A Survey of Security Issues in Cloud Computing and Key Management

[1]Kruti Patel, [2]Vijaykumar Gadhavi, [3]Kaushal Jani
[1]M.E. Student, Dept. of CE, Gujarat Technological University, Gujarat, India
[2,3]Assistant Professor, Dept. of CE, Gujarat Technological University, Gujarat, India

***Abstract* -- Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. It is an Internet based technology where quality services are provided to users including data and software, on remote servers. Advantages of cloud computing includes creating and storing data at remote servers, hence utilizing the client resource to the minimum level. But this advantage implicitly contains drawback of data security. In this paper, I representated the major security issues and challenges present in cloud computing today and few of Key management concepts are also highlighted.**

***Index Terms* - Cloud Computing, Security issues, Key Management, Data Security**

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [5].The cloud computing is a new computing model that provides the uniform access to wide area distributed resources on demand. Cloud computing is a way of leveraging the Internet to consume software or other IT services on demand. There are no shrink wrapped boxes containing discs or hardware for you to buy and set up yourself. Cloud providers typically charge monthly recurring fees based on your usage [1].The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to reshape their business models to gain benefit from this new paradigm [2].

However, there still exist many problems in cloud computing today. A recent survey by Cloud Security Alliance (CSA) shows that security have become the primary concern for people to shift to cloud computing.

In this paper, we survey the security concerns of current Cloud Computing systems. As Cloud Computing referred to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centers) that provide those services [4], we present the security concerns in terms of the diverse applications and infrastructures. More concerns on security issues, such as availability, confidentiality, integrity control, authorization and so on, should be taken into account.

II. KEY CHARACTERISTICS OF CLOUD COMPUTING

1. On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service's provider[5].
2. Ubiquitous network access: Accessed through standard mechanisms on heterogeneous thin and thick clients. Both high bandwidth and low latency are expected[5].
3. Location-independent resource pooling: The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. Rapid elasticity: Lets us quickly scale up (or down) resources.
5. Measured service: are primarily derived from business model properties and indicate that cloud service providers control and optimize the use of computing resources through automated resource allocation, load balancing, and metering tools[5].

III. THREE LAYERS OF CLOUD COMPUTING

The three architectural layers of Cloud Computing are (see Fig. 1):

i) Infrastructure as a Service (IaaS) : Here, the IT resources like operating system, middleware packages like Microsoft .Net and data storage facility on demand with administrative capability are provided. The users avail the cloud facility through virtualization, e.g. using software package like VMWARE [3].

ii) Platform as a Service (PaaS): Here, facilities like development of applications with middleware packages, Web development tools etc are provided. The PaaS also provides the facilities like running of applications, hosting of Web services, data storage[3].

iii) Software as a Service (SaaS): Here, some applications like e-mail usage with limited administrative capability and storage facility are provided.

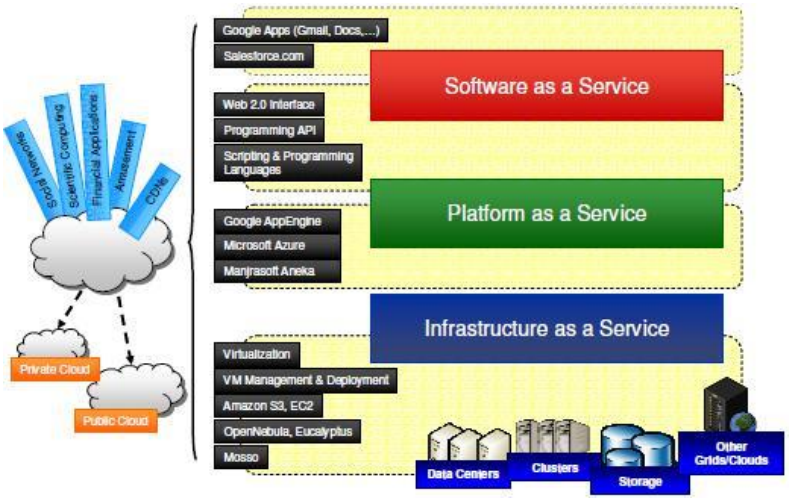

Fig 1. Cloud Computing Architecture

IV. CLOUD DEPLOYMENT MODELS

There are four cloud deployment models:

i) Public cloud: In public cloud, the resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services. The customers can quickly access these resources, and only pay for the operating resources. As multiple customers are sharing the resources so major dangers to public cloud are of security, regulatory compliance and Quality of Service (QoS) [6, 7, 8].

ii) Private cloud: In the private cloud, computing resources are used and controlled by a private enterprise. In private cloud, resource access is limited to the customers that belong to the organization that owns the cloud. The main advantage of this model is that the security and privacy of data is increased as compliance and QoS are under the control of the enterprises [6, 7].

iii) Hybrid cloud: A third type can be hybrid cloud that is typical combination of public and private cloud. Through this environment an organization can provide and manage certain resources in-house and have others provided through external resources.

iv) Community cloud: The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

V. SECURITY ISSUES ASSOCIATED WITH THE CLOUD

There is a number of security issues associated with cloud computing. These issues are categories as: security issues faced by cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

The following list contains several security issues highlighted by Gartner [9]:

- Privileged access: Who has specialized/privileged access to data? Who decides about the hiring and management of such administrators?
- Data location: Does the cloud vendor allow for any control over the location of data?
- Data segregation: Is encryption available at all stages, and were these encryption schemes designed and tested by experienced professionals?
- Data availability: Can the cloud vendor move their entire client's data onto a different environment should the existing environment become compromised or unavailable?
- Regulatory compliance: Is the cloud vendor willing to undergo external audits and/or security certifications?
- Recovery: What happens to data in the case of a disaster, and does the vendor offer complete restoration, and, if so, how long does that process take?
- Investigative Support: Does the vendor have the ability to investigate any inappropriate or illegal activity?
- Long-term viability: What happens to data if the cloud vendor goes out of business, is client's data returned and in what format?

