Cloud Computing

Security in Cloud Computing - Vulnerabilities, Challenges, Models and path ahead

By
Anand Mukundan
Bina Bhaskar

1. Abstract

Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There are 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 most cases, the provider must ensure that their infrastructure is secure and that their clients’ data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. 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 that can be referenced to combat such threats hence, we would also like to discuss certain security models that have been proposed in recent times.

2. Introduction

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

One of the major reasons why cloud computing has gained momentum in the recent times is the availability of cheap and affordable infrastructure which reduces the investment costs by a great deal. There have been many studies carried out in the recent times to expose the extent and importance of security vulnerabilities in cloud. One may ask “why is this such an important issue to consider?” In response to this, there have been many surveys and studies that have been undertaken recently which clearly indicate that security concerns make cloud computing less popular among certain business sectors. Concerns related to the above mentioned categories of vulnerabilities have made cloud computing less adaptable to certain business sectors such as health and pharmacy sector, some business sectors, government and research facilities. One of the major concerns of these sectors is the way data is stored
Cloud Computing

Cloud computing is a service oriented architecture as can be seen from the above figure, it provides application, infrastructure and platform as services. As can be inferred from the figure above due to the complexity of the architecture and just the fact that all these services can be shared between so many devices makes the architecture more prone to security attacks since many loopholes can be detected and exploited. Thus, with regard to cloud computing it is the responsibility of the various service providers to assess all the security threats and provide appropriate security audits to the customers. One of the major reasons of concern amongst customers is the lack of enough details regarding measures taken to ensure security. Such a situation arises when the providers do not provide enough details about the security measures adopted by them and insist that consumers only go by the reputation of the provider or basically trust that the provider would have met all the requirements since even the consumers might not have enough knowledge base about security issues.
"Ultimately, we believe that the best solution is simply to expose the risk and placement decisions directly to users," the researchers say. "A user might insist on using physical machines populated only with their own VMs and, in exchange, bear the opportunity costs of leaving some of these machines underutilized. Regardless, we believe such an option is the only foolproof solution to this problem and thus is likely to be demanded by customers with strong privacy requirements." [8]

Thus it is very essential for the consumers and vendors to identify the vulnerabilities that may exist and it is equally essential for the vendors to provide the consumer with the appropriate documentation regarding security audits and measures taken to combat the vulnerabilities. In the following section we make a list of vulnerabilities that a consumer and vendor must be aware of.

4. Types of Vulnerabilities

4.1 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 [5]. The following figure 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 rootkits into the memory of running operating system kernels, performing file system trickery as a side-effect of having direct, unabstracted/raw access to nonvolatile storage mediums, and pretty much anything one wished to do.

4.2 Securing Data Storage –

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for a number of reasons. 

- The 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.
- Some of the 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 [2].
- 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 [2].

In most of adversary models related to securing a cloud storage system the following kinds of attackers are identified. By identifying the target of the attacker better preventive measures can be put in place to check such attacks.

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. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident [3].

4.3 VM Placement attacks –

According to 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. In particular, to maximize efficiency multiple
Cloud Computing

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 [4]. 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 (e.g., via a vulnerability that allows an “escape” to the hypervisor or via side-channels between VMs) and violate customer confidentiality.

Side channel attacks include:

- Denial of Service
- Measure cache usage (measure CPU utilization on the physical machine; or “how busy are their servers?”)
- Load-based co-residence detection (aka detecting co-residence without relying on sending any network probes)
- Estimating traffic rates (sounds harmless but can be used to deduce targets activity patterns, peak trading times for maximal DoS effect etc)
- Keystroke timing attack (remote keystroke monitoring)

“The researchers were able to pinpoint the physical server used by programs running on the EC2 cloud and then extract small amounts of data from these programs, by placing their own software there and launching a side-channel attack. Security experts say the attacks developed by the researchers are minor, but they believe side-channel techniques could lead to more serious problems for cloud computing.” [10]

4.4 XML Signature –

SOAP (Simple Object Access Protocol) is an XML based protocol consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing procedure calls and responses. By modifying the XML content of the message a malicious user can make sure that the resulting message still contains a valid signature of a legitimate user, thus the service executes the modified request.

Setting up a virtual machine to send spam mails is just one example what an attacker can do—using the legitimated user’s identity and charging his account [6].

4.5 Malware Injection Attack –

In this attack the adversary creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and adds it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary’s code is executed. Such an attack could be a major hindrance to bank applications in the cloud as malicious applications taking its place could swindle the bank’s clients [6].
4.6 Denial of Service –

When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually to some extent even supports the attacker by enabling him to do most possible damage on a service’s availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service.

In the worst case, an adversary manages to utilize another Cloud Computing system for hosting his flooding attack application. In that case, each Cloud would provide more and more computational resources for creating, respectively fending, the flood, until one of them eventually reaches full loss of availability [6].

5. 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 four primary ways in which Cloud services are deployed and are characterized,
5.1 Private
Private Clouds are provided by an organization or their designated service provider and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of Cloud. The physical infrastructure may be owned by and/or physically located in the organization’s datacenters (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively. The consumers of the service are considered “trusted.” Trusted consumers of service are those who are considered part of an organization’s legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

A great example of this could be VMWare or Citrix with the virtual servers hosting given applications, maybe virtual desktops running on Thin Clients, or even applications being hosted on a central system and delivered to a user via a client. Citrix has been a leader in that market for years with their metaframe product line, and now their Xenapp product line.

5.2 Public
Public Clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of Cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider’s datacenters (off-premise.) Consumers of Public Cloud services are considered to be untrusted.

In a public cloud environment, the end user has a solution that is highly automated. Customers can put their applications in the cloud and control all of the individual attributes of their services. The public cloud does not have the visibility or control of a private model. You give up some control over the location of processing when using the public cloud. In a private cloud, you have fewer people sharing resources with more pinpoint control. Managing the security risks of each environment is attainable by following some best practices for both internally and externally.

5.3 Managed
Managed Clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of Cloud. The physical infrastructure is owned by and/or physically located in the organization’s datacenters with an extension of management and security control planes controlled by the designated service provider. Consumers of Managed Clouds may be trusted or untrusted.

5.4 Hybrid
Hybrid Clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate Cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. Consumers of Hybrid Clouds may be trusted or untrusted.
Cloud Computing

A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other. Here are a couple of situations where a hybrid environment is best.

- Your company wants to use a SaaS application but is concerned about security. Your SaaS vendor can create a private cloud just for your company inside their firewall. They provide you with a virtual private network (VPN) for additional security.
- Your company offers services that are tailored for different vertical markets. You can use a public cloud to interact with the clients but keep their data secured within a private cloud.

The management requirements of cloud computing become much more complex when you need to manage private, public, and traditional data centers all together which becomes a rather daunting task.

“To complicate things, the lines between private and public clouds are blurring. For example, some public cloud companies are now offering private versions of their public clouds. Some companies that only offered private cloud technologies are now offering public versions of those same capabilities.”


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.

6.1 Three level security model –

![Figure 4: Data Security Model for Cloud Computing](image)
This model uses three-level 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.

6.2 Cloud Cube Model –

The Jericho Forum has identified 4 criteria to differentiate cloud formations from each other and the manner of their provision. The Cloud Cube Model summarizes 4 dimensions. The purpose of having such a model is to clearly understand at what level security needs to be re-enforced and at what level the data is stored which in turn allows us to judge the kind of policies that can be put in place to protect it [8].

![Figure 5: Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration by Jercho Forum](image)

**Dimension 1: Internal (I) / External (E)**

This is the dimension that defines the physical location of the data: where does the cloud form you want to use exist - inside or outside your organization’s boundaries.
• If it is within your own physical boundary then it is Internal. Hence any enforcement of security policy is your concern there is complete independence since all the factors must be within a known periphery.
• If it is not within your own physical boundary then it is External. Enforcing security is a major concern here since there might be unknown factors to consider as well, it requires a lot of research to identify possible vulnerabilities and then to find ways to encounter them is the next step.

**Dimension 2: Proprietary (P) / Open (O)**
This is the dimension that defines the state of ownership of the cloud technology and services. It indicates the degree of interoperability, as well as enabling “data/application transportability” between your own systems and other cloud forms, and the ability to withdraw your data from a cloud form or to move it to another without constraint. It also indicates any constraints on being able to share applications.
• Proprietary means that the organization providing the service is keeping the means of provision under their ownership. As a result, when operating in clouds that are proprietary, you may not be able to move to another cloud supplier without significant effort or investment.
• Clouds that are open are using technology that is not proprietary, meaning that there are likely to be more suppliers, and you are not as constrained in being able to share your data and collaborate with selected parties using the same open technology.

