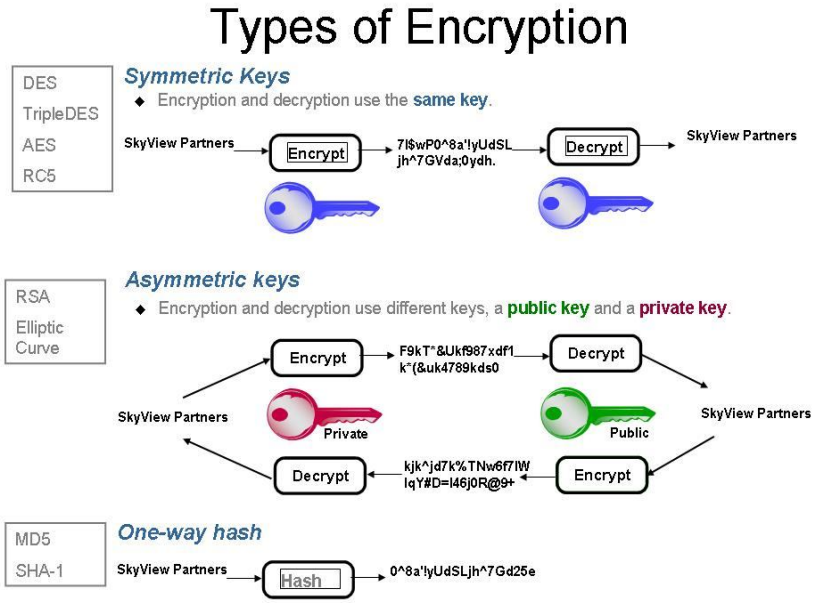

Figure 4.1 : Three types of Encryptions

A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only

You know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

- *Hash Function Cryptography:* The hash function cryptography (One way cryptography) offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages [11]. The most used hash function cryptography techniques are: SHA1, MD5.

We can compare all these methods using various parameters. It is clear from the below table 1 that compared to symmetric and asymmetric, hash function has more advantages.

Table 1: comparisons of all techniques

Metric	***Symmetric***	***Asymmetric***	***Hash***
Collision Resistant	NO	NO	Yes
Key agreement	Problem	No Problem but complex mathematical calculations	No problem
Complexity	Less	More complex	Less
Speed	Fast	Slow	Fast
Delays	Less	More	Less
Security	Less	Medium	High
Implementation	Difficult	Difficult	Simple

We can see that hash functions are less complex and simple to implement and at the same time very hard to break a hash function.

V FUTURE WORK

Cryptography relies on stable and unique key to encrypt and decrypt messages. As many cryptographic algorithms are be used in security like given below. The key point is that it is no longer adequate to simply encrypt your data. You must now actively select the appropriate cryptographic algorithms

Table 2: Famous Cryptography Algorithms

Type	Algorithm
Symmetric	DES, AES, RC5
Asymmetric	RSA, ECC
Hash	MD5, SHA1

Based on NIST and ANSI guidance, below table 3 provides the comparative strengths of various cryptographic algorithms. We try to look into how Various Hash function and ECC algorithms and how these can be used to protect the data in cloud computing.

Table 3 : Comparing Similar cryptographic algorithm strengths.

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	Elliptic Curve Field Size	RSA Modulus Size
80 bits	2 Key Triple DES	SHA-1	160 bits	1,024 bits
112 bits	3 Key Triple DES	SHA-224	224 bits	2,048 bits
128 bits	AES-128	SHA-256	256 bits	3,072 bits
192 bits	AES-192	SHA-384	384 bits	7,680 bits
256 bits	AES-256	SHA-512	512 bits	15,360 bits

VI CONCLUSION

Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users [14].Although cloud computing has many advantages, there are still many actual problems that need to be solved. According to a Gartner survey about cloud computing revenues, market size for Public and Hybrid cloud is $59 billion and it will each USD 149B by 2014 with a compound annual growth rate of 20 [15]. The revenue estimation implies that cloud computing is a promising industry. But from another perspective, existing vulnerabilities in the cloud model will increase the threats from hackers.

VII ACKNOWLEDGEMENT

I Convey my thanks to ***Prof. AMCV Srinivas,*** Head of MCA department for his support and conveniences for this paper. I also extend my sincere thanks to ***Principal, AMC Engineering College***, Bangaluru, Affiliated to Visvesvaraya Technological University, Belagavi for support and encouragement for research works.

REFERENCES

[1] Mell, P., Grance, T. (2009) The NIST Definition of Cloud Computing Version 15. NIST

[2] The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014 by Andras Cser and Ed Ferrara, November 17, 2014

[3] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.

[4] A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing,"IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[5] Subashini S, Kavitha V (2011) A survey on Security issues in service deliverymodels of Cloud Computing. J Netw Comput Appl 34(1):1–11

[6] Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1 "An analysis of security issues for cloud computing" Hashizume et al. Journal of Internet Services and Applications 2013, 4:5

[7] Mohammed A.AlZain, Eric Pardede, Ben Soh, James A.Thom2012."Cloud ComputingSecurity:From Single to Multi-Clouds" 2012 5thHawaii International Conference on System Sciences

[8] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu Data Security and Privacy in Cloud Computing Data Security and Privacy in Cloud Computing.

[9] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no.5, pp. 11–14, 2012.

[10] William Stalling, A Handbook on "Cryptography and network Security" by Pearson Education, 2009

[11] K. Dubey, M. Namdev, S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference, 2012.

[12] Sun Cloud Architecture Introduction White Paper

[13] LEMOS, R. 2009. Inside One Firm's Private Cloud Journey. Retrieved April 7,2011, from http://www.cio.com/article/506114/Inside_One_Firm_ s_Pri vate_Cloud_Journey.

[14] Ramgovind, S. Eloff and M.M. Smith, E.,"The management of security in Cloud computing", in Information Security for South Asia (ISSA), 2010,pp.1-7.

[15] Gartner DataQuest Forecast on Public Cloud Services ocIDG00200833, June 2, 2010

