Paper Title:

Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures

Paper Link:

https://ieeexplore.ieee.org/document/6488089

1 - Summary

1.1 Motivation

The paper describes techniques of virtualizing a CCI, types of attacks on VCCI, vulnerabilities of VMMs and the significance of security tools and techniques for securing a VCCI.

1.2 Contribution

The Virtual Machine Monitor (VMM) or hypervisor, a key element of the Virtualized Cloud Computing Infrastructure (VCCI), oversees and controls the Virtual Machines (VMs) through kernel-based software.

1.3 Methodology

This paper illustrates some security tools for safeguarding the Virtual Machine Monitor (VMM), including Encryption and Key Management, Access Control Mechanisms , Intrusion Detection Tools (IDTs), Virtual Trusted Platform Module, Virtual Firewalls, and Trusted Virtual Domains (TVDs).

1.4 Conclusion

The paper highlights that multi-tenancy in cloud computing, involving sharing resources among clients, offers benefits but is prone to attacks, especially on the Virtual Machine Monitor (VMM).

2 - Limitations

2.1 First Limitation

As the study was done, it is yet to be given sustained effort for establishing and upholding security in cloud environments, with a specific emphasis on identifying and addressing security issues from both governance and operational standpoints in cloud computing.

3 - Synthesis

The findings can be applied in cloud shared resources among clients, facing security challenges, securing the virtualized environment, enhancing protection.