**Dimension 3: Insourced / Outsourced**
“Who do you want running your Clouds?” This is the question that is answered by this dimension. Depending on answers to this question one can make a choice of what level of security needs to be implemented. Most of the policies are decided in this stage and it is important that the providers of the service make sure to provide the consumers with appropriate documentation and audits about the valid security measure adopted. These 2 states describes who is managing delivery of the cloud service(s) that you use. This is primarily a policy issue (i.e. a business decision, not a technical or architectural decision) which must be embodied in a contract with the cloud provider.
• Outsourced: the service is provided by a 3rd party
• Insourced: the service is provided by your own staff under your control

**6.3 Cloud Storage Model**

![Cloud Storage Model: Normal Session working flow analysis](image)

Figure 6: Cloud Storage Model: Normal Session working flow analysis
Cloud storage systems might provide massive storage space at the 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 on 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) [4].

When exchange of message needs to be made non-repudiation information is exchanged between the two interacting parties. For example, 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 message 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 [4].

7. Policies

7.1 Application security –

- Securing inter-node (or host) communications must be done as there can be no assumption of a secure channel to exist between nodes (or hosts).
- It is important to manage application credentials and key material.
- Care should be undertaken with the management of files used for application logging and debugging, as the locations of these files may be remote or unknown and could contain sensitive information.
- Customers must secure permissions to perform remote vulnerability assessments from Cloud Service Providers.
- Different surveys and measurements should be used to gauge the effectiveness of application security programs to thwart/mitigate security threats.
- Attention should be paid to how malicious actors will react to new cloud application architectures that hide application components from their access [7].

7.2 Maintaining Integrity –

- Usage of encryption would ensure that only authenticated users can access the data.
- When opting for encryption care must be taken to select the technique that adheres to the present standards.
Cloud Computing

- We must separate the keys used for encryption from the cloud provider that hosts the data ensuring that the cloud provider that hosts the data cannot access the data due to the presence of the keys locally.
- In case of Key Management to be done by the provider the user must be kept informed of how the keys are generated, deleted and whether the same key is used for multiple users.
- Attention should be paid to how sensitive information will be handled and what encryption mechanisms are used to protect the data by default [7].

7.3 Authentication / Access Control –

- Creating a VPN connection to connect to an IaaS will ensure that no malicious user can sniff packets when an authorized user is working with the infrastructure.
- Access privileges extended to different set of users must be controlled appropriately to ensure that there is no kind of misuse.
- One of the different successful authentication techniques like kerberos, one-time passwords and digital signatures should be carefully selected and adopted by cloud providers.
- Enterprises should consider using user-centric authentication such as Google, Yahoo, OpenID, Live ID, etc., to enable use of a single set of credentials valid at multiple sites.
- Cloud customers should change or add to their authoritative repositories of identity data so that it contains cloud applications/processes.
- Access control model must be selected after carefully considering the user profile information and privacy policies for the data, thereby ensuring the appropriateness of the model [7].

In addition to the above policies there are following which need to be taken care of:

- We must communicate with the cloud provider in case there is a (or suspect) breach into our data or application
- Study how the cloud provider handles the data with respect to storage so that we can adopt the best possible security model to protect it.
- We must also verify to see that the cloud provider is adopting all the requirements as expected by the client.
- Virtualized operating systems should be supported by security technology provided by third party vendors in order to reduce dependency on the platform provider.
- The users must ensure the validation any VM image originating from the cloud provider before using it to ensure that the state of the VM has remained the same since last used by the user.

8. Road ahead for Security in Cloud

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? Ofcourse 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.
9. Suggested Framework

- User level authentication is done by enforcing the usage of three level security framework. This model ensures that only valid users can login into the system.
- In order to ensure non-repudiation, fairness and avoidance of replay attacks we make use of the cloud storage model which is basically meant for the data storage protection.
- Additionally we also provide non-repudiation between the data and application (can be done by technologies like watermarking) to make sure that only permitted applications can process the corresponding data.
- In order to prevent attacks from other malicious users we have a unique firewall like mechanism in place to permit only valid users to access the data and applications.
- Finally, based on the dimensions mentioned in the cloud cube model we can select the appropriate policies required to guide the smooth functionality of the cloud system, which will ensure the applicability of all the legal and regulatory norms related to data storage and usage in the cloud environment.

10. References


Cloud Computing


