Data Security Models in Cloud Computing

Paridhi Singhal

Abstract: Cloud computing provides convenient on-demand network access to a shared pool of configurable computing resources. The resources can be rapidly deployed with great efficiency and minimal management overhead. Cloud is an insecure computing platform from the view point of the cloud users, the system must design mechanisms that not only protect sensitive information by enabling computations with encrypted data, but also protect users from malicious behaviors by enabling the validation of the computation result. There is a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers [1]. In the following report we would like to establish the various security related concerns, their implementations and policies. We first start of by determining the various vulnerabilities that could infrastructures face after which we explain the challenges in facing these security related issues. Once the vulnerabilities are identified we can propose security models.

Index Terms: Cloud Computing, Data Integrity, Data Recovery, Security, Design, Reliability.

1 INTRODUCTION

Organizations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments. Cloud promises huge cost benefits, agility and scalability to the business [2]. All business data and software are stored on servers at a remote location referred to as Data centers. Data centre environment allows enterprises to run applications faster, with easier manageability and less maintenance effort, and more rapidly scale resources (e.g. servers, storage, and networking) to meet fluctuating business needs. A data center in cloud environment holds information that end-users would more traditionally have stored on their computers. This raise concerns regarding user privacy protection because users must outsource their data [3]. The movement of data to centralized services could affect the privacy and security of users' interactions with the files stored in cloud storage space. The use of virtualized infrastructure as a launching pad might introduce new attacks to user's data. Data integrity is defined as the accuracy and consistency of stored data, in absence of any alteration to the data between two updates of a file or record. Cloud services should ensure data integrity and provide trust to the user privacy. Although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it's lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users [3]. Cloud computing poses privacy concerns primarily, because the service provider at any point in time, may access the data that is on the cloud. The Cloud service provider could accidentally or deliberately alter or delete some information from the cloud server. Hence, the system must have some sort of mechanism to ensure the data integrity. The current Cloud security model is based on the assumption that the user/customer should trust the provider. This is typically governed by a Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations.

In order to ensure the integrity and availability of data in Cloud and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. However, the fact that users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional cryptographic primitives for the purpose of data integrity protection [3]. Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the entire data files [3], [4], [5], [6]. The data stored in the cloud may not only be accessed but also be frequently updated by the users, including insertion, deletion, modification, appending, etc. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging [7]-[3].

While cloud security concerns can be grouped into any number of dimensions all these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues. It is also important to understand the levels at which there can be security vulnerabilities in our opinion the following areas can be identified where security loop holes can appear and hence safeguarding these fronts is essential.

- VM Security- Related to the virtual infrastructure vulnerabilities.

• Data Security- Related to data storage vulnerabilities
• Software Security- Application vulnerabilities

2 TYPES of VULNERABILITIES

2.1 VM Placement attacks

In this particular vulnerability, it is possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed in the vicinity of the target. Such a placement can then be used to mount cross-VM side-channel attacks to extract information from a target VM on the same machine. Particularly, to maximize efficiency multiple VMs may be simultaneously assigned to execute on the same physical server. Moreover, many cloud providers allow "multitenancy" — multiplexing the virtual machines of disjoint customers upon the same physical hardware [8]. Thus it is conceivable that a customer's VM could be assigned to the same physical server as their adversary. This in turn, engenders a new threat — that the adversary might penetrate the isolation between VMs and violate customer confidentiality.

2.2 Securing Data Storage

Cloud Computing inevitably poses new challenging security threats for a number of reasons:-

- Data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.
- There are some techniques that have been proposed in this regard can be useful to ensure the storage correctness without having users possessing data, but these techniques cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations [7].
- Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss of control of their data under Cloud Computing.

Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging [7].

2.3 Hypervisor Holes

In a virtualized cloud environment, each client has a VM that is running client specific applications. As the operating system (OS) of cloud provider is running multiple VMs concurrently, it's a challenging task to manage the entire VMs. Recently; however, black hat hackers and other security experts have discovered security holes in some hypervisor implementations. Hypervisors are getting more and more common, and are growing in deployment in everything from datacenter systems to embedded consumer electronics. But, as their deployment increases, more and more security concerns come into play, including a variety of attack methods and the dire consequences of a compromised hypervisor.

Holes include the ability to insert code into virtual machines, the disclosure of unauthorized information, and potential disruption of service [10]. The following figure1 depicts the architecture of the role that a hypervisor plays. Once a compromise is made at the hypervisor level one can easily penetrate the operating system that resides on that particular VM and its storage system including the access to perform malicious operations on the applications that reside on the machines. So if one were to breach the hypervisor running several varieties of guest operating systems, one could use root access to the hypervisor to commit dirty deeds such as planting root kits into the memory of running operating system kernels, performing file system trickery as a side-effect of having direct, raw access to nonvolatile storage mediums, and pretty much anything one wished to do.

