A SURVEY ON CLOUD COMPUTING THREATS

***S. Nirmal**
Assitant Professor
Sambram College
Bangalore

ABSTRACT

Cloud computing has been envisioned as the next generation architecture of IT enterprise. Cloud shared infrastructure & associated services make it cost-effective alternative to the traditional approaches. However this new approach may also introduce new security breaches & privacy issues. Many research works on cloud security exists in partial forms.

In this paper an attempt has been made to consolidate the various threats in a classified manner and to illustrate how these vulnerabilities affect the different cloud computing service models.

Keywords: Cloud Computing, Security Challenges, Threats.

1. INTRODUCTION

Cloud is a synonym for describing web as a space where computing has been preinstalled & exist as a service such as information, infrastructure, applications, storage and processing power. It exists on the web ready to be shared. To the users cloud computing is a pay-per-use-on demand environment that can be easily accessed for shared IT resources through internet.

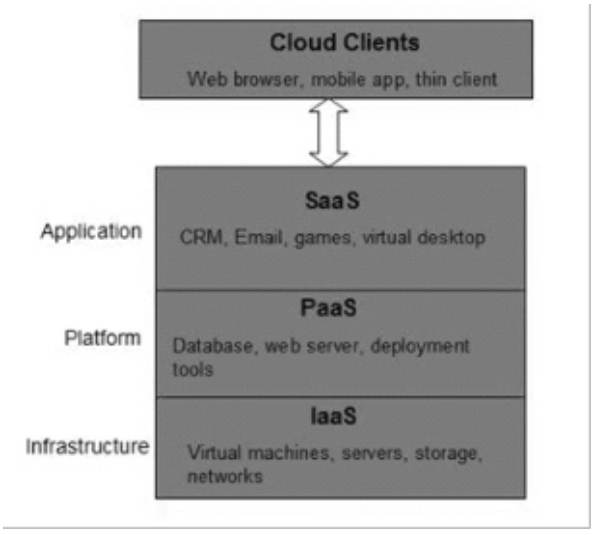
Cloud computing has been widely practiced by IT industry as well as business enterprises in the recent times but research on it is still at immature stage, many existing issues have not been fully addressed, newer problems are arising due to its extensive usage.

2. CLOUD SERVICE MODELS

Cloud computing can be classified based on services offered and deployment models.

According to the services offered cloud computing can be considered to consist of three layers.

IaaS : Infrastructure as a Service is the lowest layer that provides basic infrastructure support service. IaaS refers to the sharing of H/W resources for executing services typically using virtualization technology. With IaaS approach multiple users can use the available resources. The resources can be easily scaled up on demand from users & are charged pay-per-use basis. They all are virtual machines thus a governance framework is required to control the creation & usage of virtual machines.



PaaS : Platform as a service is the middle layer which offers platform oriented services besides providing the environment for hosting the user's applications.PaaS model aims at protection of data especially in case of Storage- as- a – service.

SaaS : Software as a Service is the topmost layer which features a complete application offered as a service on demand [1,2]. SaaS ensures that the complete applications are hosted on the internet & user uses them. The payment is made on a pay-per-use model. It eliminates the need to install & run the application on the customer's local computer. Thus reducing the burden of software maintenance.

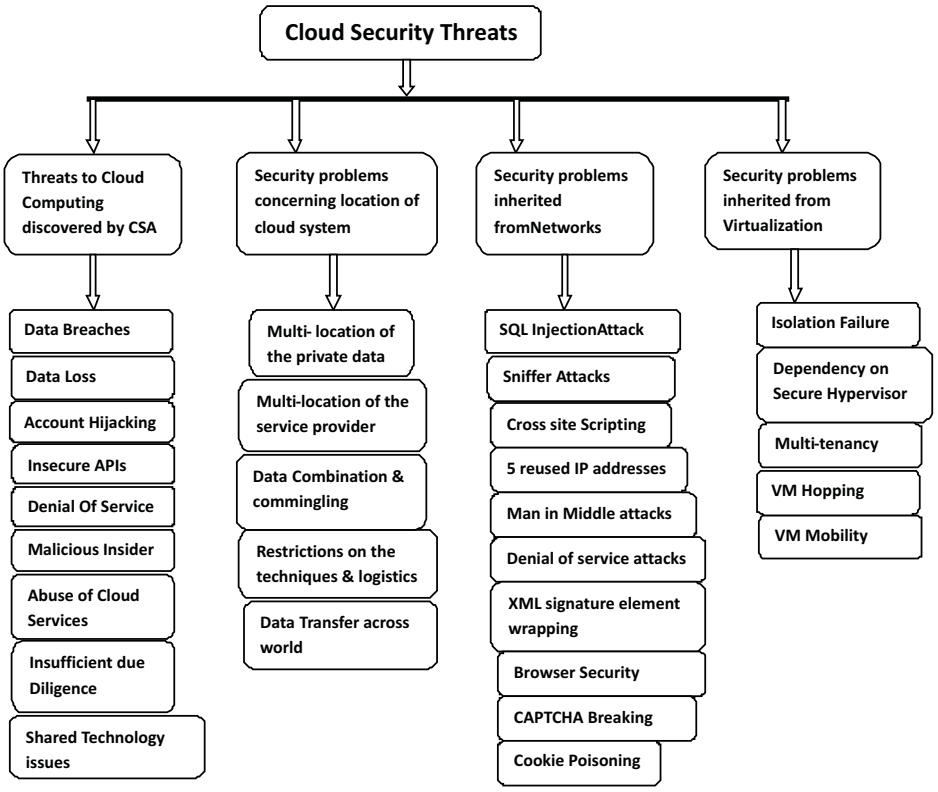
Two types of servers are used by SaaS model, Main Consistence Server (MCS) & Domain Consistence Server (DCS). If MCS is damaged or compromised the control over the cloud environment is lost. Hence securing MCS is of great importance.

3. SECURITY ISSUES FOR CLOUDS

There are numerous security issues for cloud computing as it encompasses many technologies including Networks, Databases, Operating Systems, Virtualization, Resource scheduling, Transaction Management, Load Balancing, Concurrency control & Memory Management. Therefore security issues for many of these systems & technologies are applicable to cloud computing.

For example the N/W that interconnects the systems in a cloud has to be secured. Virtualization introduces several security issues in cloud computing. Security problems related to the location of the cloud system in addition to the resource allocation & memory management algorithms have to be secure.

The schematic diagram depicts the security threats at various levels.



In this paper only Threats to cloud computing discovered by "Cloud Security Alliance" are illustrated (CSA)[3]

Cloud Security Alliance is a well-known community related to the cloud security. It has proposed the threats of cloud systems. These threats are illustrated as follows and are ranked according to the severity:

3.1: Data Breach:

It is a top threat by which an organizations sensitive internal data falls into the hands of their competitors. Cloud Computing introduces significant new avenues of attack. The researchers have published a paper on how a virtual machine could use side channel timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. However in many cases if a multitenant cloud service database is not properly designed a flaw in one client application could allow an attacker not only client's data but every other client's data as well. [4]

Encryption may be used to reduce the impact of data breach but if the encryption key is lost then the data is lost. Conversely if we decide to keep offline backups of data to reduce the impact of data loss this increases the exposure to data to data breach.

3.2: Data Loss:

Data loss refers to the permanent unavailability of data. This may be due to data stolen from the data center virtually or even physically. Data stored in the cloud can be lost due to reasons other than malicious attacks. Any accidental deletion by the cloud service provider or a physical catastrophe such as fire, earthquake etc could lead to permanent data loss, unless the provider takes adequate measures to backup data.

Further the burden of avoiding data loss is not only the responsibility of the service provider because if a customer encrypts his or her data before uploading it to the cloud but lose the encryption key the data is unavailable for use.

3.3: Account/ Service Hijacking:

Attacks such as Phishing, Spam Campaigns & Denial of service attacks still achieve results, credentials & passwords are often reused which amplifies the possibilities of such attacks. Cloud solutions add a new threat to the landscape. If an attacker eavesdrops on your activities & transactions, manipulates data, returns falsified information & redirect your clients to illegitimate sites[5]. Your account & service instances may become a new base for the attacker. From here they may leverage use the power of your reputation to launch subsequent attacks. With stolen credentials attackers can often access critical areas of deployed cloud compromising services. Allowing them to compromise the confidentiality, integrity & availability of those services.

3.4: Insecure interfaces & APIs:

Cloud computing providers expose a set of S/W interfaces or APIs that customers use to manage & interact with cloud services. Provisioning, management & monitoring all performed using these interfaces. The security & availability of these general cloud services are dependent on these basic APIs.From authentication & access control to Encryption & Activity monitoring these interfaces must be

designed to protect against both accidental & malicious attempts to violate the policies. While most providers strive to ensure security is well integrated into their service models, it is critical for the consumers of those services to understand the security implications associated with usage, management & monitoring of cloud services. Reliance on a weak set of interfaces & APIs expose organization to a variety of security issues related to confidentiality, Integrity, availability &accountability.

3.5: Denial of services:

These attacks simply prevent the consumer from receiving the service from cloud. It is achieved by flooding excessive requests to the target server causing an intolerable system slowdown & leaves all the legitimate users not able to receive the service since the server is busy servicing the attacker.

There are many ways to perform DoS attack such as SYN flood. A SYN flood requests connections to the target server & ignoring the ACK from the server. This makes the server to wait for the ACK from the attacker wasting time &resources[6]. Because of which the server does not have enough resources to provide services to the clients. This attack can be prevented by authorizing strict access to the cloud & using cryptographic protocols to ensure that right personnel are accessing the cloud.

3.6: Malicious Insider

A malicious insider such as a system administrator in a improperly designed cloud scenario can have access to potentially sensitive information. From IaaS to PaaS&SaaS the malicious insider has increasing levels of access to more critical systems & eventually to data. Systems that are solely dependent on CSP for security are at great risk. Even if encryption is implemented the keys are not kept with the customer & are only available at data-usage time the system is still vulnerable to malicious insider attack.

Malicious insider working as a cloud employee collecting confidential data or taking complete control of the cloud service with minimal or no possibility of detection. [7]. Therefore it is an important challenge as to how an organization can restrict its internal employees, contractors, vendors & other people who have access to critical resources from within the N/W. Authorization plays an important role in securing the cloud.

Transparency is very important in the security & management. When cloud provider hires their employees certain factors such as hiring standards, policies regarding how their employees can access to virtual & physical assets & how the employees are being monitored in their work are to be clarified. If the cloud provider does not consider the significance of these factors, this situation may create more opportunities to the hackers.

3.7: Abuse of cloud services:

The greatest advantage of cloud service is that it allows even small organizations to access vast amount of computing power. It would be difficult for most of the organizations to purchase the high end infrastructure but at the same time renting them from a CSP is affordable. To CSP of IaaS & PaaS hackers may be able to conduct susceptible activities like the spamming & Phishing [8].

This threat is more of an issue for cloud service providers than cloud consumers but it does raise a number of issues for the providers.

How to detect people abusing your service— How to define abuse—How to prevent doing it again—

3.8: Insufficient Due Diligence:

Many organizations rushing into the promise of cost reductions, operational efficiencies & improved security. These can be realistic goals for organizations that have the resources to adopt cloud technologies properly. Without a complete understanding the CSP environment applications are services being pushed.

An organization that rushes to adopt cloud technologies subjects itself to a number of issues. Contractual issues arise over obligations on liability, response or transparency by creating mismatched expectations between the CSP & the customer. Pushing applications that are dependent on "internal" network level security controls to the cloud is dangerous when those controls disappear or do not match the expectations of the customer. Unknown operational & architectural issues may arise when designers & architects unfamiliar with cloud are designing applications being pushed to the cloud. The bottom line for enterprises & organizations moving to a cloud technology model is that they must have capable resources and perform extensive internal & CSP due-diligence to understand the risks it assumes by adopting the new technology model.

3.9: Shared Technology Vulnerabilities:

Cloud service providers deliver their services in a scalable way by sharing infrastructure, platforms & applications. The underlying components that make up this infrastructure were not designed to offer strong isolation properties for a multitenant architecture (IaaS), re-deployable platforms (PaaS), or Multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all the delivery models. A defensive in-depth strategy is recommended & should include compute, storage, network, application & user security enforcement, and monitoring.

A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in SaaS environment exposes more than just the compromised customer, rather it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it can affect an entire cloud at once [9].

4. CONCLUSION

Any application relying upon an emerging technology should consider the different possible threats. Such an application with an inability to anticipate or handle the threats may eventually lead to failure. The threats /issues presented in this paper would definitely benefit the customers & CSPs to handle them efficiently

REFERENCES

[1] Ramgovind S, Ellof MM & Smith E, " The management of Security in Cloud Computing", IEEE 2010

[2] Minqi Z, Rong Z, Wei X, Weining Q, "Security & Privacy in cloud computing: Asurvey", sixth international conference on semantics knowledge & Grid Nov 2010.

[3] AkhilBehl, " Emerging Security challenges in cloud computing, an insight to cloud security challenges & their mitigation", IEEE 2011

[4] PrashanthShrivastava, Satyam Singh, Ashwin Alfred Pinto, ShvetankVerma, Vijay K, Rahul Gupta, " An architecture based on proactive model for security in cloud computing", IEEE 2011.

[5] Yinqian Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart, "Cross-VM Side Channels and Their Use to ExtractPrivate Keys", IEEE 2012

[6] As Cloud Use Grows, So Will Rate of DDoS Attacks

http://www.infoworld.com/d/cloud-computing/cloud-use-grows-so-will-rate-of-ddos-attacks-211876

[7] Insider threats to cloud computing http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/

[8] Pirate Bay Ditches Servers and Switches to the Cloud

http://news.cnet.com/8301-1023_3-57534707-93/pirate-bay-ditches-servers-and-switches-to-the-cloud/

[9] Perfecting the unknown: Cloud Computing

http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php