

Degree Thesis

Master's Programme in Network Forensics, 60 Credits



VIRTUALISATION SECURITY ISSUES

Security Issues Arises In Virtual Environment

School of ITE, 15 credits

Kirandeep Kaur



Virtualization Security Issues

DEDICATION

I dedicate my work to my family. A special feeling of gratitude to my loving mother, Gurmeet Kaur, and my husband Navraj Singh Dhaliwal. I also dedicate this work to my In-Laws family and my sister and my few friends who supported me throughout the process.

ACKNOWLEDGMENTS

I would like to thank and pay my special regards to my supervisor and examiner Mark Dougherty, and our program director and professors Olga Torstensson; Stefan Axelsson; and Muhammad Ahsan Rasool for the unconditional support and guidance at every step during studies.

I wish to express my deepest gratitude to Slawomir Nowaczyk; Reza Khoshkangini; Abbas Orand; Sepideh Pashami; Mahmoud Rahat; Linus Andersson; Matts Skagshøj and all others who provided us great knowledge as well as my class fellows and my group mates.

To Halmstad University, thank you for an unforgettable experience.

TABLE OF CONTENTS

1. ABSTRACT.....	8
2. INTRODUCTION.....	9
3. BACKGROUND.....	9
3.1 THE VIRTUALIZATION ARCHITECTURE.....	10
3.2 THE HYPERVISOR: VIRTUAL MACHINE MONITOR (VMM)	11
3.3 HYPERVISOR TYPES	11
3.4 VIRTUALIZATION/CLOUD COMPUTING	12
3.5 THE INFOSEC AND CIA PRINCIPLES:	13
4. PROBLEM DESCRIPTION AND RESEARCH QUESTIONS.....	14
4.1 RESEARCH QUESTIONS:.....	14
4.2 RESEARCH OVERVIEW:	15
4.3 RESEARCH METHODOLOGY:	17
4.3.1 THE SYSTEMATIC LITERATURE REVIEW:	17
4.3.2 VIRTUALIZATION SECURITY ISSUES REVIEW PROTOCOL:	18
4.3.3 SEARCH AND DATA EXTRACTION STRATEGY:	18
5. RESEARCH FINDING	20
5.1 RECOGNIZED SECURITY ISSUES	20
5.2 HIGHLIGHTS ON SECURITY ISSUES	21
5.3 EFFECTS OF VIRTUALIZATION SECURITY ISSUES ON INFORMATION SECURITY:.....	28
6. MITIGATION OF VIRTUALIZATION SECURITY ISSUES:	29
6.1 PROPOSED MITIGATION 1:	29
6.1.1 THE FIRST FRAMEWORK:	30
6.1.2 SECOND FRAMEWORK:	33
6.1.3 REMARKS ON THE COMPARISON OF THE TWO FRAMEWORKS: ...	35
6.2 PROPOSED MITIGATION 2:.....	36
6.3 PROPOSED MITIGATION 3:	38
7. CONCLUSION.....	42
7.1 GENERAL REMARKS.....	42
7.2 SUMMARY	43

7.3 FUTURE CONSIDERATIONS:	46
8. REFERENCES:	47

LIST OF ABBREVIATIONS

- ACA – Access control agent
- ACE – Access control entry
- API - The application program interface
- CIA - Confidentiality, integrity, availability
- CTB - Cloud traceback
- DoS - Denial-of-service attack
- DMZ - Demilitarized zone
- IaaS - Infrastructure as a service
- IDS - Intrusion detection system
- IO - Input/output
- IPS - Intrusion prevention system
- LDAP - Lightweight Directory Access Protocol
- MAC - Media access control
- MCS - Multi-Category Security
- NGFW - Next-generation firewalls
- NIST - The national institute of technology
- MLS - Multi-level security (MLS)
- NSA - National Security Agency
- PaaS - Platform as a service
- PM - Policy management
- PMD - Policy management database
- PVI - Private virtual Infrastructure
- RBAC - Role-based access control
- SaaS - Software as a service
- SC - Security contract
- SCD – Security contract database
- SIG - Virtualization Special Interest Group
- SLA - Service level of agreement
- SSO - Single sign-on
- SOAP - Simple object access protocol
- TE - Type enforcement
- VIDS - Virtual intrusion detection system

- VIPS - Virtual intrusion prevention system
- VLAN - A virtual LAN
- VM - Virtual machine
- VME - Virtual Machine Environment
- VMI - VM image management
- VMM - Virtual Machine Manager
- VPN - Virtual private network
- VREM - Virtual Machine Reliability Monitor
- VSEM – Virtual machine security monitor

1. ABSTRACT

This Thesis is submitted in Partial Fulfilment of the Requirements of a Master's degree in Network Forensics at Halmstad University, Sweden. The author had selected Virtualization Security as a valid issue for cloud computing service. In choosing this topic had the intention to apply the acquired knowledge during the Master's course, in search of practical solutions for computer security issues. This study report is classified into six segments and a conclusion. These are the introduction, background, research methodology, literature review, summary, discussions, conclusion, and future considerations. Information Technology (IT) sector had encountered numerous and ever-emerging security issues, including those in virtual environments, which have become a big concern for organizations. Virtualization is the use of software to accommodate multiple operating systems on a computer system simultaneously, which can be applied from anywhere, given that there is internet connectivity. So the user can have access and can resolve the security issues. However, some constraints are limiting the benefits of the Virtualization of servers. The objective of this project is to study Virtualization as a valid means of solving IT security issues. Also, to assess mitigation approaches that can enhance Virtualization in the computing environment. To accomplish such objectives, this study had undergone a systematic literature review in order to learn the variety and nature of security issues of the virtual environment. Accordingly, the study had undertaken the classification of security issues to determine effective mitigation methods. The study had realized that there are around twenty-two known security issues, which are classified and described in section six of the report. On Virtualization, as the subject study: three mitigation schemes are reviewed and discussed to alleviate important virtualization security issues (chapter seven of this Thesis). Moreover, the effects of the proposed mitigation techniques on the virtualization security issues on the CIA model (**Availability, Integrity, and Confidentiality**) are explained in brief. The model allows the researcher to quickly find the appropriate mitigation technique to manage the security issues of any virtual environment. In conclusion, the study provided a metadata reading of the security issues in the virtual environment. And apply the selected methods to solve the security issues, which proves that the virtualization technology is the critical element of the utilizing computing power to its maximum capacity by executing process simultaneously without downtime, however IT security issues are continuously evolving, and the research mission is always to conceive new techniques.

2. INTRODUCTION

This research scheme is about virtual environment security issues and how to mitigate these issues. Compare to the computer, a **virtual machine (VM)** is a mimicry of a computer system.

Virtualization can be defined as the use of a software layer that environs or/and underlies the operating systems which will be deployed on the same server (hardware settings) while providing the same inputs, outputs, and behavior that would be demanded from physical hardware. The software which plays this role is called **Hypervisor** or **Virtual Machine Monitor (VMM)**. The function of the Hypervisor is to provide an environment to the hosted operating system which looks and performs similar to the host system, but it detaches the hardware state ^[1].

The virtualization system, which contains virtual environments, is also called virtual machines (VM), where operating systems can be installed in them. VMs are not by the state of the physical hardware; hence a multiple VMs can be installed in a single server/computer. Due to the enormous development in the technology concept in the last two decades, Many may think that the virtualization concept is a recent invention. But in reality, is the virtualization concept dates back to the late 1960s and the early 1970s. The foundational the research was undertaken in the early 1970s [Goldberg 1973, 1974] ^[2]. During the last ten years, the rapid growth of the demand for virtualization solutions had been realized.

The benefit of Virtualization in IT technology is vast; it increases IT agility, flexibility, and scalability, whereas creating significant cost saving. Virtualization allows the mobility of the workload, enhance the performance and availability of the resources, the automated operations.

The Major conceptualized Benefits of Virtualization are to make IT simpler to control and operate, as well as to reduce the cost of operation and ownership of the equipment. Ease of management, less downtime, quicker disaster recovery, centralization of control.

3. BACKGROUND

Research at this level tries to highlight some basic technical concepts pertaining to Virtualization versus physical (hardware) computing practices to proceed further into the subject matter of virtualization security issues and how they can be mitigated.

In principle, the Majority of Computer systems require more threads than what the processor can support directly. The Core in a consumer machine can have at least a single thread of CPU execution. The operating system facilitates a high level of interface for software by allowing process multiplexing; also can handle the hardware management issues.

3.1. THE VIRTUALIZATION ARCHITECTURE

Virtualization, on the other hand, allows working remote, or wireless, or with requirement than the physical setups of the computing systems.

Virtualization architecture is a theoretical model withstand all the interrelationships of defined components involved in delivering virtual machines with the same functionality as the physical ones ^[4], such as an operating system (OS), a server, a storage device or network resources.

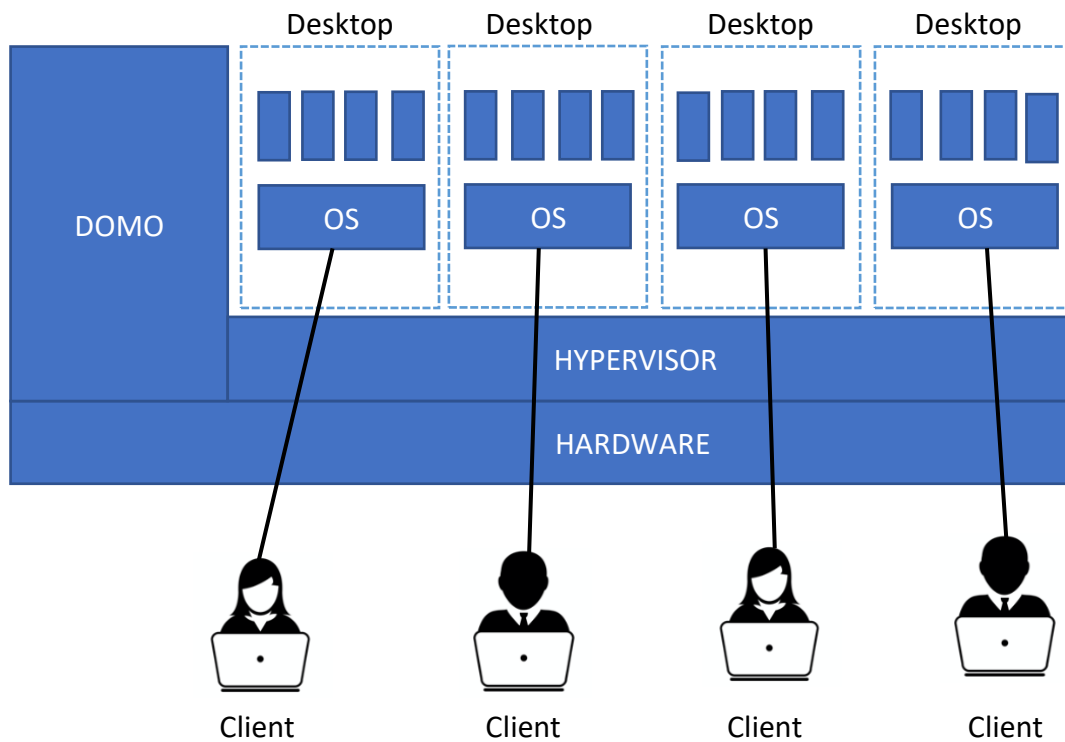


Figure 2.1. Virtualization architecture

In virtualization architecture, the operating systems offer a degree of reflection over the hardware, allowing the possibility of simultaneously running multiple processes. Such configuration enables a single operating system to work on a single hardware setup. The operating system deployed on the hardware setup holds higher privileges; it can perform any operation that the hardware can support.

However, an application running within the operating system will have less privilege, which it cannot execute operations except those, which the operating system permits. These privilege levels are often called rings, the lower the number of rings (ring0), the higher and the privilege. The Kernels of the operating system usually have the lowest ring, which gives it the highest privilege, and thus it controls the other lower privileges.

3.2. THE HYPERVISOR: VIRTUAL MACHINE MONITOR (VMM)

The Hypervisor or Virtual machine monitor (VMM) is the computer software that can initiate and run a VM. A host machine is a computer/server/ physical machine in which the Hypervisor is installed on it. Guest machines are virtual machines.

A hypervisor is an extremely privileged software that runs either alone or can underlay the operating system; it is implemented to be "an efficient, isolated duplicate of the real [physical] machine" [Popek and Goldberg 1974]. Furthermore, a single hypervisor can run multiple networked systems.

The virtual machine monitor defers from an emulator. An emulator interrupts the instructions; an emulator intercepts all the commands, a virtual machine monitor is distinct from an emulator. An emulator intercepts all instructions; on the other hand, a virtual machine monitor intercepts sensitive instructions (which interface with the VMM operations). The non- sensitive instructions are executed directly on the hardware setup.

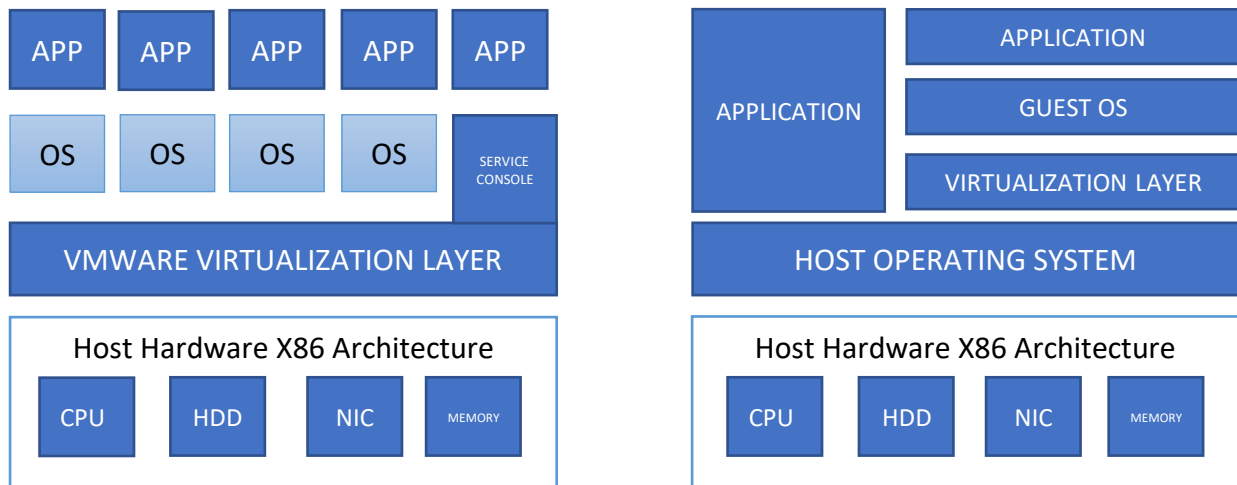
3.3. HYPERVISOR TYPES

A hypervisor in a simple it can be a type of virtualization software that supports the creation and management of virtual machines by an underling and separating the guest operating systems from its hardware. It interprets requests between physical and virtual resources. The Hypervisor can be categorized into two types: Type 1: Native or bare Metal and Type 2 is Hosted hypervisors

TYPE 1:- NATIVE OR BARE METAL HYPERVISOR

A software Installed directly on the hardware setup of the physical machine; it is positioned between the hardware and the guest operation system (virtual machines), figure 2 illustrates the native Hypervisor and hosted Hypervisor. A certain bare-metal hypervisor is embedded into the firmware with the same level as the motherboard basic input/output system (BIOS),

which is usually used in automotive, industrial (RTOS of the real-time control), and medical field it is used in patient monitoring and treatment control.



TYPE 1: NATIVE OR BARE METAL HYPERVERSOR

TYPE 2: HOSTED HYPERVERSOR

Figure 2.2. Type 1 (Native bare-metal Hypervisor) And Type 2 (Hosted Hypervisor)

TYPE 2:- HOSTED HYPERVERSOR

In this type (Hosted Hypervisor) the Hypervisor is installed or hosted as a program on an existing operating system, after the installation, the Hypervisor uses the some of the resources that appear to the operating system. Any problem that occurs to the host operating system will affect the functionality of the Hypervisor, hence may affect the guest virtual machines in it. Occasionally the Hypervisor above the host operating system might be secure, but the guest virtual machine will be available for the copy as OVF, OVA VMDK, examples for hosted Hypervisor such are Oracle VM Virtual Box, VM Ware Server (discontinued), and Workstation, Microsoft Virtual PC, KVM, QEMU, and Parallels.

3.4. VIRTUALIZATION/CLOUD COMPUTING

The concept of virtual computing and cloud computing has no difference in the sense of the functions and components. The national institute of technology (NIST), US Department of Commerce has an official description of cloud/virtual computing³: which says that:

"Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."^[5]

The Virtualization of servers provides three essential services

1. Software as a Service (SaaS): the users run applications on the virtual environment, the application can be accessed through different hardware form the side.
2. Platform as a Service (PaaS): PaaS delivers to users with multiple programming languages, libraries, services, and tools supported by the provider.
3. Infrastructure as a Service (IaaS): IaaS provides on-demand virtual computing services and provides access to computing resources in a virtualized environment.

3.5. The InfoSec and CIA PRINCIPLES

Information security (InfoSec) is set methods and procedures with the main focus of data protection and mitigation of security risk.

InfoSec includes stop or decrease the probability of the unauthorized access to data, or the illegitimate use, modification, reviewing deletion, or corruption of the data.

InfoSec also involves actions intended to reduce the opposing effect of such events.

The focus of information security is balancing the protection of the CIA troika model: confidentiality, integrity, and availability of the data/information, while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

The CIA MODEL consists of three factors for confidentiality, integrity, and availability. The prime attention of information security is providing confidentiality, integrity, availability, accountability, and assurance. Accountability and assurance are beyond the framework of this Thesis.

- **CONFIDENTIALITY:** Confidentiality to achieve information confidentiality, we need to ensure information is accessible by the dedicated user. A key factor in providing information

confidentiality is encryption. On the same hand enforcing file permission and access control lists to limit illegal access to information is also a key component in it.

- **INTEGRITY:** Preventing unauthorized manipulation/modification and ensures the accuracy as well as reliability of the data through its life cycle. Data encryption practices and hashing algorithms are key approaches to providing integrity.
- **AVAILABILITY:** Ensures the continuity and ease of reach of the data whenever it is needed for the authorized user in the system. The factors that can affect data/service availability are numerous. Any attack that can cause the denial of access data/service to the users it affects the availability factor.

4. PROBLEM DESCRIPTION AND RESEARCH QUESTIONS:

Virtualization technology has made security a complex issue, where lots of new vulnerabilities and threats are appearing. The distinctive advantage of Virtualization is that: it allows multiple operating systems to co-reside on the same physical machine without interfering with each other and benefits from dynamic resource allocation on the same hardware.

The Hypervisor (VMM) is the center of the virtualization environment, which is used to implement the best security practice that may reduce security issues.

In Fact, there are many issues related to the hypervisor virtual machine monitor (VMM) and the guest virtual machine, which made the vulnerabilities in the Virtual environment. However, they are not new security concerns; moreover, there are no security techniques available to mitigate these issues.

The hypervisor layer plays a significant role in the operation of virtual machines. Since it controls the virtual environment, the malicious party has a chance to attack the virtualization layer, exploit security holes, and gain access to all virtual machines. Hyper jacking of the Hypervisor how it will leave a trace of the attack; the logs should show the activity of the attacker accessing the Hypervisor.

4.1. RESEARCH QUESTIONS

This research assignment is guided by some basic three questions to explore the subject matter, and to reach the intended conclusion, the research questions are:

(a) What are the security issues of Virtualization in the environments?

(b) How to mitigate security issues in the virtual environment?

(c) What is related work being done?

4.2. RESEARCH OVERVIEW

Information Security issues are massive, and various issues for any kind of networked, computerized, and storage-based Infrastructure. The virtualized environment withholds three characteristics of the information technology environment; these are: (network, computer system, and storage facilities).

Guided by the above research questions this research study had undergone profound review in the field of security issues of Virtualization, with the aim to reach satisfactory answers to the research questions.

Researchers had kept studying the security issues in the virtualization layer. A virtualized environment offers the isolation in which each of the virtual machines (VMs) is completely detached from the other and the rest of the system, and that is the role of the Hypervisor.

Breaking the confinement of the VMs, to the point of confidentiality, integrity, or availability of the VMs is compromised and considered a great achievement ^[3].

Most of the virtualization vulnerabilities are distinct and ever-increasing in the virtual environment and can hardly be mitigated by the existing solution alone.

The volume of the virtualization studies is increasing due to the expansion of the market demand; accordingly, the vulnerabilities revealed by security analysts and hackers are snowballing.

According to the realities of information security issues expansion, the Hypervisor is attracting the main concerns, because it has the supervisory duties (creation, management, isolation of the VMs).

The interconnectivity complexities and the multiple entry points in the Hypervisor will always increase the offensive activity and encourage large amounts of attack vectors^[10].

Zhang et al. ^[11] introduced a technique to Rootkit detection based on KVM hypervisor. For the last five years, Wojtkowiak ^[12] introduced 259 new virtualization vulnerabilities, as well as new types of attack (e.g., Hyperjacking, hypervisor escape, VM attacks).

Pearce et al. ^[4] showed in their work on the hypervisor vulnerability, as well as breaking the security to the Xen and KVM hypervisors.

Gupta and Kumar ^[13] had undertaken a review and elaborated on the prospect of secure system isolation and introduced issues that occur from strong Virtualization and also the issues in weak implementation of core virtualization, but the test procedures to weak implementing of core virtualization were not exactly implemented.

Perez-Botero et al. ^[14] introduced through analyzing the code to Xen and KVM hypervisor vulnerability associated with them. Perez-Botero et al. ^[14] suggested a characterization of Hypervisor Vulnerabilities, which is composed of three aspects: **The Trigger Source, The Attack Vector, And the Attack Target.**

Moyo and Bhogal ^[15] had conducted research and gave the investigation of the security issues in cloud computing also mentioned that virtual machines might use side-channeling to extract private cryptographic keys which are used by other neighboring VMs.

Kazim and Zhu ^[16] defined security issues in the cloud virtualization hypervisor, virtual, machine, and guest disk images.

Wang et al. ^[17] studied the shared memory based cross-VM side-channel attacks in the IaaS cloud.

Hussain et al. ^[18] had researched on the multilevel classification model of different security attacks across different cloud services at each layer, also the attack type classification and risk levels associated with each cloud services layer.

Zhang and lee ^[19] examined inside VM and outside-VM vulnerabilities. They explained that the VM could get infected by a malware/ OS rootkit at runtime, which will compromise the security state of the VM and can take complete control of the VM. They had stated that the threats to the host OS and co-resident VMs are hard for the user to defend against it.

Wu et al. [20] projected an access control model that can stop virtual machine escape (PVME) by adapting the BLP (Bell-La Padula) model (an access control model developed by Bell and La Padula).

Geeta et al. [21] reviewed a comprehensive survey on the state-of-art techniques in data auditing and security and presented the challenging problems in information repository auditing and security.

Dubey et al. [22] attempted to do a SWOT analysis of a cloud computing environment. They had undertaken a critical and detailed analysis by mapping its Strengths (S), Weakness (W), Opportunity (O), and Threat (T) in different ways.

Zhang and Lee [23] anticipated a flexible architecture, Cloud computing, to observe and attest to the security health of customers' VMs within a cloud system.

Ravi Kumar et al. [24] searched on different data security issues in cloud computing in a multitenant environment and proposed methods to overcome the security issues.

4.3. RESEARCH METHODOLOGY

The research methodology followed to achieve the objectives of this study includes, the systematic literature review explained below, virtualization security issues review protocol: search and data extraction strategy: identification of the specific security issues, the conceptualization of the virtualization security issues mitigation and systems descriptions.

4.3.1. THE SYSTEMATIC LITERATURE REVIEW

In this research work, the researcher had followed a systematic literature review in order to explore Virtualization security issues. A systematic literature review is here perceived that it allows the researcher to identify, evaluate, and interpret published researches to a specific research topic or question. The systematic literature review is anticipated to provide a rich and focused overview as well as summaries of current studies. The key advantages of the systematic literature review over the traditional literature review are that:

A systematic literature review tackles a defined research question by defining the evaluation procedure. It also defines search tactics whose objectives are to find the most related

literature. But distinctively, the Systematic literature review relies on inclusion and exclusion standards to evaluate potential primary studies.

- a) A systematic review is implemented mainly in three phases, which are: Planning: identifying the number of researches needed to review.
- b) Conducting the reviews relevant to the main studies, data extraction, and data synthesis.
- c) Reporting: summarizing the review and report the results to document the findings.



Figure 3.1. Phases of Systematic Literature Review

In addition, in the part of this study, a literature review is performed in order to identify methods and mitigation techniques for reducing the security issues of Virtualization Technology that is found in the following part

4.3.2. VIRTUALIZATION SECURITY ISSUES REVIEW PROTOCOL

The review protocol dictates the procedure which will be used to commence the systematic review, this is to meet the objectives by finding answers to the review questions, as indicated in the core research questions, and these are:

- i. What are the security issues of Virtualization in the environments?
- ii. How to mitigate security issues in the virtual environment?

4.3.3 SEARCH AND DATA EXTRACTION STRATEGY

To find the appropriate information to answer the review question, in this study a search study is defined, including the subsequent strategic activities: including the selection of relevant information, pursuing of relevant information, defining criteria for rejection of non-relevant standard, as well as the selection of the study research language. Research activities in the strategic direction included the following:

1. Selection of adequate and relevant information sources, where "Google scholar" is considered as the main source literature.

2. Following the direct technical definitions and search expression to find the relevant information, this is in order to reach the right and satisfactory answer to the main research question, Using the expression "virtualization security," this study had realized that there are around 90 papers of relevant topics.
3. In the rejection standards, we defined the subsequent criteria to focus our work.
4. None English articles are discarded, which had led to the removal of 3 articles that were removed in this step.
5. Articles whose contents not exactly about Virtualization are discarded.
6. The final result at this juncture was that 34 articles were chosen (appendix 1).
7. Some eight articles are discarded, those who point to a very specific domain in the virtualization realm.
8. Also, eight articles that were not accessible had also been dismissed.
9. Lastly, the subsequent papers were chosen as reliable sources of this systematic, structured literature review.

Table 1:- Shows the references used in the literature review.

[SLR1]	Effects Of Virtualization On Information Security By Shing-Han Li, David C. Yen, Shih-Chih Chenc,
[SLR2]	Virtualization: A Key Feature Of Cloud Computing By: U. Gurav, R. Shaikh
[SLR3]	Threat As A Service? Virtualization's Impact On Cloud Security" By; Hsin-Yi Tsai
[SLR4]	Secure Virtualization And Multicore Platforms State-Of-The-Art Report, By Heradon Douglas And Christian Gehrman
[SLR5]	Virtualization And Information Security: A Virtualized DMZ Design Consideration Using Vmware Esxi, By Singh Shiv Raj
[SLR6]	A Survey On Virtualization Service Providers, Security Issues, Tools And Future Trends, By Pooja Kedia, Renuka Nagpal, Tejinder Pal Singh
[SLR7]	The challenge of securing the virtualized environment by Lee Garber
[SLR8]	Virtualization Security Risks And Solutions Of Cloud Computing Via Divide-Conquer Strategy, By Xiangyang Luo, Lin Yang, Linru Ma; Shaming Chu; Hao Dai
[SLR9]	Security Framework For Virtualization Based Computing Environment By Patra.Niki Tasha, Sahoo Jyoti Prakash, Mahapatra .Subasish, Pati .Sarada Prasanna

[SLR10]	Virtualization: What Are The Security Risks By Kurt Fanning And David M. Cannon
[SLR11]	Trends And Risks In Virtualization, Master Thesis By: Ioannis Chatzikyriakidis
[SLR12]	A New Virtualization-Based Security Architecture In A Cloud By Lena Almutair, Soha Zaghloul
[SLR13]	Pouring Cloud Virtualization Security Inside Out By: Yasir Shoaib, Olivia Das
[SLR14]	Virtualization, Is It Worth It? A Technical, Financial And Economic Approach By Errol A Blake, Victor A. Clincy

5. RESEARCH FINDING

5.1. RECOGNIZED SECURITY ISSUES

Form the scrutinized articles listed in the table above, the researcher had recognized twenty-two (22) information security issues. Security issues related to the virtual environment management were excluded to remain with seventeen (17) security issues.

Shoaib et al. [SLR13] categorized the issues into three major groups, and the research added a 4th group: which can be listed as follows:

a. Security issues related to the guest virtual machines

- i) Data lifetime [SLR4]
- ii) VM Escape [SLR 2,6,9]
- iii) VM Alteration [SLR6]
- iv) VM Poaching [SLR3], [SLR6]
- v) Antivirus storm [SLR7]
- vi) Virtualization platform in building network [SLR8]
- vii) System restore [SLR11]
- viii) VM Hopping or Guest to Guest Attack [SLR3], [SLR6],[SLR9]

b. Security issues related to the host (Hypervisor / VMM)

- i) Hypervisor Hyperjacking [SLR6]
- ii) Unsecure VM migration [SLR5], [SLR6]
- iii) Network internal and external threats [SLR7], [SLR14]
- iv) VMM (Hypervisor) resource allocation vulnerability [SLR5]
- v) Vulnerabilities of the Hypervisor [SLR1], [SLR2]

c. Remote attacks against guest VMs and the host.

- i) Rootkit Attacks [SLR2], [SLR6]
- ii) Malicious Code injection [SLR6], [SLR13]
- iii) Side Channel Attacks [SLR6]
- iv) DOS Attack [SLR6], [SLR8].

d. Management issues

- i) VM Sprawl [SLR3][SLR4] [SLR6] [SLR10],
- ii) Virtualization platform's security management [SLR8]
- iii) Resource access control [SLR8], [SLR9].
- iv) VM Mobility [SLR6], [SLR8]
- v) Identity [SLR4]

5.2. HIGHLIGHTS ON SECURITY ISSUES

This section tries to give some clarifications, and description for the nature of each and each identified IT security issue; this is in purpose to provide knowledge for any deeper future analytical subsequent mitigation development, which includes:

1. **Data Lifetime Issues:** The Guest operating system may require a lifetime data process, and the virtual machine may revoke the virtual machine login mechanisms. The risk appears in the sensitive data is left in the distributed persistent storage [SLR4].
2. **VM Escape Issues:** The Operating system inside the VM may have vulnerabilities in them, which can aid the attacker to insert and execute malicious programs into it, which helps in the direct interaction with the VMM and may result in transversing executable code to the VMM.

3. **M Alteration Issues:** Vital application running in the VM with a specific Policy on which application should run in the VM. Change of the policy to run an unauthorized application in the VM or the opposite may incur some blockage [SLR6].
4. **VM Poaching Issues:** VM Poaching has similarities with the DOS attack. VM poaching happens when one VM takes up more than the allocated recourse, which will cause VM crashes [SLR6].
5. **Antivirus Storm Issues:** The antivirus uses distributed agents for VM in the virtual environment when multiple agents initialize a simultaneous scan, it can cause a noticeable slowdown in the performance of the virtual environment [SLR7].
6. **Virtualization Platform In-Building Network Issues:**
If the attacker can gain access to a single Guest VM, the security of other VMs will compromise [SLR8].
7. **System Restore Issues:** Loannis Chatzikyriakidis stated restoring into the former state is a security issue of Virtualization [SLR11]. It can cause loss of valuable security updates, patches hence making the system vulnerable.
8. **VM Hopping Or Guest To Guest Attack Issues:** For VM Hopping, a guest VM can initiate an attack and gain access to other guest VM. The attacker can monitor, modify configurations, deleting data, and causing confidentiality issues. Therefore, VM Hopping is regarded as a vital vulnerability of PaaS and IaaS. It also affects SaaS indirectly [SLR3] [SLR6]; therefore, guest isolation should be implemented and securing the virtual network.
9. **Hypervisor Hyperjacking Issues:** Hyperjacking is an attack by which the intruder takes malicious control over the VMM, which creates the virtual environment within a virtual machine (VM) host. The attack surface is the software that creates the virtual machines and manages them (Hypervisor), so that the attacker can have control over the full environment without attracting the attention of the VM users [SLR6].

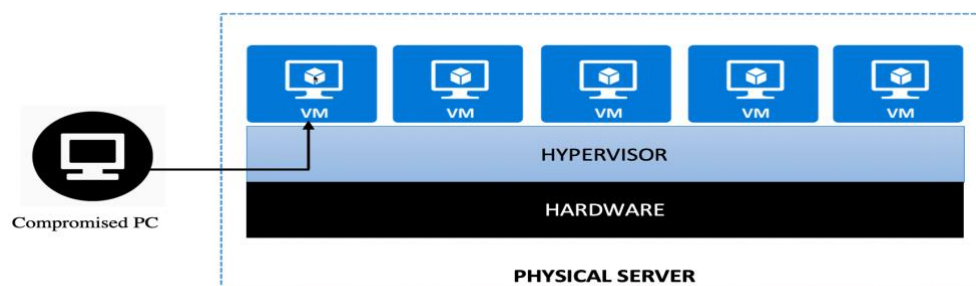


Figure 4.1 shows the Hypervisor Hyperjacking

10. Unsecure VM Migration Issues:

The data migration is an important feature in data centers; it gives the data centers high availability feature to recover from downtime due to disaster

During the migration process, the VMs are store as a file; encryption is applied to make the files incomprehensible to the interceptor. Security issues in such a case come up with the migration are of three types found in the virtual environment such as XEN and VMware [SLR5]m these are:

1. Control panel threat.
2. Data panel threat.
3. Migration module model: the Hypervisor becomes exposed in the migration process.

Shiv Raj Singh mentioned that there is a massive expansion in the use of virtualization technology in data centers. Duo to the high adaptivity and flexibility of the technology, traditional DMZ systems can be virtualized. [SLR5].

Kedia et al. mentioned that Hypervisor virtualizes all the server components to allow different processes from different VMs to utilize the full capability of the server. The Migration process is not protected against security attacks. Attackers can exploit vulnerabilities associated with the VMM to gain access to the guest VM. Vulnerabilities surface in the communication mechanisms that VMM uses during the migration. [SLR6]

11. **Software Lifecycle Issues:** the risk of a rollback of a virtual machine snapshot, appear in the software lifecycle if the version of the software in the VM snapshot is outdated or a missing security patch it may contain security vulnerability [SLR4]

12. **Network Internal and External Threats Issues:** One of the methods used to Protect the virtualized environment from the network security attacks is by routing the network traffic using a physical firewall (Device act as a firewall) to analyze the traffic and then route back to the virtual environment. Cisco's Chalasani stated this process is ineffective. [SLR7]. Blake et al. clarified that the security blind spot in the virtualized systems [SLR14]. Any loss invisibility of the network traffic is a red alert.

13. **VMM (Hypervisor) Resource Allocation Vulnerability Issues:** This is considered as a potential security risk that can lead to denial of service attacks. Hackers can exploit this vulnerability and cause a denial of service. VMM allocates system resources to the virtual machines or guest operating systems in the cloud environment.

Since VMM allocates resources, it is a single point of interaction between the virtual layer and the physical layer. In addition, VMM is responsible for preventing VMs request more resources when the virtual host is running short of its resources. In Fact, when the virtual host uses more resources beyond its allocated resources, performance will be significantly decreased. In this situation, the denial of service might happen. [SLR5]

14. **Vulnerabilities of Virtualization Software (Hypervisor) Issues:** As it is discussed in [SLR1], each virtual machine has its own virtual resources such as I/O ports, DMA channels and etc. These guest virtual machines can be run on any type of operating system because of the features of Hypervisor. For example, in VMware technology, the Hypervisor that is called "VMware Virtualization Layer" (figure 5.3) can host multiple virtual machines with sharing system resources such as CPU, memory, network driver, and hard disk. Due to complexity and a broad range of Hypervisor capabilities, there is some vulnerability against Hypervisor.
15. **Virtualization environments Issues:** As it is argued by Gaurav et al. [SLR2], there are some vulnerability issues that have been found in the virtualization software. These vulnerabilities can be exploited by a malicious user for gaining access to the system. For example, the vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could be exploited in order to run malicious code on the host or guest operating system. The other example is a vulnerability that was found in VMware, which gives users read and writes access to the system host file. Gaurav et al. discussed that consumers are not able to protect the virtual environments on their own.¹³ Cloud providers try to make their environment secure and have a minimum risk of security attacks. Thus, there is a need for a clear technical solution that guarantees the confidentiality and integrity of cloud services, and it should be verifiable by cloud customers.
16. **Rootkit Attacks Issues:** They are typically malicious software that is designed to hide the existence of some processes or programs from normal methods of detection and enable continued privileged access to the system. Detecting of these attacks is difficult sine they may subvert the software that can detect them. Rootkits are categorized into three types:[SLR6]
 - i. Binary Rootkits: they replace the binaries of the executable system utilities, and then they can hide the processes.

- ii. **Kernel Rootkits:** these kinds of Rootkits modify the system calls. They are also able to modify the kernel memory image. Since Kernel Rootkits compromise the Core of operating systems, they are considered as dangerous types of Rootkits.
- iii. **Library Rootkits:** Library Rootkits replace the standard system libraries, or they can provide a custom library. The custom library loads before any other libraries. For example, the Blue Pill is a Rootkit for x86 virtualization technology. It targets Microsoft Windows Vista. Blue Pill traps a running instance of the operating system and then acts as a Hypervisor. In this way, Rootkit gains complete control of the virtual guest machine. [SLR2]

17. Malicious Code Injection Issues: Malicious Code injection is one of the typical threats against virtual machines. Hackers can gain access to virtual machines by injecting malicious codes. SQL injection is the most common type of code injections; however, there are other types of code injections such as LDAP injection and XPath injection. [SLR6]

As it is explained by Shoaib et al. [SLR13], isolation is a benefit of the virtual environments. This feature is used by security specialists who run Malwares on the virtual systems instead of analyzing them on the production environments. Since many security specialists rely on virtual machines to analyze malicious codes, malware developers work on the methods to stop such analysis by the VM detection method. For instance, if malicious code detects a virtual environment, it can disable some of its malicious functionality so that the security team cannot detect it. Attackers have several options to detect a virtual machine. There are four categories of local virtual machine detection, including:

1. Searching for VME artifacts in the processes, file system, and registry
2. Looking for virtual machine artifacts in memory
3. Looking for specific virtual hardware
4. Looking for virtual machine specific processor instructions

18. Side-Channel Attacks: Side-channel attacks are based on side-channel information. In this kind of attack, attackers try to exploit one of the physical characteristics of the virtualization hardware and gain some information about the hardware resources. For example, timing information, power consumption, and CPU usage can provide some important information that can be exploited by hackers for breaking into virtualized systems. [SLR6]

19. **DOS Attack Issues:** As all guest virtual machines use the same physical resources such as memory and CPU, denial of service attacks can break the whole virtualization system. Virtualized environments have more overhead than the traditional systems, and even a light DOS attack can increase this overhead considerably. Hypervisor experience high overhead while using the I/O devices such as network interface. Since DOS attacks try to increase the overhead on a victim system, this situation will amplify the virtualization overhead and become much more effective at the target. [SLR6]. Luo et al. mentioned malicious applications could take too many resources and make vitalization services very slow. It can even stop all the services. [SLR8]
20. **VM Sprawl Issues:** VM Sprawl is defined as a large number of virtual machines in the cloud environment without proper IT management [SLR6]. VM Sprawl is one of the biggest issues that lots of data centers are facing. Since a new virtual machine can be created easily in a few minutes, the growth of virtual machines is not completely obvious, and after a while, organizations will face lots of guest VMs. VM diversity is one of the features of cloud computing and lets users create several virtual machines efficiently [SLR3]. VM diversity can cause the VM Sprawl issue.

Scaling is one of the benefits of Virtualization, and it enables the fast creation of new VMs. This feature destabilizes some security management activities such as system configurations and system updates and causes security issues [SLR4].

Transience: virtual machine instances can be easily created or removed. This situation is considered as a problem for consistent management, and there is a risk that some security issues such as worms remain undetected [SLR4].

Scaling and transience features of Virtualization can also cause the VM Sprawl issue. According to Fanning et al. paper, failures of IT management causes security issues (VM Sprawl) in the virtual environments [SLR10]. Ease of creating new virtual machines can cause a lack of visibility of the controls within the virtual environment. This is mainly true in the field of change management. Change management controls are frequently forgotten when virtual machines are created. In addition, distinctions between testing and production environments should be carefully considered. All logging and access controls need to be applied to the test environment (virtual systems). The other management security issue is the breakdown in the effectiveness of some logical access controls. For instance, some users that do not have an administrator right on the physical servers might

gain it in the virtual environment. This issue sometimes happens due to neglecting the system administrator. Consequently, we have to consider that Virtualization needs a big change in management policy. Ignoring change management will raise significant security issues in virtual environments.

21. Virtualization Platform's Security Management Issues: As it is explained in [SLR8], traditional methods of network management and network monitoring are not efficient in virtual environments. Network concepts are changed from hardware to software in the virtual environment. For example, a virtual switch is software that allows virtual machines to communicate with each other. With using the virtualization layer in addition to the physical layer, there is a need to monitor the logical infrastructures as well.

22. Resource Access Control Issues: Since users can only see the location of the logical data storage and they do not have any information about the location of the main storage infrastructure, they might send some confidential data to the public cloud. This situation might cause data leakage[SLR8]. Niki Tasha et al. mentioned how the host machine can control all the virtual machines. The following actions can be done from the host side:

- Start, shutdown, pause, and restart VMs.
- Monitor and modify the available resources of the virtual machines.
- Monitor the applications that run on VMs.
- The host can view, copy, and modify the data that is stored on the virtual disks.

Performance monitoring tools allow us to monitor the shared pools of CPU, memory, network, and storage resources. Internal contentions of these shared resources make it too difficult to determine the source of applications. [SLR9]

23. VM Mobility Issues: The rapid deployment of a VM can be done by duplicating installed VM; the security issues is when the duplicated VM has a vulnerability, a security threat, or misconfiguration that allows an attacker to gain access to the VM. Hence help the rapid spreading of vulnerable VM across the virtual environment. Hsin-Yi Tsai [SLR3] discussed, VM mobility is one of the features of the cloud computing environments and provides quick deployment, although it might cause some security issues. AlMutair et al. also pointed out that VM mobility can cause

security issues. They mentioned that the cloud is a loss of control [SLR12]. The user/consumer does not know where data is stored and processed. Data can cross international borders over the Internet, and this can expose cloud consumers to further security issues. A different example that illustrates the loss of control is when the cloud provider runs services that do not know the details of it. This is the dark side of the Infrastructure as a Service.

24. **Identity Issues:** Some identifying mechanisms such as MAC address or owner name might not function well in the virtual environments. System ownership and responsibilities are more difficult to track in a dynamic virtualized environment. [SLR4].

5.3. EFFECTS OF VIRTUALIZATION SECURITY ISSUES ON INFORMATION SECURITY:

Concerns and issues in the Virtual environment show as Security vulnerabilities, threats a very important and challenging issue of Virtualization. According to the latest researchers, ISO/IEC 27001 standard is one of the security standards that can be used for the evaluation of information security measures of virtualized environments.

Li et al. stated about the effects of Virtualization on information security [SLR1], that: there are a huge amount of vulnerabilities, threats, concerns that need to be solved in order to adapt and implement Virtualization. In addition, Virtualization brings new patterns of information security.

For instance, Christodorescu et al. have planned a cloud security monitoring system that can be installed on the virtual machines and monitor the cloud environment from the outside without knowing the guest operating system.

For realizing the effects of Virtualization on information security, a questionnaire was designed by Shing-Han Li et al. The questionnaire was based on three parts: personal information, company information, and questions adapted from the 32 qualified ISO/IEC 27001 controls concerning the virtualized information environment and information security.

The result of the analysis indicates that using Virtualization in companies might be beneficial for information security. For the electronics, IT, and automobile industries using

Virtualization has significant effects on information security in the aspect of physical and environmental security.

For the IT and automobile industries, Virtualization has a significant effect on information security in the aspect of access control. For IT industry professionals and IT managers, Virtualization has a significant effect on information security in the aspect of communication and operation management while for development and maintenance; Virtualization does not significantly influence information security.

6. MITIGATION OF VIRTUALIZATION SECURITY ISSUES:

This section is about frameworks and solutions for the mitigation of virtualization security. The research study in this section tries to have a direct reflection on the research question How to mitigate the security issues in the virtual environment?.

Scholars and researchers are always concerned with mitigation of the virtual security issues and other issues as well. This section is had examined some applied models to mitigate the visualization security issues

The research study reviewed and apprehended the different types of virtualization security issues (chapter 5). Having got the necessary knowledge about the virtualization security issues, it went onward to study Solution techniques for addressing some of the most important technical virtualization security issues.

The study is focusing on some selected mitigation techniques, whereas some mitigation techniques such as "VM Sprawl" that can address management security issues of Virtualization are not discussed in this part due to time limitation.

6.1 PROPOSED MITIGATION 1

The virtualization framework introduced by AlMutair et al. had suggested two virtualization security frameworks.

6.1.1 THE FIRST FRAMEWORK

This framework is divided into two modules:

- I. Virtual system security
- II. Virtualization security management

Figure 5.1 shows the first framework, which consists of two different modules; these are virtual system security and virtualization system management, which are inspired to accomplish their dedicated task without disturbing each other.

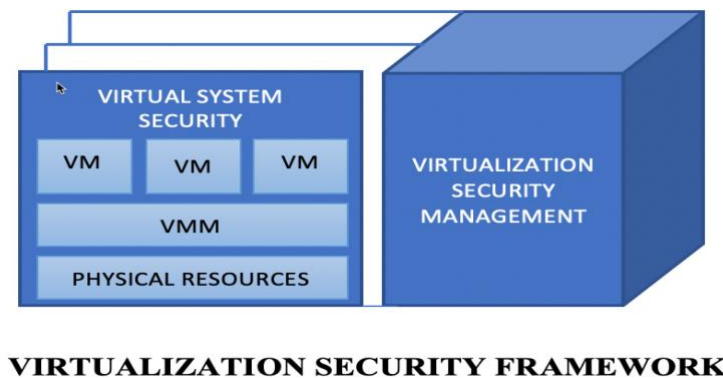


Figure (5.1) Virtualization security framework

The virtual security must incorporate the three layers of Virtualization: physical resource layer, VMM, and VMs that provide services to the consumers. Accordingly, there are four main components of the virtual system security: which are: 1/ The VM system architecture security, 2/ the Access control, 3/ the Virtual firewall, and 4/ the Virtual IPS/IDS which are discussed as follows

(a) VM Architecture Security System: The VM Architecture Security System is a system of the virtual environment which should be robust and efficient; the following Figure shows the VMM is managed through a dedicated VM called Admin VM, it has full control of the VM guests. The solutions based on virtualization architecture aim to solve security vulnerabilities by employing security measures on the virtualization components and characteristics.

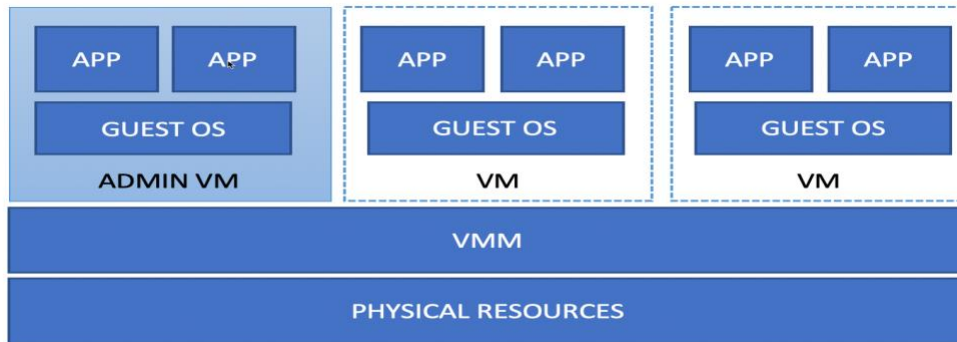


Figure 5.2. VM system architecture shows the inclusion of admin VM with the other VMs

(b) Access control: Access control is a technique that employs a list which contains the authorized user and what resource is the user can access. Physical access regulates access to the campuses, buildings, rooms, and physical IT assets. Logical access regulate and maintain the logical structure of the system component, network, resources (what is connected where). Access control examines whether the VM is authorized to have access to the dedicated physical resource or not. The following Figure elaborates on that. There are three layers in the Access control:

- Virtual machine system layer
- Virtual machine monitor system layer
- Physical resource layer

The framework comprises of access control agent (ACA) and access control enforcer (ACE). ACE governs the VM access activity based on its security policy profile. Guest VMs request access to physical resources from the ACA; the ACE receives the requests forwarded by the access control agent. After that, the ACE responds to the request according to the security policies.

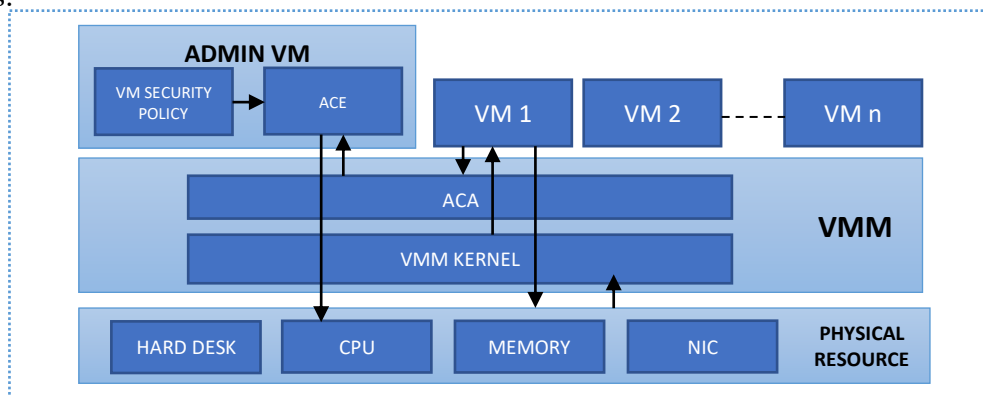


Figure (5.3) Access Control Illustration

(c) Virtual firewall: The **virtual firewall (VF)** is a network firewall or appliance running within a virtualized environment, which provides similar protection services as the physical firewall. The VF can be part of the virtual environment as a program in the VMM or as a guest VM, whose duty is to protect the network from outside attacks.

(d) Virtual IDS/IPS: Intrusion prevention is the process of finding intrusion and then stopping the detected security incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of network security infrastructure to detect and stop potential incidents.

Virtual intrusion detection and prevention system gathers and inspects the network traffic to detect and prevent counter the possible security attack. Virtualization Security

Management: This component is divided into the subsequent parts

Virtualization security management is divided into the following parts:

a. Patch management: is management uniting that is responsible for installing patches and testing the patches. Its task is to gather information regarding the recently offered patches, as well as for deciding which patches are related to the specific system. It guarantees that the patches are installed correctly, perform system test after the patch installation as well as documenting all the steps taking and the glitches found in the patch.

b. VM migration management: the VM migration is a defenseless process; An attacker can exploit any relevant vulnerability through out the process, a securing mechanism should be implemented during the migration.

c. VM image management (VMI): the unit deals with the type of file used in the VM creating, cloning as well as migration. Every process requires a special kind of format to execute the process.

As an overall assessment, each and every framework has its Advantages and its advantages.

So the following points are perceived as advantages of Framework 1:

- The two modules (virtual system security and virtualization security management) that function simultaneously and seamlessly will enhance the efficiency of the framework.

- The authorization process only allowed VMs to access the resources. Dividing the Virtual system security into three parts and each one of them is responsible for a different security issue.
- Reduced security tasks for the VMM by splitting the task to the admin VM, hence VMM overhead is reduced.
- The patch management, VM migration, and VM image management have a dedicated unite virtualization security management.

Whereas Cons of Framework 1, are perceived as that the framework can build an overhead is the number of VMs is large. Hence response time and performance of the VM will decrease substantially.

6.1.2. SECOND FRAMEWORK

While the workload of the VM increases abnormally, the VM tends to be vulnerable for exploits and attacks, hence adding a unit to the VM architecture to monitor the activities Figure (5.4) Shows the Architecture of Secured Virtualization and events of the VMs. To enhance the security performance feature such as security reliability monitoring unit (VSEM and VREM) are added. The main modules of the security system are in the Hypervisor HSEM and HREM.

The modules can detect in the VM is malicious or not. HSEM get essential information from the VSEM and HREM. Figure (5.4) below illustrates the architecture and additional units such as VSEM, VREM, HSEM, and HREM **VSEM has two control levels**, which assists the HSEM to recognize all the harmful activity with fewer processes. The VMs security activity is monitored by the VSEM and then sent to the HSEM.

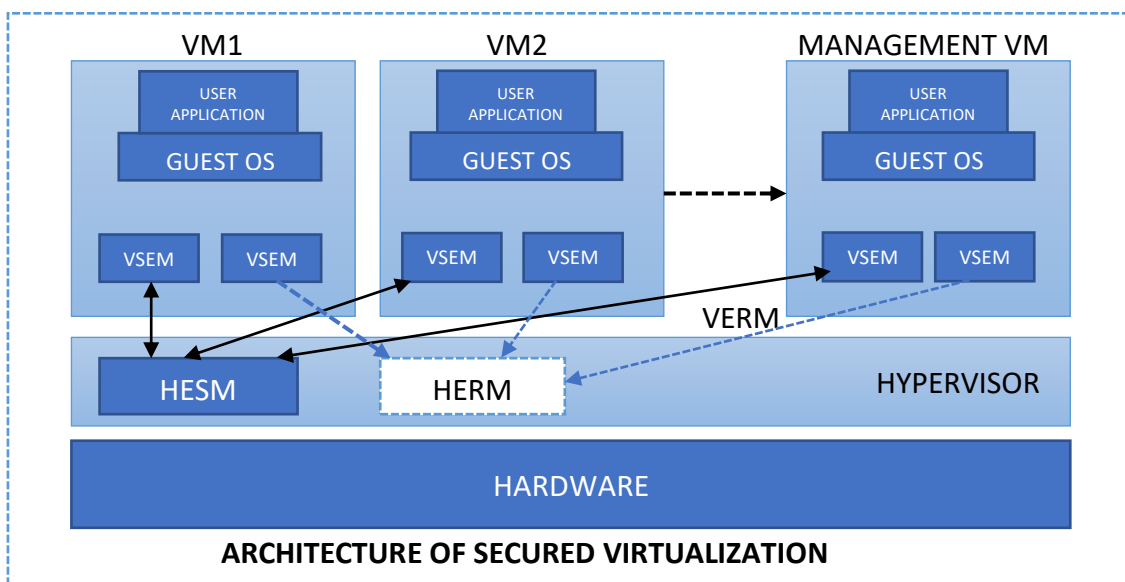


Figure 5.4. The Architecture of Secured Virtualization

VSEM CONTROL LEVEL 1:

The VSEM collects IP addresses (source, destination) as well as statistics about the transmitted data, successful and unsuccessful Packet received by the Hypervisor.

The VSEM searches for malicious activities based on the history of the VM, which the HSEM provides it. For example, the number of service requests from the Hypervisor exceeded the average (based on VM history). The system classifies the Virtual machine as a potential attacker or victim. Moreover, the VSEM changes to the second level and informs the HSEM about it. HSEM examines the VM to find harmful activities.

VSEM CONTROL LEVEL 2:

VSEM will conduct detailed monitoring of the VMs. The resource request, request sent to the Hypervisor, and packets sent to the destination will be captured. When level 2 of control is initialized, the VSEM informs the Hypervisor. The HSEM sets deploy rules to deal with suspicious VMs and set limitation for it until the VM declared not an attacker or victim

VM Reliability Monitor (VREM):

The VREM monitors the workload within the VM, using defined reliability parameters, and informs the load balancer built in the Hypervisor. VREM transmits the workload status to the HREM and requests the VM status from the HSEM. The HREM decides whether to issues more resources to the VM or not.

If the VM demands more resources (different than the observed behavior in the history usage), HREM may be a red flag an overflow attack and informs the HSEM.

Likely there are always some advantages and of the systems. So framework two, as it has two levels of control and behavioral analysis, is the VM security management (VSEM), which assists HSEM in examining the status of VM. It is perceived that it has the following advantages:

- It is flexible and dynamic, as the VSEM switches to Level 2; it notifies the HSEM about the switch.

- HSEM limits the VM access to the requested resources until it defines the VM behavior as not attacker no victim.
- Detection and prevention mechanisms are implemented within the framework.
- VM reliability is monitored by VREM.
- VREM forwards the workload status to the Hypervisor reliability management module.
- After the data analysis, the VM can get access to the resources or not.

limitation such as:

- The VSEM and VREM security components allocate and consume system resources to function with maximum efficiency.
- The problem of identifying the suspected VM is Victim or attacker.

6.1.3. REMARKS ON THE COMPARISON OF THE TWO FRAMEWORKS:

In general comparison between the framework one and two, Framework one consumes high bandwidth. For example, when the VM request to access the resources, the request is sent to the ACA which interact with the ACE in the admin VM. Many requests for a small process the bandwidth consumption will be too high.

In the framework two, security tasks are divided between the Hypervisor and the security components in the VMs (VSEM), but the HSEM makes the final decision in the Hypervisor. So framework one is understood efficiently on a small scale, while the second framework is valuable in a large number of VMs.

VM migration management, virtual firewall, Access control mechanism, virtual intrusion detection/prevention system, the first framework has security and reliability units that can handle (unauthorized access) security issues. Hence the following security issues are addressable by the reviewed mitigation method, which is: VM Escape, VMM resource allocation vulnerability, Hypervisor Hyperjacking, VM Hopping, Unsecure VM migration, and Network internal and external Threats, VM Poaching.

6.2 PROPOSED MITIGATION 2

Securing Virtualization using the SELinux-base security approach had been introduced by Ren et al. [18], by preventing unauthorized access to a virtual machine (VM escape). The SELinux provides an access control solution that can isolate virtual machine processes from the system processes. It implements a Multi-Category Security (MCS) protection Mechanism, which ensures the seamless security of multiple virtual machine processes together and individualistically to accomplish secure access to the virtualized server.

The SELinux (Security-Enhanced Linux) was developed by the National Security Agency. It utilizes MAC policy, which relies on the least privilege to be used by the programs to perform their intended tasks. The access controls are based on the type of access control characteristic, which is called a security context. Objects in the operating system such as files, sockets, and processes are associated with the security context. All the security context comprises three parts: user, role, and type identifier.

The highlighted part in the Figure below shows the security context for the "install.log," "root," "object_r," and "user_home_t," which show user, role, and the identifier types related to the security context.

```
[root@localhost ~]# ls -Z
-rw-r--r-- root root root:object_r:user_home_t 1
-rw----- root root system_u:object_r:user_home_t anaconda-ks.cfg
drwxr-xr-x root root root:object_r:user_home_t /etc
-rw-r--r-- root root root:object_r:user_home_t install.log
-rw-r--r-- root root root:object_r:user_home_t install.log.syslog
drwxr-xr-x root root root:object_r:user_home_t /var
drwxr-xr-x root root root:object_r:user_home_t /var/log
[root@localhost ~]#
```

Figure 5.5. Security context of install.log file

Securing Virtualization environment using the SELinux scheme: it consists of three main components, Mandatory access control include type enforcement (TE), role-based access control (RBAC), and multilevel security (MLS) as an optional component. The three parts are highly configurable to the user's demand. Type Enforcement (TE) is the basic model where

the other models are an advanced type of the TE model. The TE model considers the system as a set of subjects and objects, which can all be identified with types.

All accesses are identified for authorization by the SELinux model; there are no authorizations by default. In the TE based RBAC model, all the processes are restricted by the role identifier of the process security context. As previously mentioned, the entire object (files, sockets, and processes) was given a security context (user, role, and type).

Processes execution is applied to a different object; the operation right of execution is provided by the SELinux access control policy. Moreover, the TE model restricts the users to access all kind of objects if the corresponding policy is no defined. Therefore the SELinux security policy can separate independent processes from each other. Hence VM processes are restricted to its dedicated VM image file, not other Image files no the host system files.

The illustration shows the difference between a physical server and the virtual server. The security of the physical server is by placing an intrusion detection system and deploying an antivirus that can protect the server. As for the virtualized server, several VMs run in the server, and a malicious VM can directly attach other VM or the host. Securing the

A virtualized server using SELinux can be implemented to separate VMs from each other and create a protective layer for the host.

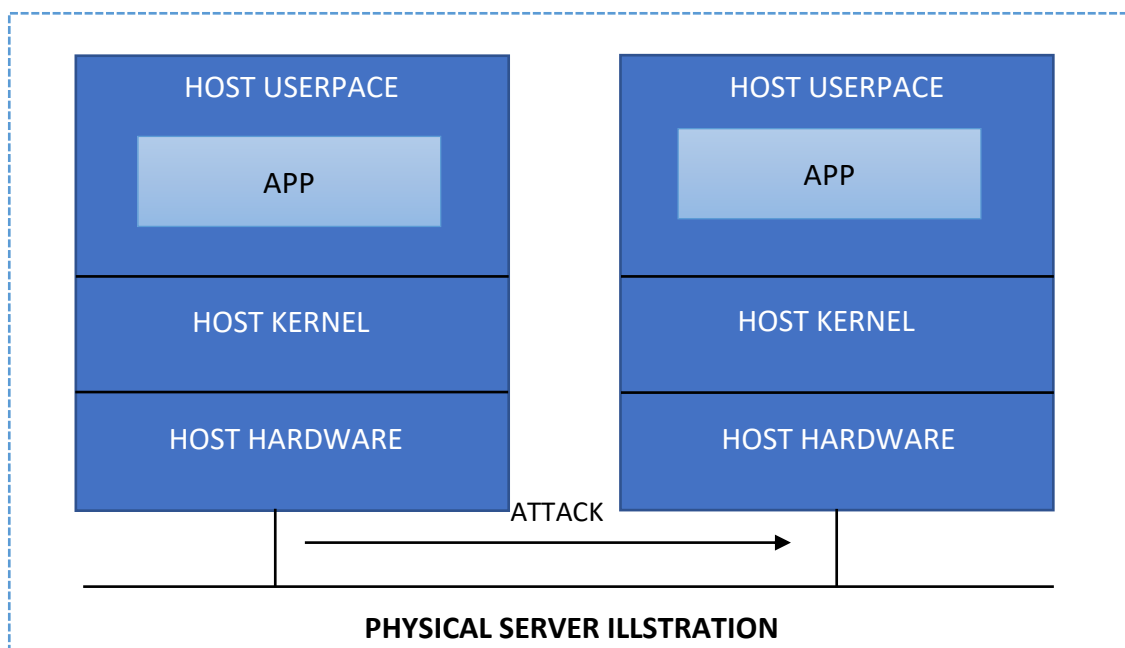


Figure 5.6 Physical server

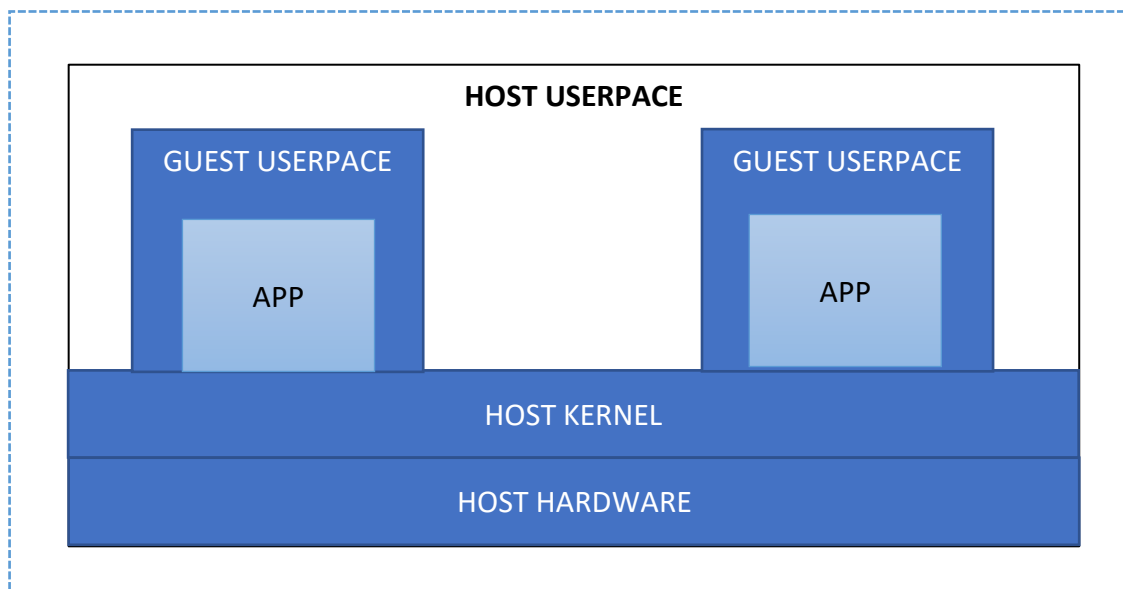


Figure 5.7. Virtualized Server

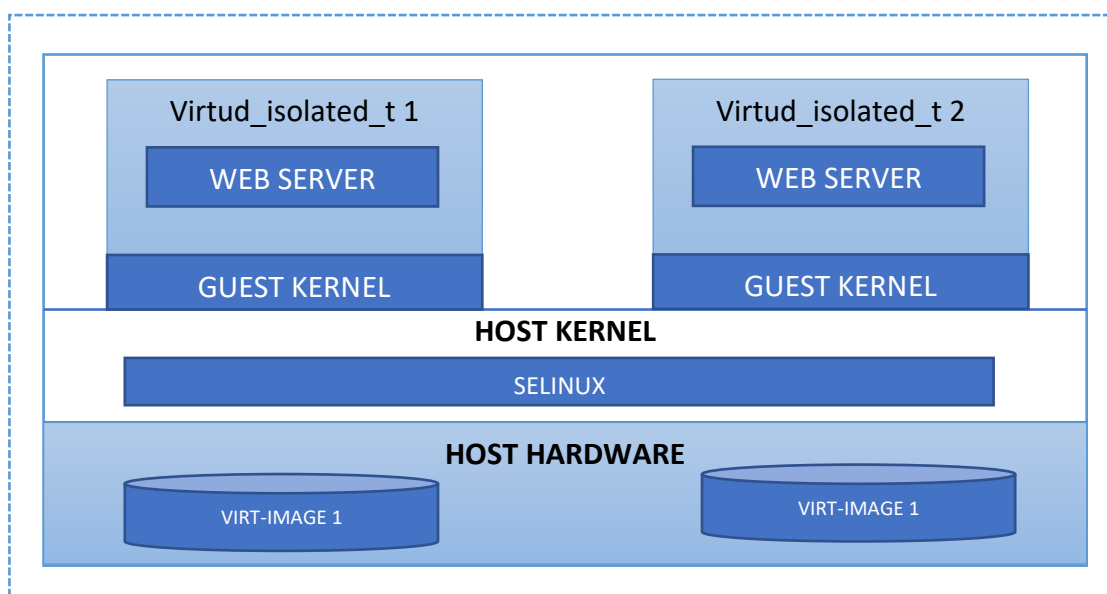


Figure 5.8. Implementation of secure virtual server using SELinux

REMARKS

Solution 2 is built on the SELinux model, which prevents unauthorized access to the virtual machine. It also provides VM isolation in terms of process, users, socket, and other VM kernel and userspace. Hence the approaches mitigate vulnerabilities in the virtual environment like VM escape and Hypervisor Hyperjacking (guest to host privileged escalation). The mentioned attacks will have reliability issues for the virtualized server.

6.3. PROPOSED MITIGATION THREE:

The data transferred between VMs and as well as between VMs and Hypervisor has no security control. It is not visible in terms of content security, which can provide security

issues in the virtual environment. Benzidinedane et al. presented a solution to fix these issues. The primary motivation is to govern the inter-VM traffic by analyzing and then stopping the malicious Packet.

The security solution goal is to control and analyze the inter-VMs frames, in order to achieve that the security approaches introduced frame tag by an agent in the VM. It is added to the payload of the IP packet, which will ensure high-level integrity. The receiving VM's agent analyzes and authenticates the impound frame, then accept or reject the packet frame based on the tag found in the frame. The frames sent from the VM must be verified by including the following identifiers in the frame tag:

- a. A VM agent produces authentication factors added to the IP packets.
- b. VM agent detects and analyzes the Packet, also rejects the noncompliant once.

The frame tag: it contains two components: The tenant tag and application tag. The frame tag transaction is between a pair of communicating agents, which are:

- Tenant tag: upon tenant creating an identity will be assigned to it; also, a tenant tag is created. The Tenant identity is stored in the database. The request between VMs in the same tenant, the agents, generated the frame tag and added to the payload. This provides a strong tenant isolation
- The application tag: An ID will be assigned to all the Installed applications in order to create the application tag. Application tag stores in the database.

The request send from APP1 in the tenant1 to DB1 hosted in different VM within the tenant, the agent in the sending VM generate the frame tag by adding (tenant and application tag)

Policy Management (PM):

The model is in charge of received/sent IP packets. The main function is to allow or discard the Packet. It has a database called (PM database PMD). The database interacts with the agent to get a regular update, which helps to define the status of the entire incoming Packet, whether to drop them or accept. Every IP packet was checked against the PM. If the tag is correct, it is forward; if not, the IP packet gets discarded.

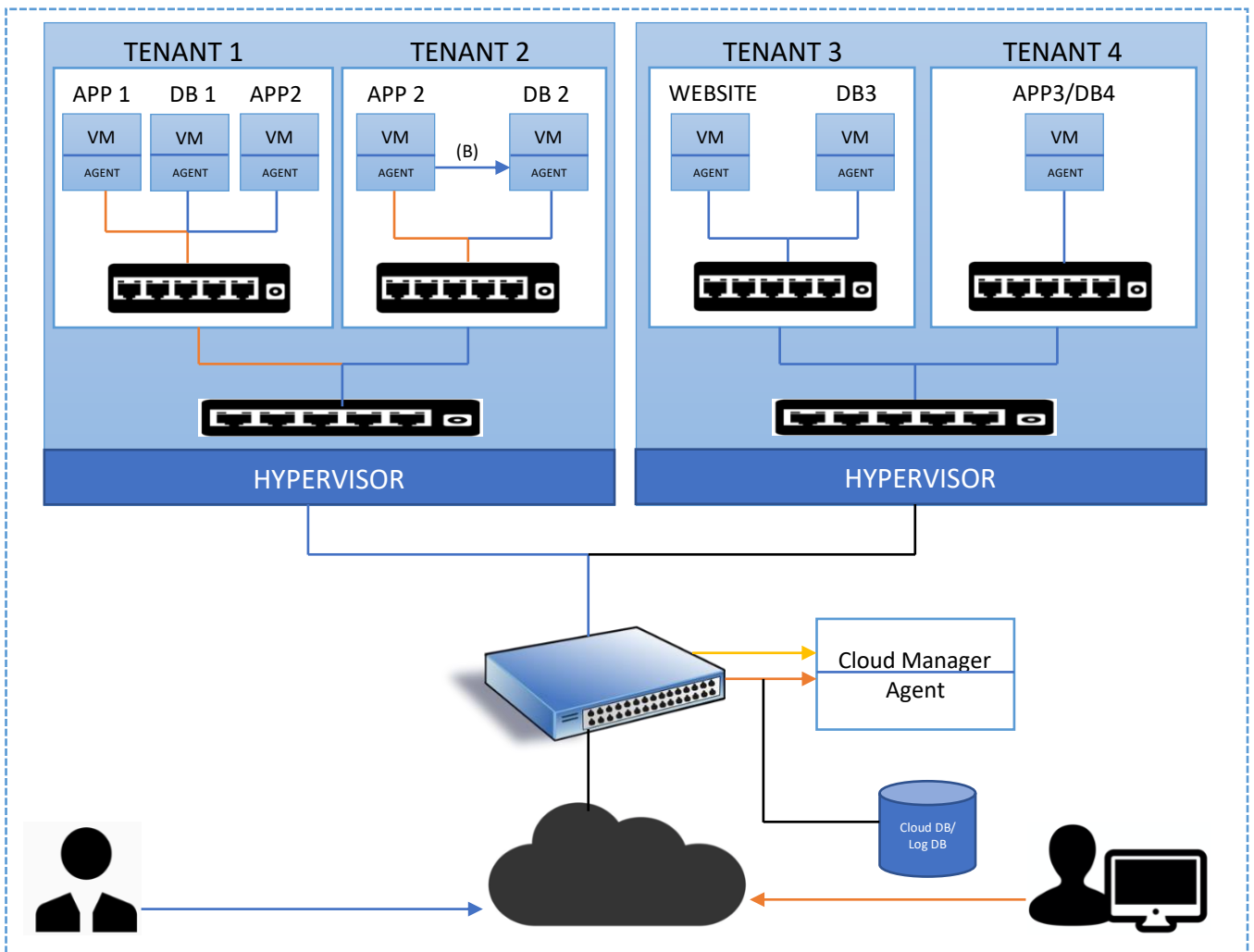


Figure 5.9. The cloud provider model

Security Contract (SC): a secure and legit frame tag is critical for the model. The SC is created to apply encryption and hash algorithm between the interacting VMs/agents to provide secure communication.

SC database (SCD): a central database shared between the agents to ease the identification of the agent. Upon SC creation, an ID is issued to it called security contract ID and added to the SC database (SC-ID).

Agent: it behaves like a lightweight IDPS /firewall; it is the prime controller of the IP layer. Moreover, the agents' responsibility is to generate all the required fields. There are two pairs of requests the work simultaneously, receiving/analyzing, or sending/generating.

When the IP packet reaches the VM, the agent checks particular fields in the IP packets and responds automatically either accept or reject the Packet according to the PM.

The agent has automated self-generated rules for the decision taken regarding the received IP packet. The component used is called the rules engine; it executes the function is base on the trust level value. The rules engine gets the tenant and application tag and evaluates the value of the trust level from the PMD in order to generate a suitable ruleset.

Flag: it is an indicator that is appended by the sending agent at the start of the payload. Flag point to the action that should be engaged by the receiving agent relying on its value. For farther classification, the flag is a set of bits to define the type of data carried in the payload. The following Figure shows the complete steps taken to send of transmitting IP packet from App1 in Tenant 1 one to DB1.

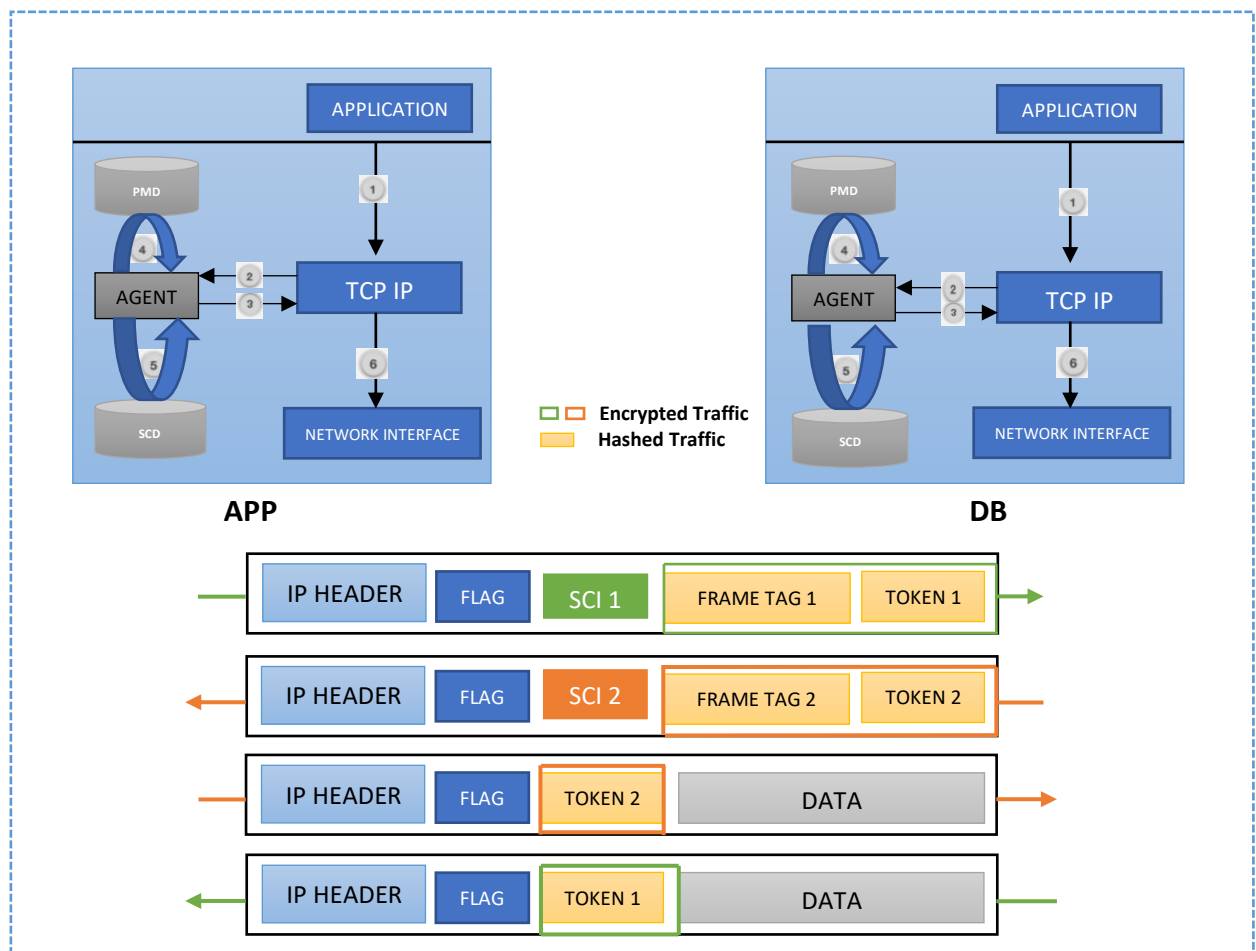


Figure 5.10. Workflow of IP packet processing

Most of the cloud service providers create template OS ready to use, with the agent embedded in them, to ensure the security of the virtual environment.

REMARKS

The solution introduces a mechanism to remove the lack of visibility and enhance the security controls in data transmission between the VMs as well as the VMs and the Hypervisor by supervisory the inter-VM traffic, analyzing, and then stopping rouge or malicious ones. The solution enhanced the VM security by utilizing authentication, integrity, and trusted transactions method, as well as implementing policies and intrusion detection means. By using this solution, we address the Hypervisor Hyperjacking, Unsecure VM migration, and VM Alteration and Virtualization platform in building network security issues.

7. CONCLUSION

At this point, the study comes to its completion and closure. The research conclusion is following some three work segments: The general remarks, a technical summary, and the future considerations

7.1. GENERAL REMARKS

The virtualization security issues were categorized into four groups. One group is non-technical, which is identified as management issues, such as VM Sprawl, Virtualization platform's security management, Resource access control, VM Mobility, and Identity issues. Management security issues were not discussed in the Thesis. Hence there is a need for more research on the topic.

In section sixth (mitigation of security issues) of this study, some three solution techniques were chosen to address the non-management security issues. They are considering the importance of the characteristics of the virtual machine in order to choose a suitable solution, such as the number of clients, the number of virtual machines, the hardware resource availability, and the application implemented in the virtual environment. For example, in the first solution (solution one), two different frameworks were introduced. The researcher claims that their effects depend on the number of VMs in the virtual environment. The first framework performs better within a small-scale virtual environment. The second one is the opposite of that. Each of the frameworks uses a different security method. Solution one is based on access control, intrusion detection, and prevention techniques as well as resource monitoring.

Solution two is based on SELinux-secure virtual server implementation. It utilizes all objects (such as files, sockets, and processes) with a security context. Implementing the SELinux approach, helps in VMs isolations, to prevent security issues like VM escape.

Mitigation (solution) three recommends a method for improving security controls and visibility during the data transfer between VMs and Hypervisor. The method proposed is to control and analyze the inter-VM traffic by applying a frame tag, which is added through an agent place in the VM. The agent adds the tag to the payload of the IP packet. Though the implementation of this method, a high level of integrity is achieved, Mitigation technique three recommends an approach for improving the visibility and security controls while transferring data between VMs and Hypervisor. This approach aims to control and analyze the inter-VM traffic by applying the Frame tag. The frame tag is added via an agent in the payload of the IP packet that ensures a high level of integrity.

Virtual environment administrators can apply multiple techniques to address security issues. For example, implementing solution one in a virtual environment will not solve "vulnerabilities of virtualization software" therefore, solution two can be used to fix the security issue.

Studying the benefits of Virtualization from an information security point of view is not within the scope of this research, more studies in this area are needed to study the effect of different mitigation methods on the CIA model. Is it possible to formulate a mitigation method that can comply with the entire CIA model?

7.2. SUMMARY

This research study had embarked on metadata of the security issues in the virtual environment, and methods to solve the security issues.

As it had been referenced before, virtualization technology is the key element of utilizing computing power to its maximum capacity by executing processes simultaneously without downtime. Also, virtualization technology is the main component of cloud computing. But it appeared that it complicates the security measures, new vulnerability, and security issues arise.

Initially, the essential terminology is of the cloud compute/ virtualization/ hypervisor is described, and the services associated with it. The main goal is to giving the reader an insight into what are Cloud and Virtualization.

A structured literature review is accomplished, to classify relevant security issues in the Virtualization environment which answer the first research question.

Google Scholar was used as the principal source of finding scientific literature in this research.

After the attentive study of the literature, 14 papers were chosen to do a structured literature review. The outcome of studying though articles led to the classifying of 23 security issues, all of which are clarified in detail in the Thesis.

Section six of the Thesis contains the Proposed mitigation and is explained for addressing the second question. Three Proposed mitigation are described to mitigate some of the major virtualization security issues.

The table below illustrates the relation between virtualization security issues and the presented solutions to mitigate those specific security issues.

Table 2:- Security issues of Virtualization and mitigation Approach

VIRTUALIZATION SECURITY ISSUES	PROPOSED MITIGATION 1	PROPOSED MITIGATION 2	PROPOSED MITIGATION 3
Vulnerabilities of virtualization software		•	
VM Mobility			
Software Lifecycle			
Identity			
Data lifetime			

VMM (Hypervisor) resource allocation vulnerability	•		
VM Escape	•	•	
Malicious code Injection			
Hypervisor Hyper jacking	•	•	•
VM Sprawl			
Side-Channel Attacks			
VM Alteration			•
Rootkit Attacks			
VM Hopping or Guest to Guest attack	•		
VM Poaching	•		
Unsecure VM migration	•		•
Antivirus storm			
Network internal and external threats	•		
Resource access control			
DOS/DDOS Attack			
Virtualization platform in building network			•
Virtualization platform's security management			
System restore			

Table 3 illustrates the relationship between the proposed mitigation methods and the CIA Model. The table shows the effect of the solutions on one guide policies for information security of the CIA model (Confidentiality, Integrity, and Availability)

	Confidentiality	Integrity	Availability
Proposed mitigation 1	•		•
Proposed mitigation 2	•		•
Proposed mitigation 3	•	•	

7.3. FUTURE CONSIDERATION

This research study on virtualization security issues had explored the extent and variety of virtualization security issues within the virtual computing environment. Furthermore, it had also tried to demonstrate some applied solutions to virtualization security issues.

The research work had realized that virtual security concerns are vast in an ever-changing world of technology. The ever-growing human need for Virtualization is exerting more and more challenges.

Virtualization and virtualization security issues are not and never being isolated from other global challenges and undertakings. Virtualization is a human creation that is applied everywhere and anytime in space, earth, demography as well as and health, etc.

1. Not to miss this specific year, when this research is being carried a unique global phenomenon happened that implies a radical change in human life, the COVID-19, which definitely enforced an extra demand on Virtualization as a global technology. (What COVID-19 had refecction on Virtualization is a valid research scheme.
2. The simple and direct answer to mitigate the virtual security issues is to ask again, how to proceed to contain the virtualization security challenges. This can be thought about several aspects, to include:
 - a. Universities and research institutions should develop strategies to support and facilitate more future studies for more knowledge generation and innovations to mitigate huge information security issues.

- b. Specific studies are necessary to update the researchers and practitioners to acquaint them with the knowledge to define and update vulnerabilities of Virtualization and the virtual environment.
- c. From identification and classification of Virtualization security issues, it is realized that there are some specific concerns pertaining the management aspect of virtualization security, this area (the virtualization management issues) which is not covered in this study, need special attention, to develop specialized information security management capacity building conferences on managing Virtual securities.
- d. Networks of professionals deem necessary for consultation and information sharing. Halmstad University can take the lead for its alumni and other potential fellowships.
- e. Information hacking and hijacking have legal and financial aspects; there is always a need to undertake studies of such backgrounds.
- f. The event of the COVID-19 pandemic lockdown had limited efforts in search of primary data; this necessitates more studies on virtualization security issues.

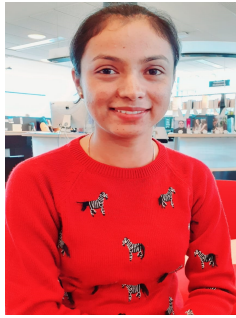
8. REFERENCES

1. Bryan Sullivan, Malicious Code Injection: It's Not Just For SQL Anymore, [Http://Searchsoftwarequality.Techtarget.Com/Tip/Malicious-Code-Injection-Its-Not-Just-For-Sqlanymore](http://Searchsoftwarequality.Techtarget.Com/Tip/Malicious-Code-Injection-Its-Not-Just-For-Sqlanymore)
2. E. S. Phalguna Krishna, E. Sandhya, M. Ganesh Karthik, Managing Ddos Attacks On Virtual Machines By Segregated Policy Management, Global Journal Of Computer Science And Technology: E Network, Web & Security Volume 14 Issue 6 Version 1.0 the Year 2014.
3. Errol A Blake, Victor A. Clancy, Virtualization, Is It Worth It? A Technical, Financial And Economised' Approach, Published In Future Information Technology, 2010 5th International Conference.
4. Gartner Executive Program Survey, STAMFORD, Conn., January 16, 2013, [Http://Www.Gartner.Com/Newsroom/Id/2304615](http://Www.Gartner.Com/Newsroom/Id/2304615)
5. Guidelines For Performing Systematic Literature Reviews In Software Engineering [Http://Www.Elsevier.Com/_Data/Promis_Misc/525444systematicreviewsguide.Pdf](http://Www.Elsevier.Com/_Data/Promis_Misc/525444systematicreviewsguide.Pdf)

6. Heradon Douglas And Christian Gehrman, Secure Virtualization And Multicore Platforms Stateof- The-Art Report, SICS Technical Report, T2009:14A, ISSN: 1100-3154.
7. Hsin-Yi Tsai, Threat As A Service? Virtualization's Impact On Cloud Security, Issue No.01 - January/February (2012 Vol.14), Pp: 32-37, Published By The IEEE Computer Society.
8. IOANNIS CHATZIKYRIAKIDIS, Trends, And Risks In Virtualization, Master Thesis, Kingston University Of London.
9. James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H.Spafford, Security Models For WEB Based Applications, February 2001/Vol. 44, No. 2 COMMUNICATIONS OF THE ACM.
10. Karim Benzidane, Sad Khoudali, Abderrahim Sekkaki, Secured Architecture For Inter- VM Traffic In A Cloud Environment, Cloud Computing And Communications (Latincloud), 2nd IEEE Latin American Conference, Pages 23-28, December 2013
11. Kitchenham B, Charters S. (2007) Guidelines For Performing Systematic Literature Reviews In Software Engineering, Keele University And Durham University Joint Report.
12. Kurt Fanning And David M. Cannon, Virtualization: What Are The Security Risks, Volume 22, Issue 5, Pages 41–44, The Journal Of Corporate Accounting & Finance / July/August 2011
13. Lee Garber, The Challenges Of Securing The Virtualized Environment, Computer, Volume.45- No. 1, Pp. 17-20 January 2012,
14. Lena Almutair, Soha Zaghoul, A NEW VIRTUALIZATION-BASED SECURITY ARCHITECTURE IN A Cloud Computing Environment, The Third International Conference On Digital Information Processing And (Communications (ICDIPC2013)
15. Patra. Nikitasha, SAHOO.JYOTIPRAKASH, MAHAPATRA .SUBASISH, PATI .SARADA PRASANNA, Security Framework For Virtualization Based Computing Environment, International Journal Of Engineering Science And Technology (IJEST), Vol. 3 No. 8 August 2011
16. Peter Mell, Timothy Grance, The NIST Definition Of Cloud Computing, Special Publication 800 -145
17. Pooja Kedia, Renuka Nagpal And Tejinder Pal Singh, Survey On Virtualization Service Providers, Security Issues, Tools And Future Trends, International Journal Of Computer Applications (0975 –8887), Volume 69– No.24, May 2013.

18. Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Virtualization Security For Cloud Computing Service, Cloud And Service Computing (CSC), 2011 International Conference On, P. 174 – 179, Publisher: IEEE
19. Shing-Han Li, David C. Yen, Shih-Chih Chenc, Effects Of Virtualization On Information Security, Computer Standards & Interfaces, Volume 42, November 2015, Pages 1–8.
20. Shiv Raj Singh, Virtualization And Information Security A Virtualized DMZ Design Consideration Using Vmware Esxi 4.1, Master Thesis, Unitec Institute Of Technology, New Zealand, 2012.
21. Sina Manavi, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah, Secure Model For Virtualization Layer In Cloud Infrastructure, International Journal Of Cyber- Security And Digital Forensics (IJCSDF) 1(1): 32-40
22. S. Subashini, V. Kavitha, A Survey On Security Issues In Service Delivery Models Of Cloud Computing, Journal Of Network And Computer Applications (2010), Doi:10.1016/J.Inca.2010.07.006.
23. Tal Garfinkel And Mendel Rosenblum. When Virtual Is Harder Than Real: Security Challenges In Virtual Machine Based Computing Environments. Proceedings Of The 10th Workshop On Hot Topics In Operating Systems (Hotos-X), 2005
24. U. Gurav, R. Shaikh, Virtualization: A Key Feature Of Cloud Computing, ICWET 10 Proceedings Of The International Conference And Workshop On Emerging Trends In Technology, Pages 227-229.
25. Xiangyang Luo, Lin Yang, Linru Ma , Shanming Chu , Hao Dai, Virtualization Security Risks And Solutions Of Cloud Computing Via Divide-Conquer Strategy, Multimedia Information Networking And Security (MINES), 2011 Third International Conference. Page(S):637 – 641, Publisher: IEEE
26. Xun Yi Ren, Yang Yu, Selinux-Based Secure Server Virtualization, Advanced Materials Research Vols. 756-759 (2013) Pp 2829-2833 - Trans Tech Publications
27. Yasir Shoaib, Olivia Das, Pouring Cloud Virtualization Security Inside Out, [Http://Arxiv.Org/Abs/1411.3771](http://Arxiv.Org/Abs/1411.3771)
28. Alameri I, Radchenko G (2017) Development Of Student Information Management System Based On Cloud Computing Platform. Journal Of Applied Computer Science & Mathematics 11:9–29. <https://doi.org/10.4316/JACSM.201702001>
29. Sosinsky B (2011) Cloud Computing Bible. <https://doi.org/10.1145/358438.349303>

30. .Zhu G, Yin Y, Cai R, Li K (2017) Detecting Virtualization Specific Vulnerabilities In Cloud Computing Environment. In: IEEE International Conference On Cloud Computing, CLOUD2017-June, Pp 743–48
31. Pearce M, Zeadally S, Hunt R (2013) Virtualization: Issues, Security Threats, And Solutions. *Acmcomputsurv*45(2):17:117:39.<https://doi.org/10.1145/2431211.2431216>
32. Asad S, Fatima M, Saeed A, Raza I (2017) Multilevel Classification Of Security Concerns In Cloud Computing. *Appl Comput Inf*13(1):57–65.<https://doi.org/10.1016/j.aci.2016.03.001>
33. Granneman (2012) Virtualization Vulnerabilities & Virtualization Security Threats.<https://searchcloudsecurity.techtarget.com/Tip/Virtualization-Vulnerabilities-And-Virtualization-Security-Threats>
34. Sempolinski P, Thain D (2010) A Comparison And Critique Of eucalyptus, Opennebula And Nimbus.<https://doi.org/10.1109/Cloudcom.2010.42>
35. Nagar N, Suman U (2016) Analyzing Virtualization Vulnerabilities And Design A Secure Cloud Environment To Prevent From Xssattack. *Int J Cloud Appl Comput* 6(1):114.<https://doi.org/10.4018/IJCAC.2016010101>
36. Kaur A, Gupta G, Bhathal GS (2017) Role Of Virtualization In Cloud Computing. *Global J Eng Sci Res* 4(7):143–150.<https://doi.org/10.5281/zenodo.835421>
37. Wu J, Lei Z, Chen S, Shen W (2017) An Access Control Model For Preventing Virtual Machine Escape Attack. *Future Int* 9:2.<https://doi.org/10.3390/fi9020020>
38. Zhang Y, Juels A, Oprea A, Reiter M (2011) Home Alone: Co-Residency Detection In The Cloud Via Side-Channel Analysis. In: IEEE Symposium On Security And Privacy (Oakland), Oakland, CA, Pp 313–328.<https://doi.org/10.1109/SP.2011.31>
39. Wojtkowiak A (2012) Protection For Virtual Environments? IBM Virtual Server Protection. IBM Corporation
40. Gupta S, Kumar P (2013) Taxonomy Of Cloud Security. *Int J Comput Sci Eng Appl* 3(5):47–67.<https://doi.org/10.5121/ijcsea.2013.3505>



Kirandeep Kaur is a creative woman filled with initiative and drive and who always ready to help others.



PO Box 823, SE-301 18 Halmstad
Phone: +35 46 16 71 00
E-mail: registrator@hh.se
www.hh.se