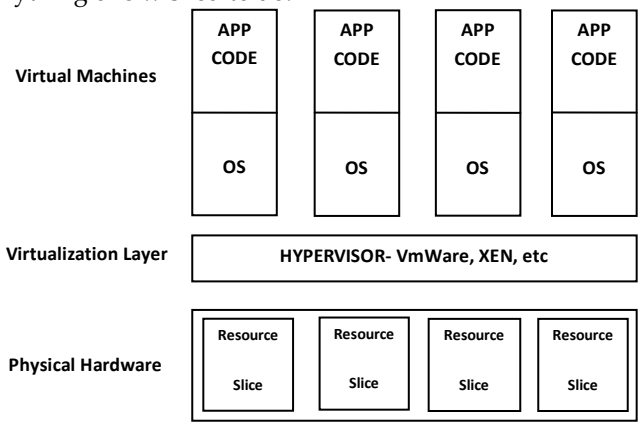

Figure 1: Architecture of Hardware Virtualization with Virtual Machines

3 CLOUD SERVICE DEPLOYMENT AND CONSUMPTION MODALITIES

It is very important to understand which kind of service fits the category of cloud computing that is being offered by the provider. With the growth in the usage of cloud computing many different models of providing cloud services have emerged. For now, regardless of the delivery model utilized (SaaS, PaaS, IaaS,) there are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services:-

3.1 Public Cloud

A public cloud is one in which the services and infrastructure are provided off-site over the internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks.

3.2 Private Cloud

A private cloud is one in which the services and infrastructure are maintained on a private network. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings. [11].

3.3 Hybrid Cloud

A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises". By integrating multiple cloud services users may be able to ease the transition to public cloud services while avoiding issues such as PCI compliance. [12].

4 SYSTEM MODEL

Cloud networking can be illustrated by three different network entities:

4.1 User:

Who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations?

4.2 Cloud Service Provider (CSP)

Who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

4.3 Third Party Auditor (TPA)

Who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

4.4 Adversary Model [13]

There are two different sources for Security threats faced by cloud data storage.

CSP can be self-interested, un-trusted and possibly malicious. It may move data that is rarely accessed to a lower tier of storage for monetary reasons, but it may hide a data loss incident due to management errors, Byzantine failures and so on.

Economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users 'data while remaining undetected by CSPs for a certain period [14].

There are two types of adversary

Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent [9].

5 Models for Security in Cloud

Needless to say depending on the kind of the cloud service being provided by a vendor a respective security model has to be adopted. There cannot be one universally accepted security model but refinements can be made to distinguish and recognize the areas that need protection. Apart from this enhancements to security policies can be undertaken corresponding to every type of cloud service offered. In the recent times there have been some proposals related to the kind of security models that can be referenced by cloud computing vendors. Here is a description of such security models.

5.1 Cloud Storage Model

The Cloud storage systems might provide massive storage space at same time be cost effective. However potential users will be reluctant to move sensitive data to the cloud unless the security issues are well addressed. This model proposes a new protocol called Multi-Party Non-Repudiation (MPNR) which takes one of three important security issues disputation, fairness and roll-

back attacks in storage. The protocol ensures that every message has data transmission information as evidence in the form of NRR (Non-Repudiation of Receipt) or NRO (Non-Repudiation of Origin) [8]. When exchange of message needs to made non-repudiation information is exchanged between the two interacting parties. For e.g.: The Originator who wants to send information to a group who first upload information to the cloud using the NRO message. The cloud service provider would then verify the message and then send NRR to the originator, who in turn encrypts both NRO and NRR using a group encryption and send it to them. Now a user in the group could send a request to the provider for the data using the messaged received.

The example demonstrated what happens in a normal working mode, however if the originator or the user does not receive a valid message from the provider it goes into the resolve mode wherein a trusted third party (TTP) where a new session is started using a reliable channel monitored by the TTP which ensures that the originator or the user always gets back a reply from the provider [8].

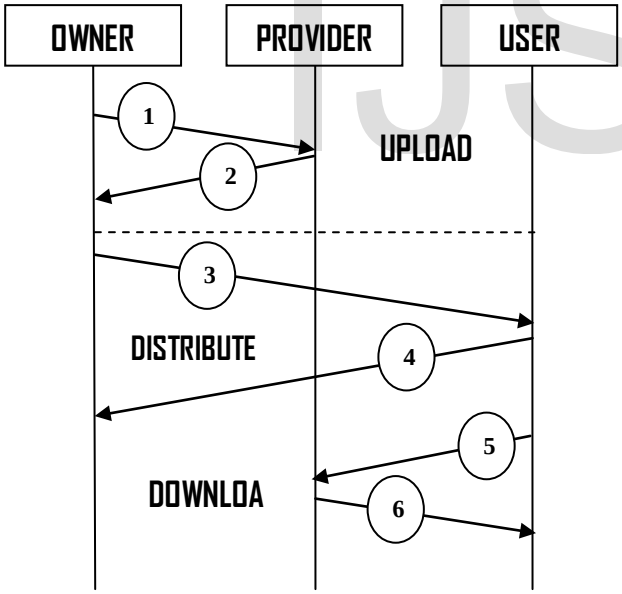

Figure 2: Cloud Storage Model

5.2 Three level security model

In this model, there are three-levels of defense system structure, in which each layer performs its own duty to ensure that the data security of cloud layers.

The first layer: responsible for user authentication, the user of digital certificates issued by the appropriate, manage user permissions.

The second layer: responsible for user's data encryption, and protect the privacy of users through a certain way.

The third layer: The user data for fast recovery, system protection is the last layer of user data.

With three-level structure, user authentication is used to ensure that data is not tampered. The user authenticated can manage the data by operations: Add, modify, delete and so on. If the user authentication system is deceived by illegal means, and malign user enters the system, file encryption and privacy protection can provide this level of defense. In this layer user data is encrypted, even if the key was the illegally accessed, through privacy protection, malign user will still be not unable to obtain effective access to information, which is very important to protect business users' trade secrets in cloud computing environment. Finally, the rapid restoration of files layer, through fast recovery algorithm, makes user data be able to get the maximum recovery even in case of damage.

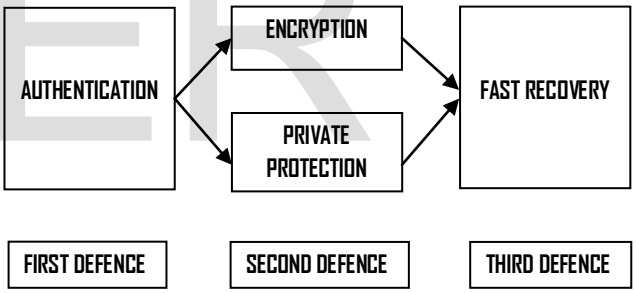

Figure 3: Data Security Model

CONCLUSION

Cloud Computing is gaining remarkable popularity in the recent years for its benefits in terms of flexibility, scalability, reliability and cost effectiveness. Despite all the promises however, Cloud Computing has one problem: Security. In this paper, we studied the problems of data security, VM Security and Software, which are essentially a distributed storage system. An effective and flexible distributed scheme is proposed to ensure the correctness of9 users' data in the cloud servers. If this correctness verification is too much resource consuming on the user's side, the task can be delegated to the third party auditor and the pre-computed tokens could be either in the user's local device or cloud server in encrypted format. By detailed

security and performance analysis, we show that our scheme is highly efficient in recovering the singleton losses almost immediately and recovers from busty data losses. Having covered the different vulnerabilities faced and also the security models used in cloud we see that the success of a service or application in cloud is highly dependent on "how secure the cloud system is? Of course there are factors and guidelines that can be developed in order to ensure maximum security in cloud environments. Security in cloud needs to be constantly updated to ensure that that they are not riddled by attacks. The domain of security in cloud will be the deciding factor in the success or failure of a cloud system in future

REFERENCE

[1].wikipedia
http://en.wikipedia.org/wiki/Cloud_computing_security
[2]. Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K. Chaurasiya, Rahul Gupta, "An architecture based on proactive model for security in cloud computing" in IEEE-International Conference on Recent Trends in Information Technology, June 2011.
[3]Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.
[4]. D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.
[5]. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.
[6] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in Proc. of ACM workshop on Cloud Computing security (CCSW'09), 2009, pp. 43–54.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. of IWQoS'09, July 2009, pp. 1–9.
[8] Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds by Thomas Ristenpart, Eran Tromer, Hovav Shacham and Stefan Savage.
[9] Enhancing Cloud Storage Security against Roll-back Attacks with A New Fair Multi-Party Non-Repudiation Protocol by Jun Feng, Yu Chen, Douglas Summerville, Wei-Shinn Ku, Zhou S.
[10] Security in Public and Private Cloud Infrastructures, Joyent white paper.
[11]Rohit Maheshwari, Department of Computer Science, Kautilya Inst. Of Technology, International Journal of Recent Technology and Engineering (IJRTE) ,March. 27, 2012
[12] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology, International Journal of Recent Technology and Engineering (IJRTE) , April ,12- 2011
[13] National Institute of Standards and Technology - Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing/
[14] Security Guidance for Critical Areas of Focus in Cloud Computing. http://www.cloudsecurityalliance.org/guidance/csaguide.pdf.