SECURITY ISSUES IN CLOUD COMPUTING

T. Chandu harshitha[1] , G.Pranav Aditya[2] and G.Prabhu Teja[3]

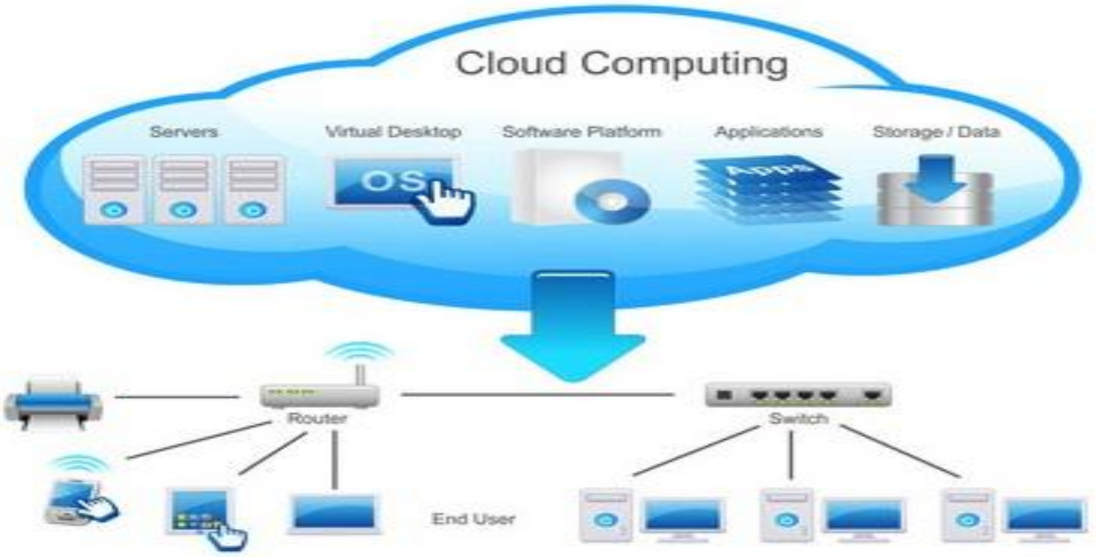
Student, B.tech, KL University

Abstract— The Cloud computing is an on demand service provided over internet. User can use the services provided by the service providers of the cloud environment. Customer can also store their data in the cloud rather than their internal system. In this context they don't have any ownership on their data i.e., they don't know the location where their data is stored in the cloud. Out of cloud's outstanding features like multi-tenancy, No installation costs, Accessing devices from anywhere over the internet, Rapid elasticity, etc., there are security issues which are making the business organizations to foot-step backwards in moving to cloud environment. The major security issues or threats in cloud are Account or Service traffic hijacking, Data breaches, Malware Injection, Insecure API's, Cloud Abuse, Denial Of service(DOS), Data loss etc., As the customers store their data in clouds they must ensure that cloud service providers(CSP) are securing their data and CSP must provide secure environment to store their data.

KEYWORDS: Cloud computing, virtual machine, Security, multi tenancy, Two-factor authentication, Cloud providers, Service providers, Customers, Hypervisor, Infrastructure-As-A-Service (IAAS), Platform-As-A-Service (PAAS), and Software-As-A-Service (SAAS).

I. INTRODUCTION

Cloud Computing: Cloud computing is essentially an extreme form of outsourcing the delivery of hosted service via the internet. The cloud acts as virtual server that users can access via the internet on an as needed basis. It includes any subscription based or pay-per use service that extends IT Capability allowing users to access stored information remotely. It is a promising technology that is transforming traditional computing ad IT industries. It encompasses activities such as use of networking sites and other forms of interpersonal computing. Cloud computing is the way to increase the capacity or add capabilities dynamically without investing in new infrastructure. It is a pay-per-use technology where customer or user of a service needs to pay for what they have used from the cloud provided by cloud providers



Deployment models:

There are 4 deployment models in cloud computing. They are: Private cloud, Public cloud, Hybrid cloud, Community cloud.

Private cloud:

It is used to describe offerings that emulate cloud computing on private networks. It is used with an organization's internal enterprise data centre. Scalable resources and virtual applications provided b cloud vendor are pooled together and made available for cloud users to share and use. It is similar to intranet functionality. Organization designated stake holders can have access.Private cloud (also called internal cloud) is a marketing term for an enterprise computing architecture that's protected by a firewall. In this type of cloud only the specified client can operate. However, under the private cloud model, the cloud is only accessible by a single organisation providing that organisation with greater control

II. SECURITY ISSUES

Despite the potential gains achieved from cloud computing, the enterprises are slow in accepting it due to security issues and challenges associated with it. Security is hampering the growth of cloud.