VI. KEY MANAGEMENT ROLE

Key management plays an important role enforcing access control on the group key (and consequently on the group communication). It supports the establishment and maintenance of key relationships between valid parties according to a security policy. It encompasses techniques and procedures that can carry out[11]:

i) Providing member identification and authentication: Authentication is important in order to prevent an intruder from impersonating a legitimate group member. In addition, it is important to prevent attackers from impersonating key managers. Thus, authentication mechanisms must be used to allow an entity to verify whether another entity is really what it claims to be.

ii) Access control: After a party has been identified, its join operation should be validated. Access control is performed in order to validate group members before giving them access to group communication (the group key, in particular)[12].
iii) Generation, distribution and installation of key material: It is necessary to change the key at regular intervals to safeguard its secrecy. Additional care must be taken when choosing a new key to guarantee key independence. Each key must be completely independent from any previous used and future keys, otherwise compromised keys may reveal other keys.

VII. KEY MANAGEMENT FUNCTIONS

The following are the important key management functions [10]:

- Generate Key
- Generate Domain Parameters
- Bind Key and Metadata
- Bind a Key to an Individual
- Activate Key
- Deactivate Key
- Backup Key
- Recover Key
- Modify Metadata
- Rekey
- Suspend a Key
- Restore a Key
- Revoke a Key
- Archive a Key
- Destroy a Key
- Manage TA Store

VIII. KEY MANAGEMENT SECURITY REQUIREMENTS

The following are general key management security requirements:[10]

1. Parties performing key management functions are properly authenticated and their authorizations to perform the key management functions for a given key are properly verified.
2. All key management commands and associated data are protected from spoofing, i.e., source authentication is performed prior to executing a command.
3. All key management commands and associated data are protected from undetected, unauthorized modifications, i.e., integrity protection is provided.
4. Secret and private keys are protected from unauthorized disclosure.
5. All keys and metadata are protected from spoofing, i.e., source authentication is performed prior to accessing keys and metadata.
6. All keys and metadata are protected from undetected, unauthorized modifications, i.e., integrity protection is provided.
7. When cryptography is used as a protection mechanism for any of the above, the security strength of the cryptographic mechanism used is at least as strong as the security strength required for the keys being managed.

IX. BENEFITS AND DISADVANTAGES OF CLOUD COMPUTING

A. The Benefits of Cloud Computing:

Cloud computing offers the possibility of extending the information system of an enterprise at the request of the latter, according to the intended use. Services provided in the cloud are extensive. Particularly, the Company may benefit from the capacity of processing information, infrastructure, storage capacity and storage as well as computer applications [1].

B. The Disadvantages of Cloud Computing:

Cloud computing seems to promise a great future. Many people or companies are against this notion, as the famous Richard Stallman (founder of the "Free Software Foundation")[1] who starts from cloud computing as a trap. The problem that comes up most is related security. How to guarantee the security of information stored in the cloud? More broadly Cloud Computing leads to the loss of control over the lifecycle of applications.

X. CONCLUSION

Cloud computing is a new technology widely studied in recent years. Now there are many cloud platforms both in industry and in academic circle. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Many enhancements in existing solutions as well as more mature and newer solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. Cloud computing is still in its infancy, and how the security and privacy landscape changes will impact its successful, widespread adoption. These issues mentioned above will be the research hotspot of cloud computing. There is no doubt that cloud computing has a bright future.

REFERENCES

[1] Laboratoire de recherche xbrainlab, Le Cloud Computing : Réelle révolution ou simple evolution, Livre blanc, 2011.
[2] Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Application 1(1), 7–18 ,2010.
[3] Atanu Basu, Indranil Sengupta, and Jamuna Kanta Sing : Secured Cloud Storage Scheme Using ECC Based Key Management in User Hierarchy, ICISS 2011, Springer-Verlag Berlin Heidelberg.
[4] Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A.: Security and privacy in cloud computing: a survey. In: The Proceedings of IEEE 6th International Conference on Semantics, Knowledge and Grids, pp. 105–111,2010.
[5] Mell, P.,Grance, T.: The NIST definition of Cloud Computing, version - 15. National Institute of Standards and Technology (NIST), Information Technology Laboratory October 7, 2009, http://www.csrc.nist.gov.
[6] Takabi, H, Joshi, J.B.D.: Security and privacy challenges in cloud computing environment. IEEE Journal on Security and Privacy 8(6) ,November 2010.
[7] Yang, J., Chen, Z.: Cloud computing research and security issues. In: The Proceeding of IEEE International Conference on Computational Intelligence and Software Engineering, pp. 1–3 ,2010.
[8] Kaur, P., Kaushal, S.: Security concerns in cloud computing. In: Accepted For International Conference on High Performance Architecture And Grid Computing-2011. Chitkara University, Rajpura 2011.
[9] Brodkin, J.: Gartner: Seven cloud-computing security risks. In: Infoworld 2008, http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-53?page=0,1.
[10] Ramaswamy Chandramouli,Michaela Iorga: Cryptographic Key Management Issues & Challenges in Cloud Services.
[11] Sandro rafaeli , David Hutchison: A Survey of Key Management for Secure Group Communication ,Computing Department, Lancaster University ACM Computing Surveys, Vol. 35, No. 3, September 2003.
[12] Damgrd, Ivan, et al. "Secure key management in the cloud." Cryptography and Coding. Springer Berlin Heidelberg, 2013. 270-289.