****

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY 2015

IT 501 - Information and Network Security

Assignment 01 – Year 1 Semester 2

Lecturer: Mr.Lakmal Rupasighe

**Security issues in cloud environments**

S.S.Niranga - MS14901836

# Acknowledgement

I would like to express my special thanks of gratitude to Dr. Samantha Thelijjagoda for providing me with the opportunity to study at SLIIT as well as my Mr.Lakmal Rupasinghe who gave me this golden opportunity to do this assignment on the topic " Security issues in cloud environments and End Note", which also helped me in doing a lot of research and I came to know about so many new things and I am really thankful to them. Secondly, I would also like to thank wife and friends who helped me a lot in finishing this project within the limited time.

I am making this assignment not only for marks, but to also increase my knowledge.

Thanks again to all who helped me.

Table of Contents

[Acknowledgement 2](#_Toc421305804)

[Introduction to cloud computing 4](#_Toc421305805)

[Security issues in cloud environments 4](#_Toc421305806)

[Data Leakage and Consequent Problems 4](#_Toc421305807)

[Malicious Attacks: 5](#_Toc421305808)

[Backup and Storage: 5](#_Toc421305809)

[Shared Technological Issues: 5](#_Toc421305810)

[Service or Account Hijacking: 5](#_Toc421305811)

[Malicious VM Creation: 6](#_Toc421305812)

[VM Hopping: 6](#_Toc421305813)

[VM Mobility: 7](#_Toc421305814)

[VM Denial of Service: 7](#_Toc421305815)

[XML Signature Element Wrapping: 7](#_Toc421305816)

# **Introduction to cloud computing**

History has a funny way of repeating itself, or so they say. But it may come as some surprise to find this old cliché applies just as much to the history of computers as to wars, revolutions, and kings and queens. For the last three decades, one trend in computing has been loud and clear: big, centralized, mainframe systems have been "out"; personalized, power-to-the-people, do-it-yourself PCs have been "in." Before personal computers took off in the early 1980s, if a company needed sales or payroll figures calculating in a hurry, you'd most likely have bought in "data-processing" services from another company, with its own expensive computer systems, that specialized in number crunching; these days, you can do the job just as easily on your desktop with off-the-shelf software. Or can you? In a striking throwback to the 1970s, many companies are finding, once again, that buying in computer services makes more business sense than do-it-yourself. This new trend is called cloud computing and, not surprisingly, it's linked to the Internet's inexorable rise.

Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user—it's just somewhere up in the nebulous "cloud" that the Internet represents.

# Security **issues** in cloud environments

## Data Leakage and Consequent Problems

Data insertion or deletion without the backup leads to certain drastic data related problems like security, integrity, locality, segregation and breaches. This would lead to sensitive data being accessed by the unauthorized users. One solution to this data leakage problem is side-duplication with allowing limitation on number of user uploads per time window. The term de-duplication means storing only single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data. Second solution is Fragmentation-redundancy-scattering

## Malicious Attacks:

The threat of malicious attackers is augmented for customers of the cloud services by these of various IT services which lacks the lucidity between the procedure and process relating to the service providers. Malicious users may gain access to certain confidential data and thus leading to data breaches. An access control mechanism tool can be thought of to control unauthorized user in accessing secured data. Infrastructure as a Service as one of the service that exposes challenges with using virtualization as a frontier security protection to defend against malicious cloud users.

## Backup and Storage:

The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As per the study more the server virtualization increases, a very difficult problem with backup and storage is created. De-duplication in cloud storage is carried out with the misuse of data backup. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes.

## Shared Technological Issues:

IaaS vendors transport their services in a scalable way by contributing infrastructure. But this structure does not offer strong isolation properties for a multi-tenant architecture. Hence in order to address this gap, virtualization hypervisor intercede the access between guest operating system and the physical compute resources. Spite of several advantages, these hypervisors have exhibited flaws that have permitted guest operating systems to expand inappropriate levels of control or authority on the underlying platform. This certainly led to security issues on the cloud.

## Service or Account Hijacking:

Service hijacking is considered as one of the top most threat. Service hijacking associated with gaining an illegal control on certain authorized services by various unauthorized users. It accounts for various techniques like phishing, exploitation of software and frauds. Account hijacking has been pointed as the severe threats. The chances of hijacking ones account increases considerably as no native API’s (Application Program Interface) are used for registering various cloud services. The Countermeasure provided on Hijacking by a non-profit. Organization Cloud Security Alliance (CSA) that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance which provides a list of recommended best practiced to assure identities and secure access management.

## Malicious VM Creation:

An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository. The one solution for malicious virtual machine creation is MIRAGE the author proposes a virtual machine image management system in a cloud computing environments. This approach includes the following security features: access control framework, image filtering, a provenance tracking, and repository maintenance services. However, one limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer’s confidential data.

## VM Hopping:

This concluded that with VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM’s resource procedure, alter its configurations and can even delete stored data, thus, putting it in danger the VM’s confidentiality, integrity, and availability. A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM’s IP address. Although PaaS and IaaS users have partial authority, it shown that an attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs to fetch user’s IP. Thus it can be inferred that VM hopping is a rational threat in cloud computing. Additionally, multi- tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a critical vulnerability for IaaS and PaaS infrastructures.

## VM Mobility:

The content of VM virtual disks are saved as files such that VMs can be copied from one host to another host over the system or via moveable storage devices with no physically pilfering hard drive. VM mobility might offer quick use but could show the way to security problems likewise, the rapid spread of susceptible configurations that an attacker could make use of to endanger the security of a novel host. Several types of attacks might take advantage of weaknesses in VM mobility which includes man in-the- middle attacks. The severity of the attacks ranges from leaking perceptive information, to completely compromising the guest OS. A PaaS provider offers a variety of pre- configured computing platform and solution stacks to the service users. The users take advantage of the libraries and APIs (Application Program Interface) to build up their individual applications on permanent computing platform by importing their VM images.

## VM Denial of Service:

Virtualization lets numerous VMs split physical resources like CPU, network bandwidth and memory or disk. A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. In cloud computing, DoS attacks could still happen, but having service providers place sufficient configurations to put a ceiling on the resources owed to the VMs decreases their probability. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

## XML Signature Element Wrapping:

It is found to be a very renowned web service attack. It protects identity value and host name from illegal party but cannot protect the position in the documents. The attacker simply targets the host computer by sending the SOAP messages and putting scrambled data which the user of the host computers cannot understand. As per the studies by researchers at Ruhr University, and mentioned, the XML Signature wrapping attack changes simply the content of the signed part of a message without tampering the signature. This would not let the user to understand the twisted data, thus misguiding and misleading the user.The best countermeasure approach would be to enhance the interface between the signature verification function and the business logic. In this approach, the signature verification returns some sort position description of the signed data, next to a Boolean value. The business logic may then decide if data about to be processed has been signed or not.