2.1. Issues in various delivery models:

Each of the delivery models is experiencing some form of threat. In IAAS, hardware, Storage and network should be secured so that confidentiality, integrity is maintained. Denial of Service attack can happen to the network. The attacker can overload the network so that authorized users cannot use the services effectively. Similarly, in SAAS, applications of various clients should be secured so that they must be accessed only by the authorized individuals. As these software's are accessed via web browsers, web browser security is important. Various methods available for securing SAAS applications are web services(WS) security, XML encryption, Secure Socket Layer(SSL), etc.,. In PAAS, Virtual machines as the act as a catalyst in PAAS must be protected from malicious attacks such as cloud malware. Therefore maintaining integrity in applications and well enforcing accurate authentication checks during transfer of data across entire networking channels is fundamental.

2.2. Issues in various deployment models:

In private cloud, keeping track of all the activities carried out in the cloud is necessary. It may be the employee of the organization having a particular private cloud is trying to make an attack on the cloud so that fame and trust on that particular organization can be lost. So the moment it is out of track, the moment security of that particular cloud might be lost.

In public cloud, there is a concept called multi-tenancy. Multi-tenancy is ability that multiple clients can share resources. Clients' doesn't know who is sharing their resources. So one flaw can make other tenant to access other clients' data easily. Security threat in public cloud is more compared to private cloud as it accessed by public.

III. CHALLENGES IN CLOUD COMPUTING

Major challenges in hindering cloud computing acceptance are:

1. Security
2. Costing model
3. Charging model
4. Service level agreement(SLA)
5. What to migrate
6. Cloud interoperability issue

In this paper, we were mainly concentrating on security issues. There are several issues in cloud computing. They are: Availability of service, Data security, Confidentiality, Auditability, Account or service traffic hijacking, Data breaches, Data loss, Insecure interfaces, Denial of service, Malicious insiders, cloud abuse, Insufficient due diligence, Shared technology vulnerabilities.

3.1. Confidentiality:

It is meant for secure data transfer and access. The information in the cloud should be accessed only by the authorized user. Cloud computing involves storing users data on remote servers owned or operated by others and accesses through the internet. The entire contents of user's storage device may be stored with a single cloud provider or with many cloud providers. The data compromise increases in the cloud, due to the increased number of devices and applications involved, which increase the number of points of access. In cloud computing, confidentiality plays a major role especially in maintaining control over organizations' data situated across multiple distributed databases.

Confidentiality can be achieved through proper encryption techniques like symmetric or asymmetric encryption algorithms. Key length and key management in case of the symmetric cipher must be taken into consideration. Actually, it is all based on the cloud provider. It also depends on the customers' awareness that they can encrypt their information prior to uploading it.

Multi-tenancy presents a number of privacy and confidentiality threats. Infrastructure reusability is an important characteristic of cloud environments, but reusable infrastructures must be carefully controlled otherwise they will create a serious vulnerability.

3.2. Availability:

Availability is one the most critical security requirements in cloud computing. Availability is a property of a system being accessible upon demand by an authorized entity. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Denial of service attack and natural disasters are some of the threats to availability. The goal of availability for cloud systems is to ensure that users can use them at any time, at any place. The system must have the ability to continue operations even in the possibility of a security breach.

3.3. Auditability:

It is meant for tampering of applications security. It tells whether security is tampered or not. It can be achieved by using some remote attestation techniques. These techniques are used to validate current location of data, to establish a trust relationship in a cloud. It should be added as an extra level away from the virtualized OS in one logical layer maintain some responsible related to confidentiality and audit ability.

3.4. Denial of service:

A DoS attack makes our network or machine unavailable to the intended users by flooding them with connection request. An attacker will take network into his control and try to induce something so that network will not be available for the customers to utilize the services from the cloud.

3.5. Cloud Abuse:

A bad guy using a cloud service to break encryption key which is too difficult to crack on standard computer. Eg: Malicious hacker using cloud servers to launch DDoS attack, share pirated software.

IV. ADVANTAGES

- Many of the issues can be solved by using the existing techniques.
- Confidentiality can be maintained by using cloud cryptographic protocols.
- Authentication can be achieved by using passwords to some extent.
- Auditability can be maintained by proper monitoring of VMs.
- Many organizations can have some trust to move on to the cloud by solving all these concerns.
- Denial of service attack can be reduced by limiting the resources to a VM so that service utilization can be done effectively.

V. DISADVANTAGES

- Away from these issues, there are lot more security threats that need to be addressed.
- Authentication by using passwords can only protect data to some extent.
- By using simple encryption techniques we cannot maintain integrity.
- Some digital signatures are needed to address integrity.
- Most of the organizations' are not willing to move to the cloud due to some issues that are still need to be addressed.
- By having these solutions, fraudulent charges imposed by the attacker on the customer cannot be avoided.

MULTI-FACTOR AUTHENTICATION:

It is a technique that provides high level of authentication by combining any two of the three provided below:

1. Something the user knows (e.g., password, PIN)
2. Something the user has (e.g., ATM card)
3. Something the user is (e.g., biometric characteristic, such as a fingerprint)

One time passwords can be used. Physical tokens and software tokens which generates one time password. Key along with password which user has.

Biometrics like finger print retina scan can be used to provide security to the cloud. Highly confidential data uses this.

Defence in depth- It is another mechanism in security which uses multiple security measures to reduce the risk of security threats. If one component of the protection gets compromised then we may have other layers to eliminate or avoid the attack. We may have antivirus in our desktops which may not capture attacks through network.

In addition to Multi-tenancy there are some more security concerns. They are Velocity of attack, Information assurance, Data privacy, Ownership.

Velocity of attack (VOA) - Thousands of servers are in same location. cloud infrastructure in use surface for attack is huge. VOA is huge. potential loss due to attack is high and difficult to mitigate the spread of attack.

To counter the challenge of VOA, CSP's need to adopt more robust security enforcement mechanisms eg-defence in depth.

Information assurance and data ownership - Ensure confidentiality of data so that these can be maintained. Cloud is hosted by CSP who have access to data. Organization is owner. Data should be protected using encryption and access control mechanisms.

Data privacy – It is an unauthorized disclosure of private data of client. CSP need to deploy data privacy mechanisms which are compliant with regional legal regulations.

VI. VARIOUS THREATS

1. VM theft - Vulnerability that enables attacker to copy a VM in an unauthorised manner.

Attacker will use it for attacking. VM is a file located on Virtual environment. It is a result of inadequate control on VM files allowing unauthorized copies or move operations. Copy and move restrictions are essential to safeguard against VM theft.

These may bind VM to specific physical machine. With this a VM cannot run on other hypervisor installed on other server. These restrictions use virtualization management and storage management services for effective environment. Limit applying such restrictions to critical or sensitive VM's only.

2. Hyperjacking:

It enables an attacker to install a rogue hypervisor or virtual machine monitor that can take control of underlying server resources. Attacker can run unauthorised applications on guest OS without OS realizing it. Attacker could control interaction between VM's and underlying server. Hypervisor is component which virtualizes sever. It takes control of entire infrastructure. Regular security measures are ineffective in case of hyperjacking.

Measure against this can be h/w assisted secure launching of hypervisor. Scanning hardware level details to assess integrity of hypervisor and locating the presence of rogue hypervisor

3. Data leakage:

Side channel attack can be used for data leakage. It extracts information by monitoring indirect activities for ex: cache data.

Cross VM SCA could reveal information of client to another client that runs its VM in same server. Protection against cross VM SCA requires not placing those clients that have conflicts with another on the same server.

This type of vulnerability is particularly scary because hackers are able to use your reputation and the trust you have built up to manipulate your clients. In 2010, Amazon faced an attack that allowed hackers to steal the session IDs that grant users access to their accounts after entering their passwords. This left the client's credentials exposed to the hackers. The bug was removed 12 hours after it was discovered, but many Amazon users unknowingly fell for the attack during that time.

There are some proactive steps companies can take to protect themselves. For example, companies can do this by:

1. Setting up protocol that prohibits sharing account credentials between employees or services.
2. Using a strong two-factor authentication technique and track employee use of the platform for unauthorized activity.
3. Utilizing a secure encryption management system, such as that offered by Venafi, should also be prioritized and developed specifically for use with a cloud

The hacker deceived AT&T'S system into redirecting the victim's cell phone to a fraudulent voicemail box. The hacker visited Gmail and initiated the account recovery feature for the victim's personal email address. The hacker logged into the victim's Gmail account and added his email address to the 'account recovery control' feature. The victim's linked Cloud fare account received an email informing him that the recent password was changed. The victim initiated the account recovery process and changed the password back. An email is sent to the hacker informing him that the victim changed passwords, but immediately the hacker changed the password. the victim from resetting the Gmail password.Account or service traffic hijacking can be avoided by using two factor authentication technique.

Demilitarized Zone:

It is a physical network that limits exposure of nodes in the internal network from external n/w's.

It adds additional layer of security against external attacks. An attacker has access only to DMZ rather than any other part of n/w. Services provided to the users can be placed in DMZ.

A Virtualized DMZ is a DMZ established in Virtualized environment using virtual n/w compose

VII. CONCLUSION AND FUTURE WORK

So by using cloud cryptographic protocols confidentiality and integrity can be attained with the addition of digital signatures. Two factor authentication technique is used in order to reduce account or service traffic hijacking.

VIII. REFERENCES

[1] He, Sijin; L. Guo, Y. Guo, M. Ghanem,. "Improving Resource Utilisation in the Cloud Environment Using Multivariate Probabilistic Models". 2012 2012 IEEE 5th International Conference on Cloud Computing (CLOUD). pp. 574–581. doi:10.1109/CLOUD.2012.66. ISBN 978-1-4673-2892-0. Cite uses deprecated parameters (help)

[2] Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

[3] King, Rachael (2008-08-04). "Cloud Computing: Small Companies Take Flight". Bloomberg BusinessWeek. Retrieved 2010-08-22.

[4] Hamdaqa, Mohammad. A Reference Model for Developing Cloud Applications

[5] http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud