Impact of VM based Side Channel Attack on DEPSKY Multi Cloud Model

By

Haider Ali Khan Khattak

A thesis submitted to the faculty of Department of Information Security, MilitaryCollege of Signals, National University of Sciences & Technology, Islamabad, Pakistan,in partial fulfillment of the requirements for the degree of MS in Information Security

February, 2017

Impact of VM based Side Channel Attack on DEPSKY Multi Cloud Model

Author

Haider Ali Khan Khattak

A thesis submitted in partial fulfillment of the requirements for the degree of MS Information Security

Thesis Supervisor

Col Imran Rashid, PhD

DEPARTMENT OF INFORMATION SECURITY

MILITARY COLLEGE OF SIGNALS

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY ISLAMABAD

February, 2017

Declaration

I hereby certify that I have developed this thesis titled as "Impact of VM based Side Channel Attack on DEPSKY Multi Cloud Model" wholly and solely on the basis of my personal efforts under the earnest toil and sincere guidance of my supervisor Col Imran Rashid. All the sources used in this thesis have been cited and contents of the work have not been plagiarized. Any section of the presented work has not been submitted for the degree of qualification to any other university.

Signature of Student

Haider Ali Khan Khattak

NUST201362705MMCS2521F

Language Correctness Certificate

This thesis has been read by an English expert and is free of typing, syntax, semantic, grammatical and spelling mistakes. Thesis is according to the format given by the university.

Signature of Student

Haider Ali Khan Khattak

Copyright Statement

Acknowledgments

"In the name of Allah, the most Merciful, the most Compassionate"

First and above all, I praise Allah, the almighty for providing me this opportunity and granting me the capability to proceed successfully. I would like to express my cordial gratitude to my supervisor Col Dr Imran Rashid and my co-supervisor Dr. Haider Abbass for their extensive guidance, motivation, immense knowledge and enthusiasm. Their valuable help of constructive suggestions and feedbacks through the thesis work have contributed to the success of this research. I acknowledge the contributions of Dr. Haider Abbass as spectacular for always quickly responding to my queries, and contributing constructive comments on each publication. I would also like to thanks the rest of my thesis committee members: Waleed Bin Shahid and Waseem Iqbal for their encouragement, help and thoughtful comments. I would like to thanks Ayesha Naeem who always provide me moral support and always willing to give her best suggestion.

I would like to thanks my colleagues Faisal Iqbal Jan, Muhammad Faisal, Umer Bin Saeed and Yasir Hameed who always encourage me during my research work. In the end, my deepest gratitude goes to my cherished parents. My parents have been the greatest investor in my career.

I would like to share the deep gratitude to my adored brothers Major. Awais Khattak, Waqas Khattak, Ilyas Khattak and Saad Khattak for their love and sheer support. My sincere thanks and prayer to go with my nephews Hassan Bin Awais, Hussnain Bin Awais, Muhammad Ibrahim Bin Waqas and Nieces Saweera Binte Awais and Maryam Binte Ilyas who brings such a delight and colors to our lives. I warmly thank my best friend Capt. Saad Sultan who made available his support in a number of ways and always refresh my mind with his thoughtful philosophies.

Dedication

"To my Dearest and Beloved Parents"

Abstract

The innovative model of cloud computing has been under keen observation by many organizational sectors like healthcare, financial, Telco's, private and government, realizing the benefits that can be achieved in terms of productivity, low cost, data accessibility and on demand services to its users. Like other services provided by cloud service provider, storage services has lead the organizations to store their critical records on the infrastructure provided as per their needs. DEPSKY a "multi-cloud deployment model" is a system, which ensures confidentiality, integrity, efficiency and availability of data by replicating them on different clouds that form an "inter-cloud" or "cloud-of-clouds". In this research we focus on one of the attack in multi cloud deployment model, that is VM based Side Channel Attack in which a rouge/malevolent VM occupies the read/write operations most of the time thus limiting the legitimate VM's to perform read/write operations for a very minimal amount of time. In VM based side channel attack, the aim of the attacker is to extract most of the data on the rouge VM by occupying the read/write operations for maximum time. In this attack, the goal of the attacker is to maximize the time of read/write operations on rouge VM and minimizing the amount of time for legitimate VM's to perform read/write operations. We try to analyze the impact on performance of DEPSKY multi cloud model by the presence of VM based Side Channel Attack.

Keywords: Cloud Computing, Security, DEPSKY Model, VMbSC Attack

Contents

List of Figures

List of Tables

1 Introduction

1.1 Introduction

Cloud Computing (CC) is a novel and state of the art technology for organizational sectors like financial, Telco's, healthcare, private and government, due to realization of benefits it provides in terms of on demand services to the users, accessibility of data, low costing, storage and high productivity. Single cloud deployment model has many limitations due to the unaddressed security gaps such as Single Point of Failure (SPoF), Denial of Service (DoS), Distributed Denial of Service (DDoS) etc. From this notion of security, a Multi Cloud Computing (MCC) model has emerged which addresses the security gaps more effectively. MCC architecture is formed by increasing the number of Cloud Service Provider (CSP) involved and increasing the computing resources on the virtualization layer function using virtual entities. The objective of MCC is to provide high computing resources to its end user's, for ensuring operational efficiency and effectiveness of services. There are many threats posed to MCC due to its functionality of rapid elasticity, as resources are allocated to the end user's and can be manipulated by malicious attacker. We disclosed one of the weaknesses in operational aspects of MCC that can be exploited by malicious entities. The attack we discuss in this research is Virtual Machine based Side Channel (VMbSC) attack in which a vulnerable Virtual Machine (VM) occupies the read/write operations most of the time, thus limiting the legitimate VMs to perform read/write operations for a very minimal amount of time. We try to explore this VMbSC attack in MCC which is affecting the performance of virtual entities. In this research we try to analyze the behavior of this VMbSC attack on virtual layer which shows a critical role in the effective operational performance of MCC. The model we use for the analysis of is DEPSKY multi cloud model. In DEPSKY multi cloud model, the end user's data is replicated on different clouds forming an "inter – cloud" or "cloud – of – clouds". When an end user request's for write operation, data is copied on all the clouds and a metadata (i.e. information about the data) is stored along with the data on each cloud. During the read operation, when the end user request's for read operation, the metadata is accessed from all the clouds and if required data exist in metadata then complete data is fetched at the user's end for operational processing. VMbSC attack degrades the performance of MCC, as legitimate VMs are not able to utilize the resources and bandwidth effectively as predicted in normal operations of MCC.

1.2 Cloud Computing

CC has changed the era of computing through its emergence and caused a rebellion in our lives with its innovation. CC states that computing is delivered as a provisioning of services from CSP rather than a byproduct as a utility for its end users [4, 5]. CC forms a network which creates a possibility to attain a common arsenal of configurable resources (i.e. servers, storage, networks etc.) and on demand network access to its end users by the CSP [6]. CC technology has formed dependence in our daily life that people cannot even imagine to live without it. In a report published by Gartner, it is assumed that CC will capture the market by 180 billion USD in 2015 and will influence to lodge most of the investments of IT in 2016 [7]. Most interesting and eye-catching point of CC is that, it follows pay-as-you-go model, for the provisioning of resources to its end users which means cloud resources are allocated and provisioned according to the needs and requirements of the stakeholder without thwarting additional or large amount of investments in purchasing the infrastructure [8]. Some common and most benign examples of CC are podiums such as Google Drive, Drop Box, Office 365, Yahoo mail and iCloud. Cloud computing services are shown in Figure 1.1

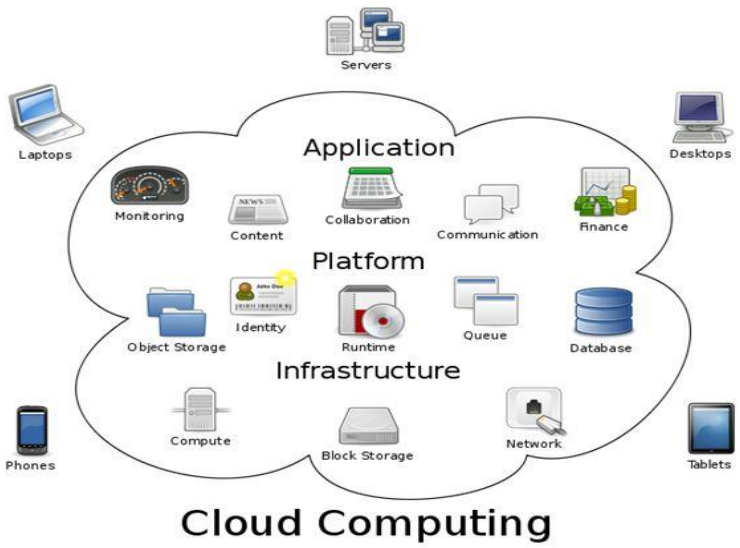

Figure 1.1: Cloud Computing Services [1]

In spite of the fact that, with the increase in demand of CC, the security requirements from end users and threat landscape that poses risks to CC technology is also on rise [9]. In an analysis of Cloud Computing Services completed by IDC IT group in 2009 highlighted that, an over 87% result considered security to be a dead-lock towards

the acceptance of CC and is making organizations to remain hesitant towards the prospect of implementation of cloud solution at enterprise level [10].

1.3 Multi Cloud Adoption Over Single Cloud

Adoption of CC is also dependent on the aspect of it deployment model (i.e. single or multi cloud). Single Cloud (SC) deployment model states that one CSP is providing services and resources to multiple end users, which is not considered to be a feasible option by end users, as SC is more vulnerable to modern threat landscape. In contrast Multi Cloud (MC) deployment model has attained more focus, as it more reliable and secure than SC. In MC, multiple CSPs are providing services and resources to multiple end users, thus eliminating the risks in MC and reduce the attack surface of CC [1]. A comparative analysis by RightScale 2016 State of the Cloud Report is shown in Figure 1.2, depicting the adoption of MC over SC in the year 2015 and 2016 [2].

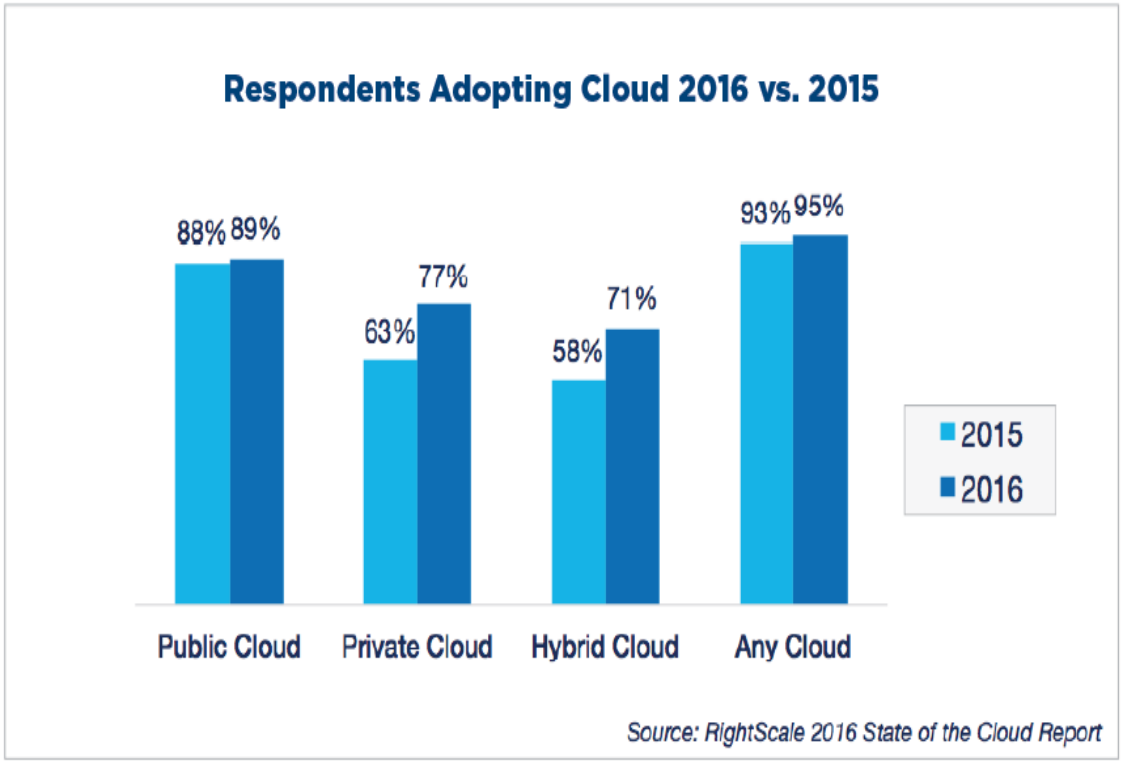

Figure 1.2: Respondents Adopting Cloud 2016 vs. 2015 [2].

Figure 1.2 illustrates that in 2016, a resilient progression towards MC (i.e. Hybrid cloud) is observed as end users have added private cloud resource pools with their

public cloud. This indicates that 63% of the respondents in 2015 have been raised up to 77% in 2016 towards adoption of private cloud. As a result, the usage of MC has been raised up from 58% in 2015 to 71% in 2016. In total, 93% of respondents towards adoption of CC in 2015 have been raised up to 95% in 2016 [2]..

1.4 VM based Side Channel Attack

The special characteristics and virtualized setup of CC provides critical opportunities to the attackers, which generates new attacks focusing to damage the normal operations of the CC. In CC, virtualization is considered to be the primary defense mechanism, but it also opens up the secret pass for the malicious users to exploit the vulnerabilities of virtualized environments. In Virtual Machine based Side Channel Attack (VMbSCA), malicious Virtual Machine (VM) is replicated along with the legitimate VM's with the same characteristics as legitimate VM's, so that the Virtual Machine Manager (VMM) believe attacker as a legitimate and thus allocate the operations to malicious VM [3]. Figure 1.3 illustrates the VMbSCA attack model.

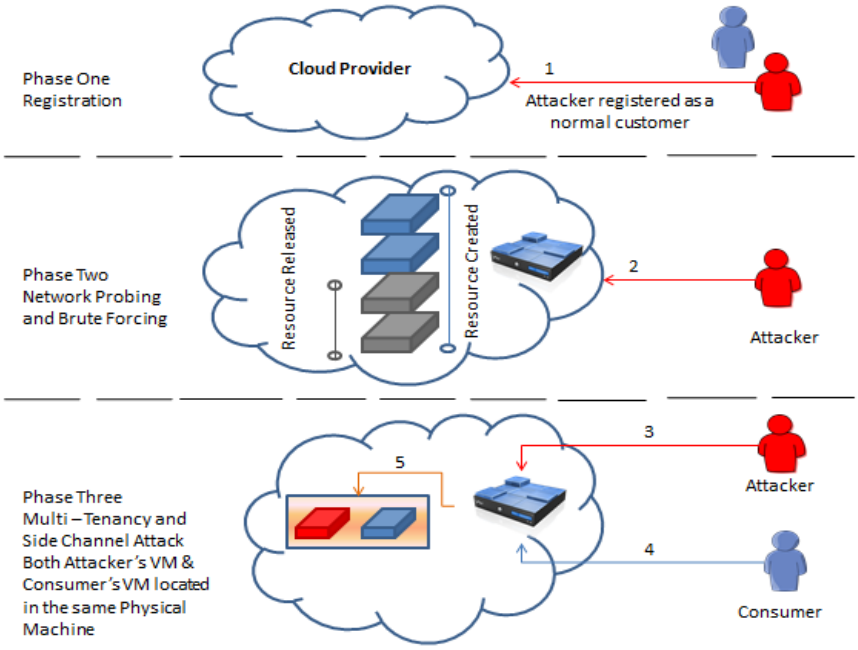

Figure 1.3: Illustration of VMbSC Attack Model [3]

VMbSCA affect the efficiency of resource utilization of CC model by generating serious interference to legitimate VMs to perform their allocated operations. VMbSCA has three motivations as mentioned below:

- **DoS Attack:** The attacker tries to launch VMbSCA by creating a channel of transmit only, which can be utilized further to launch a DoS attack by sending multiple connection requests.
- **Eavesdropping Attack:** The attacker tries to launch VMbSCA by creating a channel of receive only, which can be utilized further to launch Eavesdropping attack for extraction or theft of crypto key.
- **Man in the Middle Attack:** The attacker tries to launch VMbSCA by creating a bi-way channel, which can be utilized further to launch Man in the Middle Attack (MitMA) for exfiltration or gaining access to the information being transferred or received.

1.5 Objectives of this Thesis

MCC performance is highly dependent number of factors and one of the most critical one is Virtual entities. The performance of DESPSKY MCC model is related to read and write operations that need to be performed on virtual machines in multiple CSPs environment. Hence, the estimation of operational performance analysis to complete the read or write operations plays an important role in DEPSKY MCC model. The VMbSC attack affects the DEPSKY multi cloud model, as malicious VM tries to occupy the read or write operations most of the time by consuming the resources at highest priority and preventing legitimate VMs to access the read or write operations. In this research our aim is to provide the analysis of VM based Side Channel attack on the performance of DEPSKY multi cloud model.

1.6 Contributions

Following are the aims of this research:

1. Generation of DEPSKY multi cloud model.
2. Performance analysis of DEPSKY multi cloud model before launching attack.
3. Launch VM based Side Channel Attack.
4. Analyze the performance of DEPSKY multi cloud model after launching VM based Side Channel attack.
5. Generation of Results.

1.7 Overview of the Thesis

Chapter 1 explains the basic introduction of Cloud Computing, Multi Cloud Computing and the VMbSC attack. It also encompasses the objectives and contribution of thesis. Chapter 2 focuses on the motivation, cloud preliminary, architecture and applications of CC. Chapter 3 describes the CC diversified deployment models. Chapter 4 explains the security threats of CC. This chapter focuses on VMbSC attack, and its detection and prevention techniques. Chapter 5 includes the simulation of Single cloud and DEPSKY multi-cloud model, VMbSC attack and the performance of VMbSC attack on DEPSKY multi-cloud model. Finally, Chapter 6 concludes the thesis with relevant areas to be further investigated.

2 Cloud Computing

2.1 Motivation of CC

Due to the emerging cloud based applications and requirement for analyzing enormous amount of data, there is a prerequisite of having increased demand for computing resources. Formerly, organization's used to spend heavy investments on procurement of Information Technology (IT) infrastructure in order to start their business operations, and it led towards inadequate prospects for Small and Medium Enterprises (SME) to compete with the large scale organizations due to budgeting reasons. With the advent of Cloud computing, it provided an equal opportunity for the large scale organizations and SME to start off their business operations on Cloud Service Provider (CSP) infrastructure [2]. The vision of CC is to provide computing resources with reduced cost, increased flexibility and reliability by transmuting physical computers into virtual entities hosted in CSP infrastructure.

2.2 Preliminary: CC in a Nutshell

Considering an electric appliance connected to the socket, we haven't noticed how electricity is generated and provisioned to the appliance; this is mainly due to the reason that electricity is virtualized and is it is readily available to the appliance from wall socket hiding the distribution grid and electricity generation stations. Same concept is applied when considering Information Technology (IT) by distributing useful functionality and hiding how the internal core operates [11]. The definition of CC and its unique characteristics have been consolidated and presented by many experts. According to Armbrust et al. [7] cloud is defined as "software and hardware hosted in CSP data center is provisioned to CSC". "Cloud is a parallel and disseminated computing resources which consists of inter-connected virtual entities that are vigorously provisioned and offered as one or more cohesive computing resources as per the Service Level Agreement (SLA) between Cloud Service Provider (CSP) and Cloud Service Consumer (CSC)", as per definition of Buyya et al. [12]. Vaquero et al. [13] has stated that "CC is a large pool of virtualized resources (such as hardware platform and software platform) having the potential of vigorous scaling according

to the pay – per – use model for optimizing resource utilization". Conferring to National Institute of Standards and Technology (NIST), CC is characterized as "pay – per – use model for convenient, available, on demand network provisioning to a pool of configurable computing resources (such as servers, networks, applications, storage, services), which can be provisioned briskly with minimal or interaction from service provider" [6].

Figure 2.1 illustrates, the technological shift observed in past few decades from terminal mainframe applications towards the cloud enabled applications. This advancement depicts that; virtualization has played an eye catching point for the enterprises in adoption towards CC. Organization are keener towards the managed services platform, as it provides them opportunity to start off their operational services without investing heavy costs for purchasing the IT infrastructure.

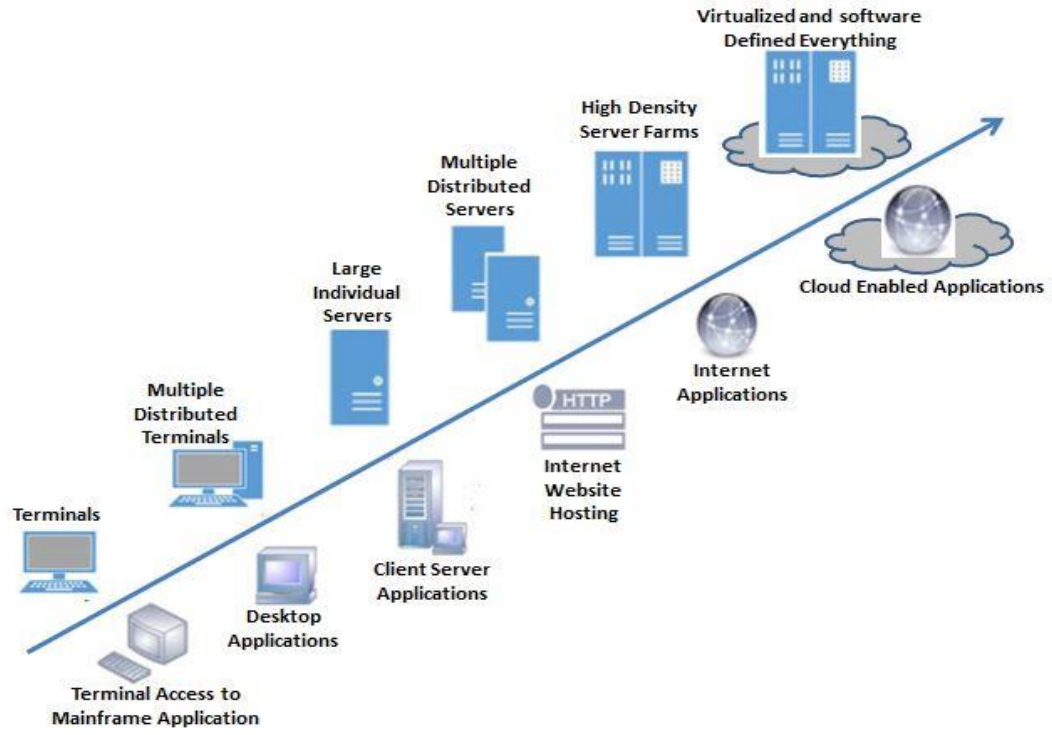

Figure 2.1: Illustration of Technological Shift towards CC

CC emerged as a consequence of combination of multiple technologies, especially in terms of distributed computing (grids, clusters), hardware (multi – core chips, virtualization), system management (automation of data center, autonomic computing) and internet technologies (service – oriented architectures, web 2.0, web services). Emergence of CC itself is closely coupled with the maturity of these technologies [14]. Figure 2.2 illustrates the convergence of technology fields that considerably pivoted towards the advancement in CC.

2.3 Architecture of CC

CC architecture is composed of software applications which utilize on-demand provisioning of services over the internet. CC architecture is essentially dependent on infrastructure, which is utilized when there is a request raised from end user to process a specific job that requires drawing necessary resources. Once the job is complete, the unused resources are released and allocated to another user if required. It is based on pay – as – you - go mockup model, which means end users are charged for the utilized resources only. This approach leads to an effective utilization of computing resources in terms of productivity, cost and maintenance [15].

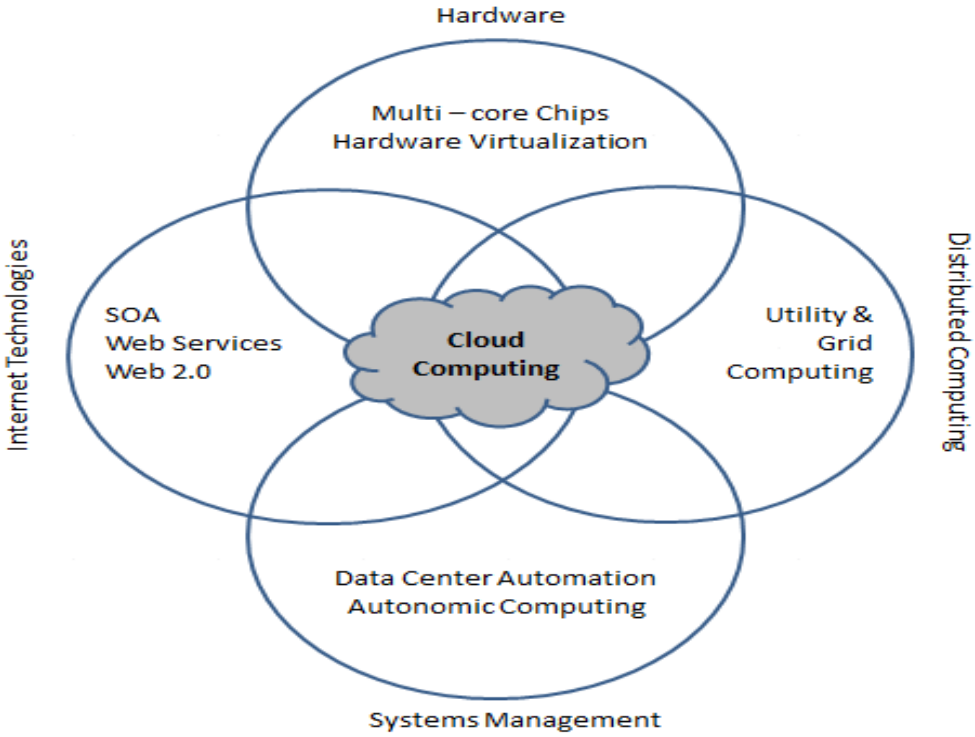

Figure 2.2: Convergence of Various Advances that Pivoted Towards the Encroachment of CC

2.3.1 General Architecture of CC

Figure 2.3 represents the general architecture of cloud computing, in which front end represents the end users and back end represents the cloud platform on which the hosted services are provided to end users through internet connection by Cloud

Service Provider (CSP). Cloud platform consists of physical servers, virtual machines software platforms, applications and storage services for end users.

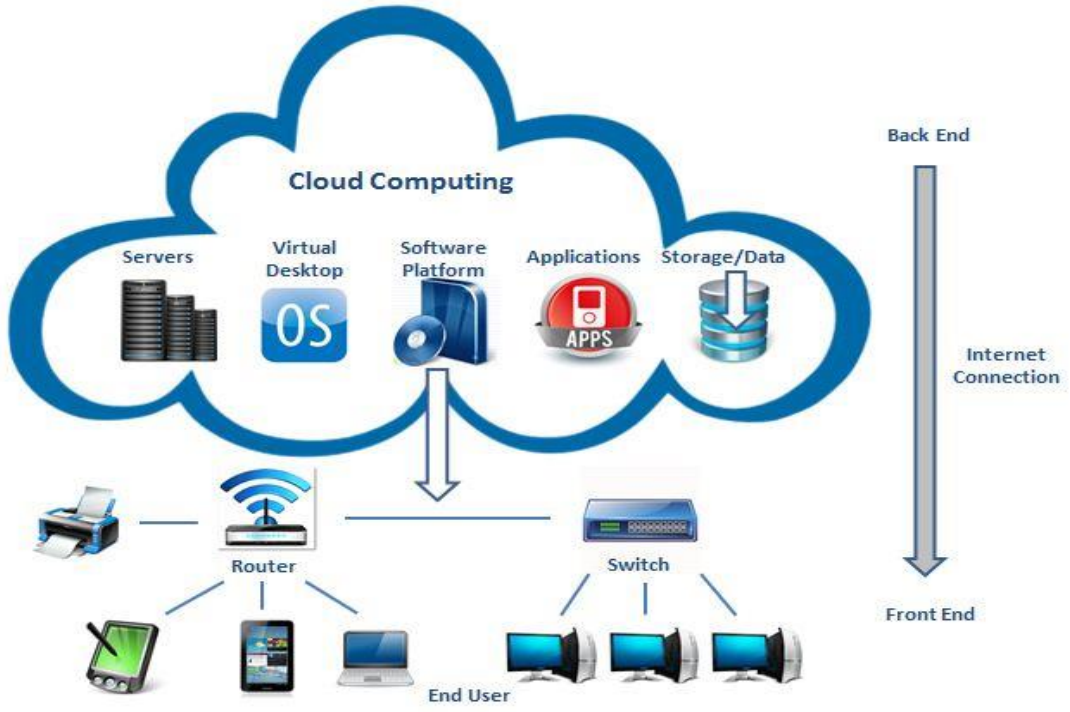

Figure 2.3: CC General Architecture

2.3.2 Layered Architecture of CC

Figure 2.4 illustrates the layered architecture of cloud computing, which encompasses 4 layers; application layer, platform layer, infrastructure layer and the hardware layer [16].

Each layer is discussed in detail:

- Application Layer: Top most layer is the application layer which is composed of cloud applications. Cloud applications have the feature of automatic scaling in order to achieve low operating cost, improved performance and availability in contrast to the traditional applications.
- Platform Layer: Platform layer is composed of application frameworks and operating systems; it is built on the top of infrastructure layer. Purpose of this layer is providing opportunities for reducing the load of application deployment into the Virtual Machine (VM) container directly.

- Infrastructure Layer: Infrastructure layer is also considered as the virtualization layer because physical resources are partitioned into a pool of computing and storage services. Partitioning of resources is done through virtualization technologies VMware [17], KVM [16] and XEN [16].
- Hardware Layer: Hardware is executed in datacenters, as it is composed of the physical resources which include power, router, switches, cooling systems and physical servers. These physical resources are then utilized in infrastructure layer for creating partition of virtual entities.

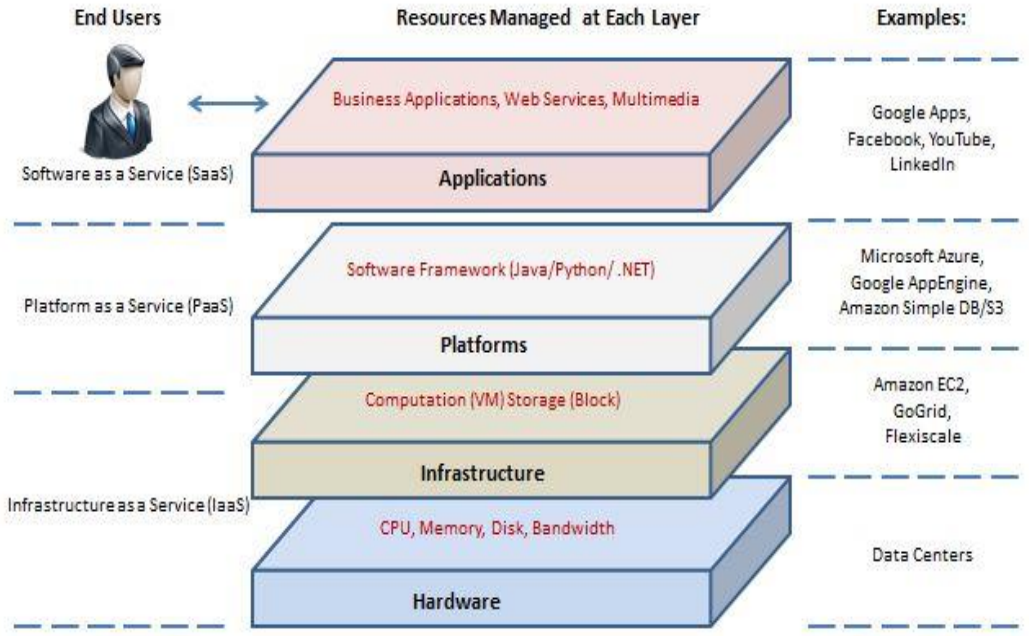

Figure 2.4: CC Layered Architecture

2.3.3 Cloud Service Models

CC services consist of different categories such as application, platform and infrastructure. These services are mainly Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [15]. Table 2.1 illustrates the cloud service models, description and examples.

Figure 2.5 illustrates the segregation of responsibilities between CSP and client side i.e. end user while opting the cloud service model. Formerly, in a traditional IT

Service Model	Description	Example	Reference
SaaS	Software as a Service model refers to providing on – demand applications to its user over the internet.	Rackspace SAP Business ByDesign	[18]
PaaS	Platform as a Service model refers to providing support related to software development frameworks and computing resources.	Microsoft Windows Azure Google App Engine	[19][20]
IaaS	Infrastructure as a Service model refers to providing the infrastructural level resources such as storage and virtual entities.	GoGrid Amazon EC2	[21]

Table 2.1: Service Models of CC, description and their examples

infrastructure environment every entity of IT infrastructure needed to be managed by the end user, as it was in – house established and retained. With the advancement of cloud concept, it provided an ease for the end user while migrating towards the managed services platform because it shared the responsibilities of end user with CSP

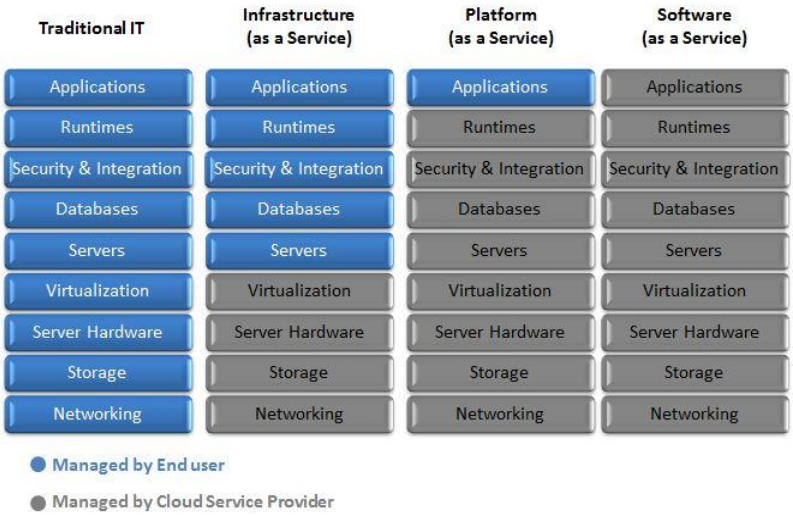

Figure 2.5: Segregation of responsibilities between CSP and End User

Cloud computing has shifted the control from end user to CSP, through the provisioning of cloud service models. In IaaS model, from networking segment to virtualization segment, it is being managed by the CSP and above all layers i.e. from servers to applications it is being managed by end user itself. While if PaaS model opted then, from networking segment to runtimes of services it is being managed

by CSP and end user has to manage only the application and the data being used by these application. Whereas in SaaS model, end user has no responsibilities and everything is being managed by the CSP itself, end user has just to start off their business operations.

2.4 Applications of CC

Area	Aim	Reference
Emergency and Public Safety	To handle crisis and precarious situations via cloud based disaster management systems	[22]
Internet of Things (IoT)	Providing a reliable and affordable cloud based IoT by integrating IoT and cloud computing forming a CloudThings architecture	[23]
Smart Grid	Cloud computing model for smart grid applications and big data	[24]
E – Learning	Cloud based E – Learning services for educational sector	[25]
Military	Cloud based system for military mission planning support and training exercises for soldiers to deal with threat situations	[26]
Wireless Sensor Networks	Cloud based wireless sensor networks to address the challenges related to memory, energy, communication, computation and scalability	[27]
Healthcare Service	Cloud based healthcare service for real time monitoring of user medical record for protracted diseases	[28]
Cognitive Radio Networks	Cognitive Wireless Clouds (CWC) for effective spectrum access, network optimization, cross network signaling and reconfiguration methods	[29]
Vehicular communication	Vehicular Cloud Computing (VCC) for Intelligent Transport System (ITS)	[30]

Table 2.2: Applications of CC and their aim

CC delivers a utility for its end users by providing pool of resources (e.g. computational power, storage, software platform etc.), which has led towards its adoption due to the vast range of services and application available. Such applications include vehicular communication, cloud robotics, mobile cloud computing, cognitive radio networks, healthcare service, wireless sensor networks, military applications, emergency and public safety applications, smart grid, e – learning and Internet of Things (IoT). Table 2.2 illustrates the applications of CC and aims.

3 CC Deployment Models

In CC there exist different deployment models, each having its own benefits and utility that can be achieved through its deployment but there are limitations observed in them as well. Moving an enterprise application in to the cloud environment can be very cumbersome, for example CSP have their own set of requirements some focus on security and high reliability while others on lowering the operating cost for end users. Mainly CC is divided into two main streams of deployment i.e. single cloud deployment model and multi cloud deployment model. Figure 3.1 illustrates the division of cloud deployment models.

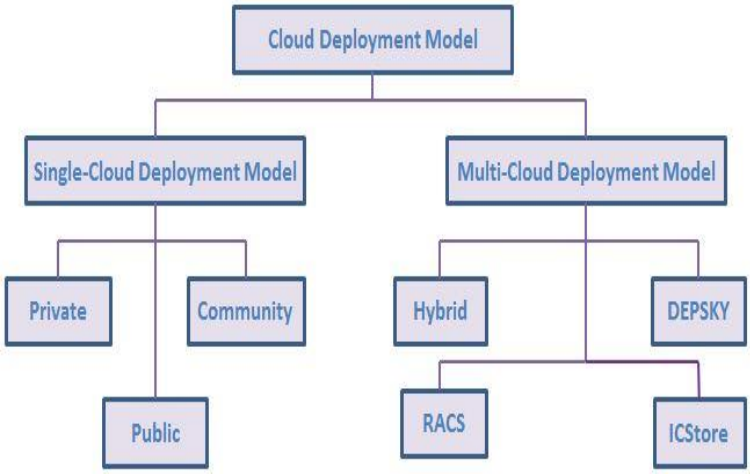

Figure 3.1: Division of CC Deployment Models

3.1 Single Cloud Deployment Model

Single cloud Deployment Model consists of three types, i.e. private cloud, community cloud and public cloud. Each single cloud deployment model is discussed briefly along with its limitations discussed in literature.

3.1.1 Private Cloud

Private clouds are configured to provide services for a single organization, also known as internal clouds. Private cloud might be configured and managed by the external service provider or itself the organization. However, private cloud are far more expensive and lacks capability of effective resource utilization because all the resources are reserved for the single customer and most of the resources may be idle most of the time [16].

3.1.2 Community Cloud

In general, community refers to the individuals having same ideology, mission, interest, policy and security needs. Community cloud is a concept of cloud resources shared by different organizations having same requirements or business needs. Community cloud can be managed by third party or by any of the organization. However, it is not a best approach for cloud deployment because every organization may have common needs but they also differ from each other as well [31]. For example, consider two organizations; organization A and organization B having same business and needs, but focus of A is towards high availability and focus of B is towards low operating cost. So in this case these two organization's requirement differs from each other based on their needs and community cloud is not suitable for them to adapt. Figure 3.2, illustrates the community cloud model.

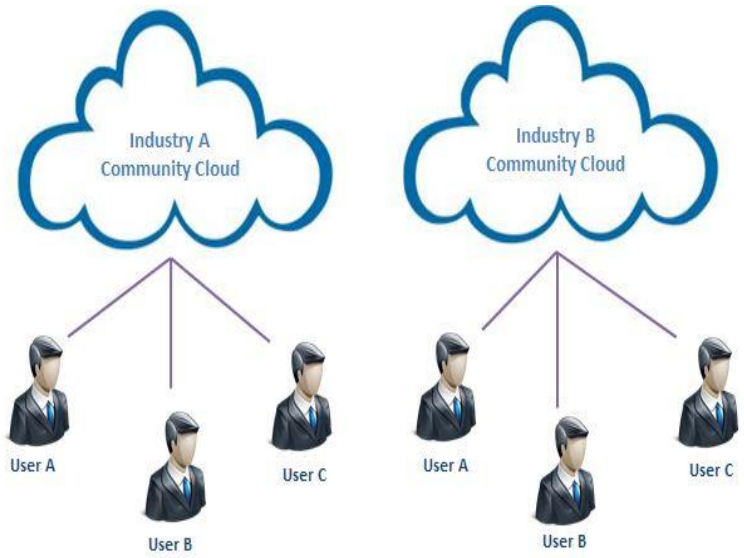

Figure 3.2: Community Cloud Model

3.1.3 Public Cloud

Term "public" refers itself as a service open for common public. In this cloud deployment model, the infrastructure is owned by the CSP and services hosted in cloud are open for public and organizations. Resources are shared among multiple end users from a common arsenal based on the requirements provided by the end user. In this model end users only pay for the services as per their intended use and needs. It requires no capital investment from the end user's perspective for acquiring infrastructure. However, in public cloud there is absence of effective controls over security settings, network and data of the end user as it is being processed on third party environment, which affects its usefulness [16]. Figure 3.3, illustrates the public cloud model.

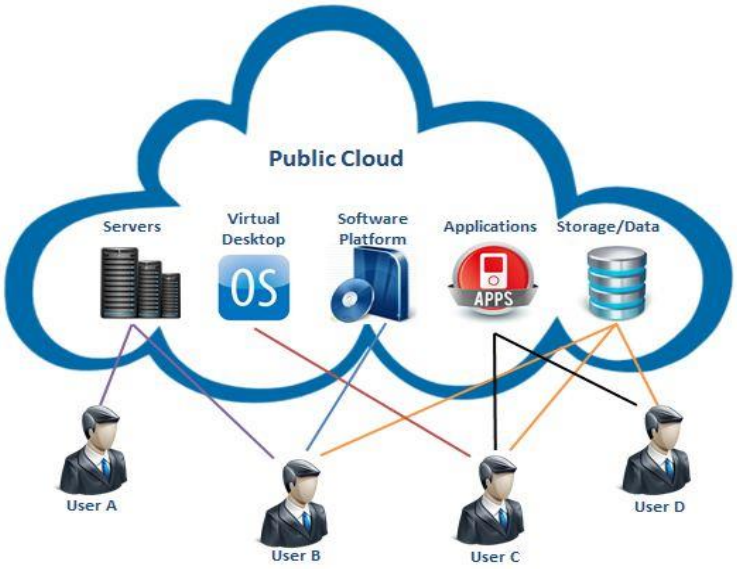

Figure 3.3: Public Cloud Model

3.2 Multi Cloud Deployment Model

There are different models that exist for deploying multi cloud environment in literature, each having its own benefits and limitations. The promising models of multi cloud deployment models include hybrid cloud, InterCloud Storage (ICStore), Redundant Array for Cloud Storage (RACS), High Availability and Integrity Layer (HAIL) and DEPSKY.

3.2.1 Hybrid Cloud

Hybrid cloud is composed of private and public cloud deployment models. This multi cloud model is proposed to overcome the limitations observed in individual deployment of either private or public cloud solely. In hybrid cloud model, the infrastructure layer services are managed and provisioned in private cloud whereas the application and platforms layer services are provisioned at public cloud. In terms of flexibility hybrid cloud model is more mature than private and public cloud because it provides adequate controls for monitoring of application relevant data with the aiding feature of increase and decrease of on-demand services. However, the limitation observed in hybrid cloud model is in its designing phase which is a very cumbersome task for identifying which layer to be included in private cloud model and public cloud model [16]. Figure 3.4, illustrates the hybrid cloud model.

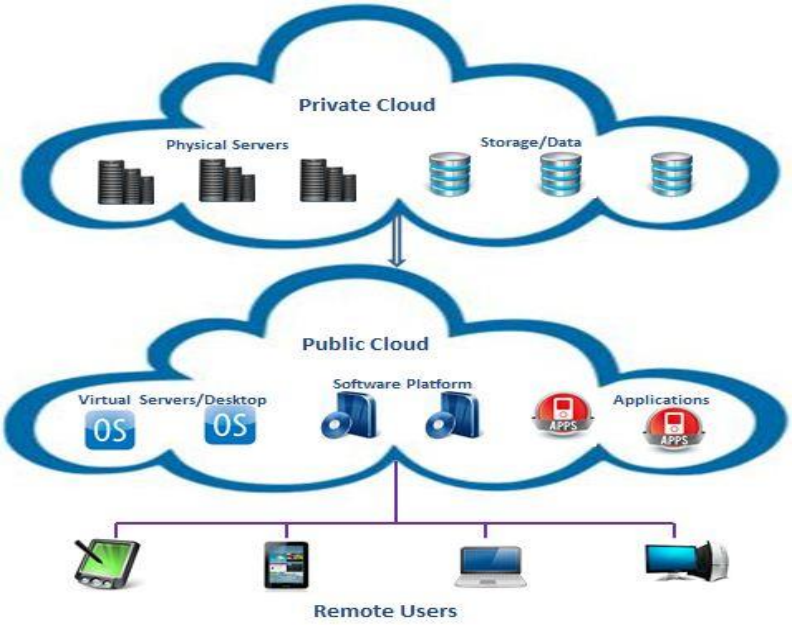

Figure 3.4: Hybrid Cloud Model

3.2.2 InterCloud Storage (ICStore)

Single domain cloud is considered to inappropriate in terms of confidentiality, integrity and customer data sanitization and isolation, because all the systems and protocols are configured to process computations in a single domain managed by one service provider. ICStore model helps to fill in the gaps observed in the single cloud domain. ICStore encourages the involvement of multiple cloud service providers by

forming an intercloud layer which exists on the top of single domain cloud layer. InterCloud layer extends the scope of single domain cloud layer, in order to form interactions among multi cloud service providers. Figure 3.5 illustrates the ICStore model.

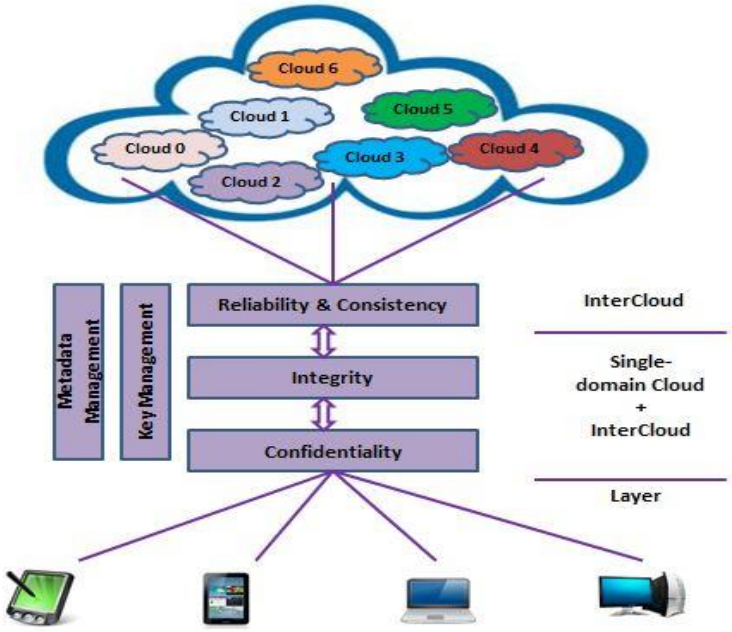

Figure 3.5: ICStore Model

ICStore is composed of three core layers i.e. Integrity, Confidentiality and Reliability & Consistency, each having its own utility. Confidentiality layer provides encryption mechanism of the data. Integrity layer provides protection against unwanted data alterations. Reliability and Consistency layer provides fault tolerant protocols which are utilized for dispersal of end user data to the intercloud, after the data is parsed through integrity and confidentiality layers [32]. However, the limitation observed in ICStore model is that it does not provide security measures against data intrusion and service availability [33].

3.2.3 Redundant Array for Cloud Storage (RACS)

A cloud storage service has increased the motivation in end users for switching data from their datacenters into the cloud storage. In single cloud domain, there is a limitation of switching cloud service providers is observed when moving into the cloud, as it is more expensive. In order to overcome this limitation Redundant Array for cloud Storage (RACS) model is proposed which works on the principle of replicating

end user data among multiple cloud service providers. It utilizes technique like Redundant Array of Inexpensive Disk (RAID), but at cloud storage level. It eliminates the possibility of single vendor lock-in issues. Figure 3.6, illustrates the single and distribute RACS proxy model.

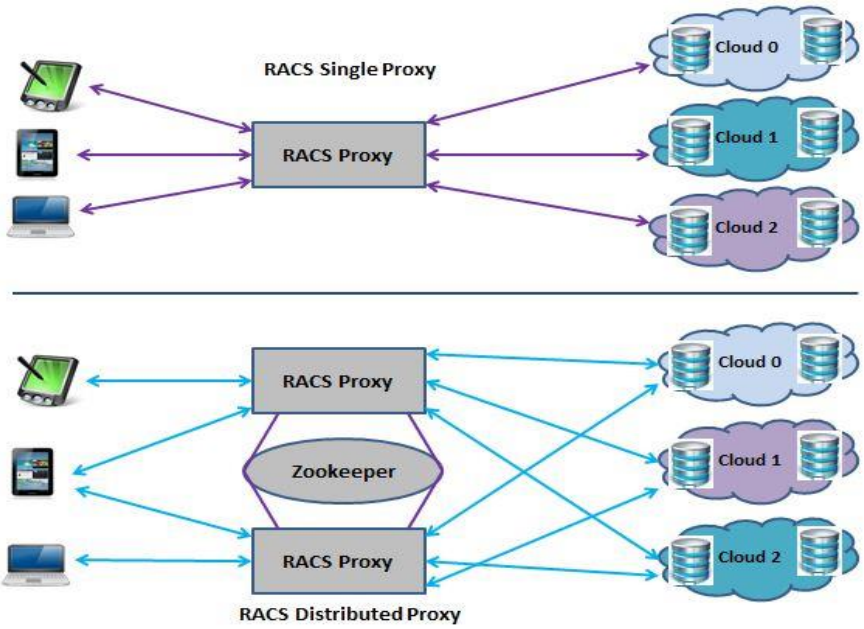

Figure 3.6: Single and Distributed RACS Proxy Model

In Single RACS Proxy Model, one RACS proxy entity is used which replicates end user data among multi cloud storage repositories; all end users read or write their data on cloud storage using single proxy. Whereas in Distributed RACS Proxy Model, there are multiple RACS Proxies that operate for stripping the data to the multi cloud storage repositories. ZooKeeper is a system which communicates and provides distributed synchronization and group services among multiple RACS proxies [34]. However, the limitation observed in RACS model is that it does not provide security measures against data integrity, intrusion and service availability [35].

3.2.4 DEPSKY Multi-Cloud System

DEPSKY system also known to be as “multi-cloud” or “Cloud of Clouds” is a virtual environment for storing end user data on different clouds. It improves the triad requirements of the data i.e. confidentiality, availability and integrity [36]. DEPSKY system utilized Byzantine Fault Tolerant mechanism to eliminate flawed performance and intrusion threshold. Byzantine fault is known to be hardware

or software related component malfunctioning. As per Byzantine Fault Tolerant mechanism, it is a necessity that every module must have diversity in terms of implementation, hardware and computational resource in order to avoid propagation of fault to other modules of the cloud [37]. Figure 3.7, illustrates the DEPSKY system model.

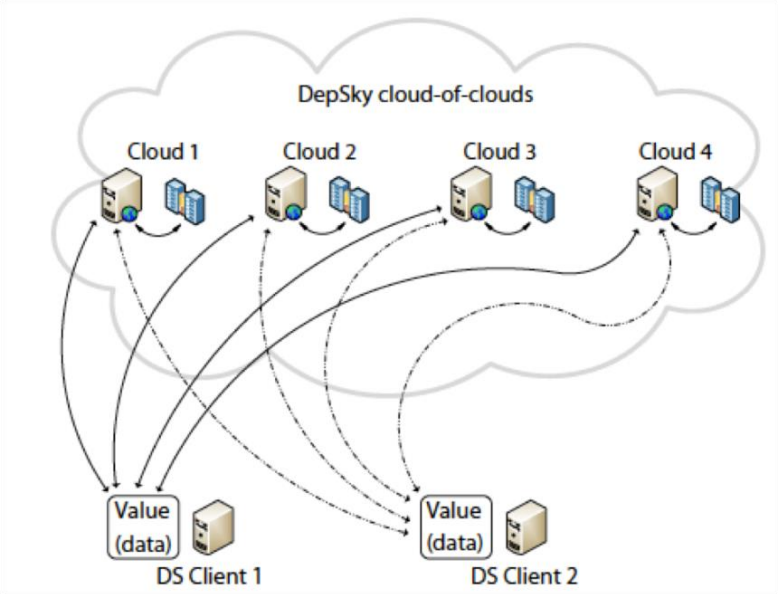

Figure 3.7: DEPSKY System Model

DEPSKY system consists of four independent clouds which communicate with end user applications. The collection of DEPSKY only allow read and write operations, no executable code run on these clouds as these are storage related only. In DEPSKY system model it consists of three domains i.e. writers, storage cloud and readers. The cloud providers have Byzantine protocols, which have storage cloud sets denoted by (n) and can be symbolized as n=3f+1, where f denotes the faulty/erroneous cloud. The data model of DEPSKY consists of three abstraction layers i.e. generic data unit, conceptual data unit and implementation of data unit [38]. Figure 3.8, illustrates the data model of DEPSKY system.

DEPSKY system has three abstraction layers. In the left most level there is "conceptual data unit", it relates to basic storage of cloud. The data unit of conceptual data unit consists of version number for supporting updates at the object level, a distinctive name (X as shown in Figure 3.7), verification number (done through cryptographic hashing of information) and the actual data of the object that is used in data unit. The second layer of abstraction is "generic data unit" which is an extended abstraction of conceptual data unit in storage of cloud; the container of generic data unit consists of a metadata and actual data. Metadata is composed of version number, other information of data and verification number and it refers to

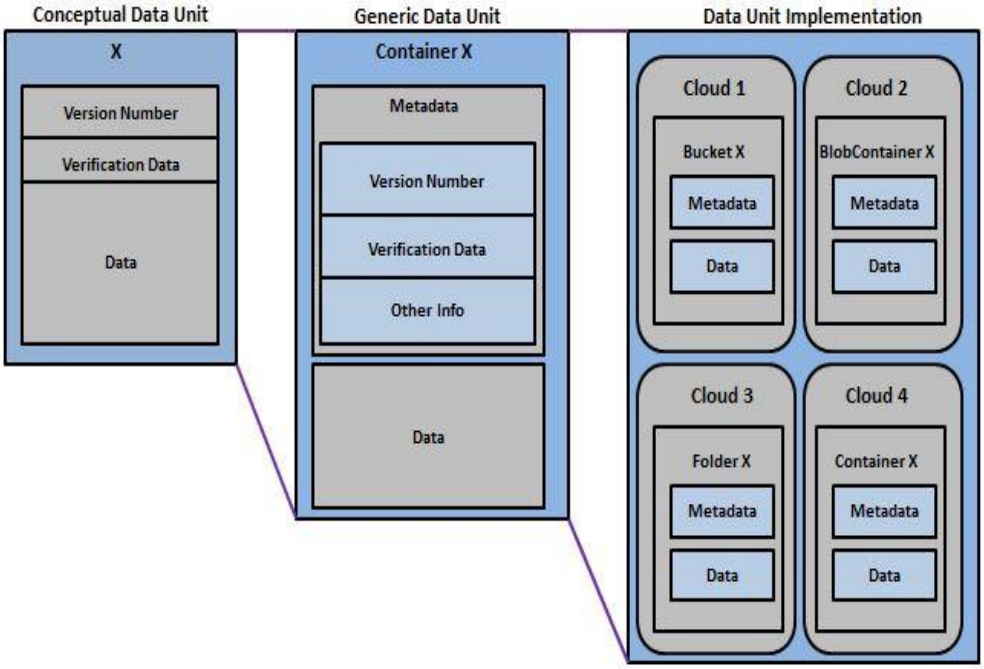

Figure 3.8: Data Model of DEPSKY System

information of data. The third and final abstraction layer is the "data unit implementation"; data unit container (generic or conceptual) is translated to each CSP according to their specific requirements (folder, BlobContainer etc.) [39].

3.3 Reason for the Selection of DEPSKY Multi Cloud Model

As there are different Multi Cloud deployment models have been proposed in literature, so it is difficult to choose which model will be suitable for implementation. For deployment of multi cloud environment, most suitable model is for implementation is DEPSKY Multi Cloud model due to its promising security features. Other models have certain limitations which are being addressed in DEPSKY multi cloud model. DEPSKY Multi Cloud model ensures the high availability of data for its customers by involving multiple CSP's. We select DEPSKY Multi Cloud model to ensure the high availability of information and to avoid the effects of VMbSC attack in CC.

3.4 Discussion

In CC, performance of network is dependent upon the availability of computing resources because in real time environment, the information is being accessed, processed and stored from the stakeholder's end. In order to ensure the high availability of resources and effective communication, there is need to involve multiple CSP's with whom the data is being pooled, so that in case of any malicious activity data could still be readily available to the stakeholder. Different models have been proposed in order to deploy Multi Cloud environment. The model we applied in this thesis is DEPSKY multi cloud model in order deploy cloud environment and to check the impact of VMBSC attack on this model.

4 Security of CC

Key advantages of CC can be realized in terms of effectiveness of services, efficiency of services, high end computational resources and low cost in order to meet the real realm challenges and problems. CC eliminates the concerns of the procurement of Information Technology (IT) infrastructure by providing the managed services platform through the invocation of third party rule. Due to vigorous model of CC, it is not easy to implement security for CC, as it involves third party access (i.e. CSP) to the data of end user. There is a vital need of ensuring security in CC environment. Security requirements vary from application to application in CC, but in general there are few basic requirements that need to be incorporated.

- Confidentiality
- Integrity
- Availability

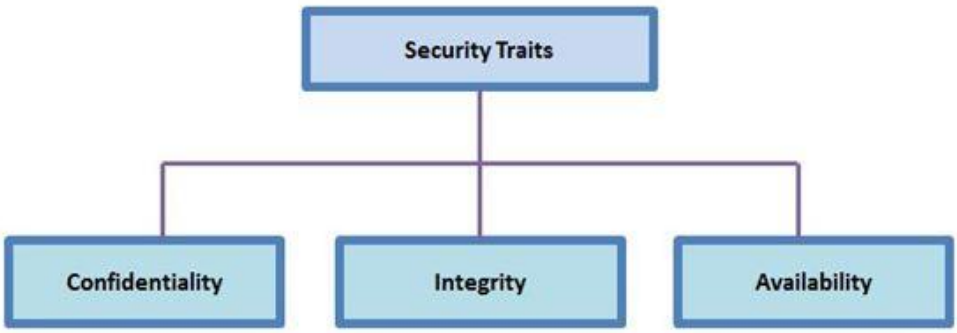

Figure 4.1: Security Requirements

1. Confidentiality: Confidentiality sentinels that information is altered in such a way that it acts like an illicit entity so that no one can access that information without having a proper authorization. In CC, it ensures that only authorized

persons have access to the desired information whereas for unauthorized persons it is not accessible. Confidentiality can be achieved by using techniques like encryption [40].

2. Integrity: Integrity sentinels that information is not altered maliciously during transit. In CC, it ensures that modification can only be made by authorized persons and all other modifications are neglected [41]. Data integrity can be ensured by using different cryptographic techniques like Message-Authentication Codes (MAC) on data blocks [42].

3. Availability: Availability sentinels that information is readily available to the authorized persons. In CC, availability is one of the major issues, as during the course of malicious activity the services often gets affected on temporary or permanent basis. The threats that directly affect the property of availability of services are DoS, DDoS attacks. In CC, it is eminent to have controls in order to avoid these kinds of attacks [43].

4.1 Attacks in CC

In this section we will discuss different attacks on CC depending upon the protocol layers and security traits as shown in Table 4.1 and Table 4.2. Following are the attacks faced by CC:

1. **Denial of Service Attack:** In DoS attack, malicious user prevents legitimate user from accessing and utilizing available computing resources. The attacker performs half connection attempts through SYN requests and not completing the TCP Three Way Handshake, as a result the VM's start allocating the resources to the incomplete connections, which leads towards the exhaustion of resources and resulting into DoS scenario [43]. DoS degrade the whole performance of system. 2. Man in the Middle Cryptographic Attack: In Man in the Middle attack, malicious user places itself in the communication channel for interception of information. The communication between two legitimate users is intercepted by malicious user and modified [44].

2. **Watering Hole Attack:** In watering Hole attack, the phishing site or already compromised site is used by malicious user for patiently waiting for the legitimate user to fall prey for the compromised website and then infecting the victim with drive by malicious program. In CC, web services often get compromised due to the exposure over the internet, so this attack is more practical and easy to conduct. As this attack operates in stealth mode and it is hard to identify.

3. **Network based Cross Tenant Attacks:** In Network based Cross Tenant attack; malicious user exploits the vulnerabilities of protocols like Dynamic Host Configuration Protocol (DHCP), Internet Protocol (IP) and Domain Name Service (DNS) protocol [45] for the distribution of traffic among various servers in the network. Usually botnets are used for this malicious purpose of abusing the fast flux of DNS characteristics for their own benefits. In a targeted attack scenario, such exploitation can lead towards the Denial of Service (DoS) to a particular server or Distributed Denial of Service (DDoS) attack on the whole network.

4. **XML Signature Element Wrapping Attacks:** In XML Signature Element Wrapping attack also known as Rewriting attack or Wrapping attack [46][44], Simple Object Access Protocol (SOAP) messages are eavesdropped and rewritten by injecting wrapper and bogus XML fields to access the victim resources. There is a deficiency in SOAP header, that it maintains valid signatures for the original documents thus making it prone to execute the modified requests.

5. **VMbSC Attack:** In VM based Side Channel attack, malicious user creates rouge VM in the among the tenants and the purpose of that rouge VM is to occupy the channel for the maximum amount of time, thus limiting the legitimate VM's to perform their desired operation and keeping them in idle state waiting for their turn.

Attacks	**Confidentiality**	**Integrity**	**Availability**
Denial of Service Attack		✔	✔
Man in the Middle Cryptographic Attack	✔	✔	✔
Watering Hole Attack	✔		✔
Network based Cross Tenant Attack			✔
XML Signature Element Wrapping Attack		✔	✔
VM based Side Channel Attack	✔		✔

Table 4.1: Attacks exploiting security traits

4.2 Virtual Machine based Side Channel Attack

One of the most prior security threats faced by CC is Virtual Machine based Side Channel (VMbSC) attack. CC is proposed to solve the availability and efficiency of computing resources without involving direct cost of infrastructure. The major purpose of CC is to provide a platform where resources are up and running all

Attacks	Physical	Link	Network	Transport	Application
Denial of Service Attack				✔	✔
Man in the Middle				✔	✔
Cryptographic Attack				✔	✔
Watering Hole Attack					✔
Network based Cross Tenant Attack	✔	✔	✔	✔	✔
XML Signature Element Wrapping Attack				✔	✔
VM based Side Channel Attack	✔			✔	✔

Table 4.2: Attacks on various layers

the time for its end users to consume and perform their daily tasks or operations in managed services platform. End users avail the resources from the pool as per their needs and requirements and store their confidential and important data on these resources. VM instances are utilized for this purpose. This leads towards the problem of virtualization layer monitoring. A malicious user who wants to extract the information can place the malicious VM entity along with the legitimate VM's in the datacenter. The purpose of the attacker is to steal the confidential data by occupying the read/write operations most of the time and keeping the legitimate VM's idle waiting for their turn. This attack is known as Virtual Machine based Side Channel (VMbSC) attack [44].

4.2.1 Impact of VMbSC Attack on CC

The manifestation of VMbSC attack ignites many potential issues for CC environments. Figure 4.2 elaborates how CC gets impacted by the presence of VMbSC attack.

- **QoS Degradation:** VMbSC attack steals the read/write operations from legitimate VM's, thus creating discontinuity in communication and services of legitimate VM's and in this way degradation in quality-of-service of CC.
- **Performance Degradation:** The foremost objective of CC is to effectively utilize the computing resources in order to avoid wastage or under-utilization of computing resources. VMbSC attack operates in a way that makes legitimate VM's waiting for their turn to perform the intended operations by stealing the read/write operations, thus degrading the performance of CC.
- **Denial of Service:** In VMbSC attack, the read/write operations are assigned to attacker's VM on priority and for the purpose of completing these operation,

all the resources are acquired by attacker's VM which results in choke down of network bandwidth and even unavailability of resources. This is referred to as denial of service (DoS) attack.

- **Information Leakage:** In VMBSC attack, the attacker's VM occupies the read/write operations on priority due to which the EU data gets compromised and leaked with malicious entity leading towards information leakage.

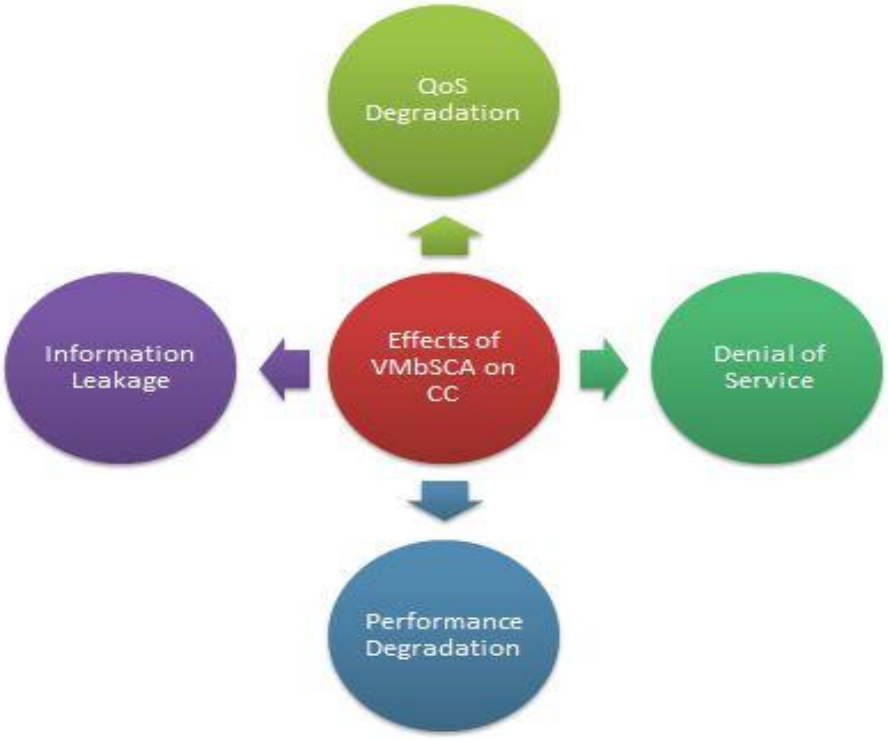

Figure 4.2: Effect of VMbSC Attack on CC

4.3 Detection & Prevention of VM based Side Channel Attack

4.3.1 HomeAlone Co-Residency Detection

In VMbSC attack, co-residency play an important role as attacker places the rouge VM with legitimate VM having shared physical resources. Through shared physical resources the threat exits that confidential information will be pooled among different VM's including the rouge VM. In order to detect and prevent VMbSC attacks,

co-residency detection technique known as HomeAlone is being used which detects the shared physical resources by using a mechanism in which activities of legitimate VM's are silenced in compartment of L2 cache for a specific time period and then cache usage is monitored to detect any unexpected activity (presence of rouge VM) [47] [48].

Limitation: By using HomeAlone co-residency detection, the operational excellence is impacted as activities of legitimate VM are turned off for specific time period in order to detect the co-residency resulting in downgrading of the performance.

4.3.2 NoHype

The idea of NoHype is to curtail the shared physical infrastructure by eliminating the hypervisor and still maintaining the properties of virtualization. The architecture of NoHype [48] [49] [50] have salient features as mentioned below:

1. It follows the principle of "one core per VM". This feature eliminates L1 side channel by removing the intervention between VM's and holds the multitenancy as multiple cores are present over a single chip.

2. It has memory partition which limits the memory access of every single VM over a designated range of memory.

3. It has dedicated virtual Input/Output devices which help in allocation of each dedicated Input/Output device to a VM.

NoHype significantly reduces the vulnerabilities of hypervisor by increasing isolation of VM's.

Limitation: It requires changing of hardware, which make it less concrete when considered applying in applying to the current environment of cloud setup.

4.3.3 Avoiding clflush Usage

In this detection mechanism, it encompasses a command of clflush for flushing the specific memory lines from the cache memory. By prohibiting the command of clflush, it would prevent attacker from using the Flush+Reload side channel attack on cache memory [51][52].

Limitation: By disabling clflush command, it will lead to disruption of memory consistency in devices where memory consistency is not supported.

4.3.4 Disabling Deduplication

By disabling deduplication, it prevents the detection of executed code by using flush and reload based detection mechanism. The partial disabling (e.g. deduplication of critical software) can also prevent the detection of library with having minimal impact on performance of CC [52].

Limitation: Memory optimization gets affected in multi-tenant environment by using the technique of disabling deduplication. Another limitation is that, spy processes named as Prime and Probe can still be triggered even after disabling the deduplication.

4.4 Discussion

This chapter focuses on security of CC. In this chapter we briefly discuss about different attacks on protocols layers and security traits in CC. This chapter also highlights on the VMbSC attack along with the detection and protection mechanism and their limitations.

5 Implementation

5.1 Simulation Environment

We used CloudSim toolkit on Java Eclipse platform for the implementation purpose. CloudSim toolkit provides basic libraries of classes which are extendable for simulation of cloud environment as per the requirement.

5.1.1 Single Cloud Environment

In SC Environment, we programmatically configured a test bed consisting of single CSP. The datacenter consisted of 3 VM's resources having the specification of 512 RAM, 2 processing cores and 595 MIPS (Million Instructions per Second). There are 3 DU (Data Unit) sizes i.e. 100Kb, 1Mb, 10Mb each having its own output and simulation run time. The read/write operations comprises of 10,000 instructions that are stored on or retrieved from the SC.

5.1.2 Depsky Multi Cloud Environment

In Depsky MC Environment, we programmatically configured a test bed consisting of 4 different CSP's. Each datacenter consisted of 3 VM's having its own specification. The specification of resources for CSP 1 comprises of 512 RAM, 2 processing cores and 710 MIPS (Million Instructions per Second). The specification of resources for CSP 2 comprises of 1024 RAM, 2 processing cores and 725 MIPS (Million Instructions per Second). The specification of resources for CSP 3 comprises of 2048 RAM, 1 processing core and 750 MIPS (Million Instructions per Second). The specification of resources for CSP 4 comprises of 4096 RAM, 1 processing core and 775 MIPS (Million Instructions per Second).There are 3 DU (Data Unit) sizes i.e. 100Kb, 1Mb, 10Mb each having its own output and simulation run time. The read/write operations comprises of 10,000 instructions that are stored on or retrieved from the Depsky MC.

5.2 Simulation Results

5.2.1 Single Cloud Environment

Table 5.1 elaborates the simulation run of SC model for 10,000 read and write operation over different sizes of DU's.

Operation	Data Unit	SC Output (ms)
10K Read	100 Kb	336.89
	1 Mb	460.77
	10 Mb	703.23
10K Write	100 Kb	252.17
	1 Mb	281.55
	10 Mb	404.12

Table 5.1: 10K Read & Write Operations on SC Model

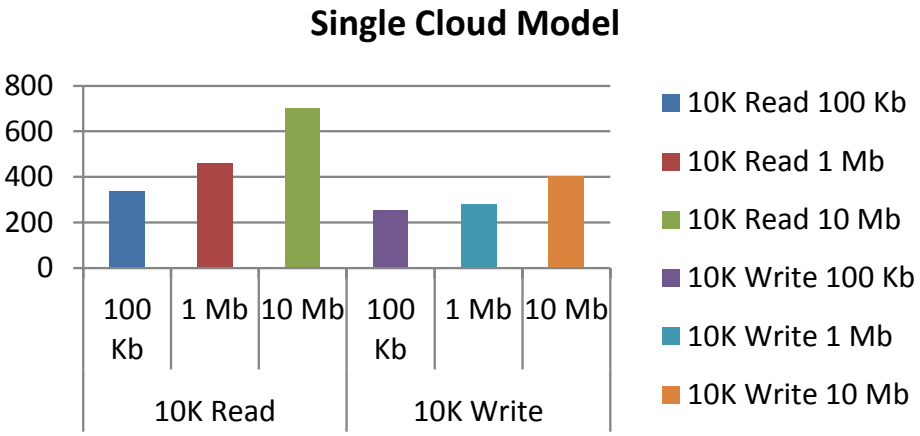

Figure 5.1: Single Cloud Model Output under Normal Operations

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time(ms)
0	0	28.07	0.1	28.17
1	1	28.57	0.1	28.67
2	2	29.07	0.1	29.17
3	0	28.07	28.17	56.23
4	1	28.57	28.67	57.24
5	2	29.07	29.17	58.25
-	-	-	-	-
-	-	-	-	-
28	1	28.57	257.23	285.8
29	2	29.07	261.77	290.84
30	0	28.07	280.76	308.83
31	1	28.57	285.8	314.37
32	2	29.07	290.84	319.92
33	0	28.07	308.83	336.89

Table 5.2: 10K Read Operations in 100Kb DU

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	21.01	0.1	21.11
1	1	21.38	0.1	21.48
2	2	21.76	0.1	21.86
3	0	21	21.11	42.11
4	1	21.38	21.48	42.87
5	2	21.76	21.86	43.62
-	-	-	-	-
-	-	-	-	-
28	1	21.38	192.54	213.93
29	2	21.76	195.94	217.7
30	0	21.01	210.15	231.16
31	1	21.38	213.93	235.31
32	2	21.76	217.7	239.46
33	0	21	231.16	252.17

Table 5.3: 10K Write Operations in 100Kb DU

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time(ms)
0	0	38.39	0.1	38.49
1	1	39.08	0.1	39.18
2	2	39.77	0.1	39.87
3	0	38.39	38.49	76.88
4	1	39.08	39.18	78.26
5	2	39.77	39.87	79.63
-	-	-	-	-
-	-	-	-	-
28	1	39.08	351.81	390.89
29	2	39.77	358.01	397.78
30	0	38.39	383.99	422.38
31	1	39.08	390.89	429.96
32	2	39.77	397.78	437.55
33	0	38.39	422.38	460.77

Table 5.4: 10K Read Operations in 1Mb DU

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	23.46	0.1	23.56
1	1	23.88	0.1	23.98
2	2	24.3	0.1	24.4
3	0	23.45	23.56	47.01
4	1	23.88	23.98	47.85
5	2	24.3	24.4	48.69
-	-	-	-	-
-	-	-	-	-
28	1	23.88	214.98	238.85
29	2	24.3	218.77	243.07
30	0	23.45	234.64	258.1
31	1	23.88	238.85	262.73
32	2	24.3	243.07	267.36
33	0	23.45	258.1	281.55

Table 5.5: 10K Write Operations in 1Mb DU

5.2.1.1 100 Kb Data Unit Output for Read & Write Operation in Single Cloud Model

5.2.1.2 1 Mb Data Unit Output for Read & Write Operation in Single Cloud Model

5.2.1.3 10 Mb Data Unit Output for Read & Write Operation in Single Cloud Model

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time(ms)
0	0	58.6	0.1	58.7
1	1	59.65	0.1	59.75
2	2	60.7	0.1	60.8
3	0	58.59	58.7	117.29
4	1	59.65	59.75	119.29
5	2	60.7	60.8	121.5
-	-	-	-	-
-	-	-	-	-
28	1	59.65	536.92	596.56
29	2	60.7	546.39	607.09
30	0	58.59	586.04	644.64
31	1	59.65	596.56	656.21
32	2	60.7	607.09	667.78
33	0	58.59	644.64	703.23

Table 5.6: 10K Read Operations in 10Mb DU

5.2.2 Depsky Multi Cloud Environment

Table 5.8 elaborates the simulation run of Depsky MC Model for 10,000 read and write operation over different sizes of DUs.

5.2.2.1 100 Kb Data Unit Output for Read & Write Operation in Depsky Multi Cloud Model

- **CSP 1**
- **CSP 2**

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	33.67	0.1	33.77
1	1	34.27	0.1	34.37
2	2	34.88	0.1	34.98
3	0	33.67	33.77	67.44
4	1	34.27	34.37	68.65
5	2	34.88	34.98	69.85
-	-	-	-	-
-	-	-	-	-
28	1	34.27	308.55	342.83
29	2	34.88	314	348.87
30	0	33.67	336.78	370.45
31	1	34.27	342.83	377.1
32	2	34.88	348.87	383.75
33	0	33.67	370.45	404.12

Table 5.7: 10K Write Operations in 10Mb DU

Operation	Data Unit	Depsky MC Output (ms)			
		CSP1	CSP2	CSP3	CSP4
10K Read	100 Kb	282.38	276.5	267.29	258.66
	1 Mb	488.94	471.6	445.41	421.98
	10 Mb	954.32	890.83	801.65	728.89
10K Write	100 Kb	180.86	177.86	173.15	168.81
	1 Mb	203.07	199.36	193.5	188.08
	10 Mb	322.44	313.24	299.06	286

Table 5.8: 10K Read & Write Operations on SC Model

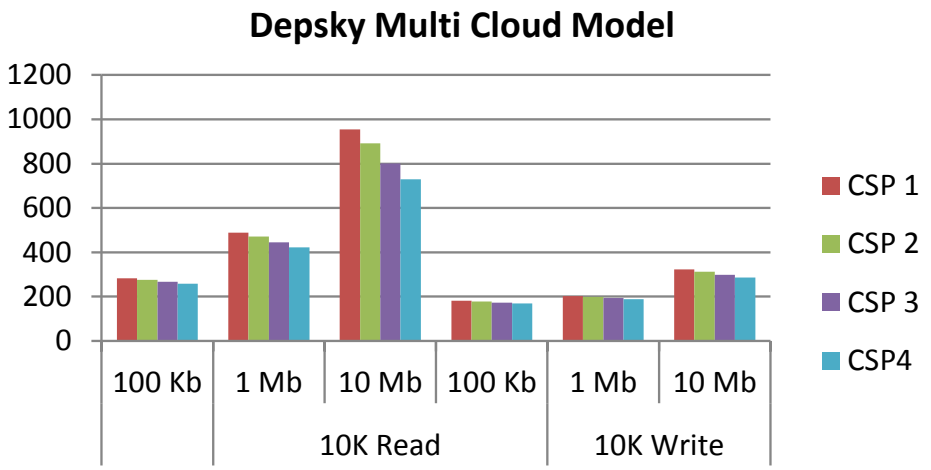

Figure 5.2: Depsky Multi Cloud Model Output under Normal Operations

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	23.56	0.1	23.66
1	1	23.97	0.1	24.07
2	2	24.37	0.1	24.47
3	0	23.52	23.66	47.18
4	1	23.94	24.07	48.01
5	2	24.37	24.47	48.83
-	-	-	-	-
-	-	-	-	-
28	1	23.94	215.68	239.62
29	2	24.37	219.39	243.75
30	0	23.52	235.34	258.86
31	1	23.94	239.62	263.56
32	2	24.36	243.75	268.12
33	0	23.52	258.86	282.38

Table 5.9: 10K Read Operations in 100Kb DU – CSP1

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	15.16	0.1	15.26
1	1	15.38	0.1	15.48
2	2	15.71	0.1	15.81
3	0	15.05	15.26	30.32
4	1	15.38	15.48	30.87
5	2	15.71	15.81	31.53
-	-	-	-	-
-	-	-	-	-
28	1	15.38	138.56	153.94
29	2	15.71	141.52	157.24
30	0	15.05	150.75	165.8
31	1	15.38	153.94	169.32
32	2	15.71	157.24	172.95
33	0	15.05	165.8	180.86

Table 5.10: 10K Write Operations in 100Kb DU – CSP1

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	23.03	0.1	23.13
1	1	23.45	0.1	23.55
2	2	23.86	0.1	23.96
3	0	23.03	23.13	46.17
4	1	23.45	23.55	47
5	2	23.86	23.96	47.82
-	-	-	-	-
-	-	-	-	-
28	1	23.45	211.13	234.57
29	2	23.86	214.85	238.71
30	0	23.03	230.43	253.47
31	1	23.45	234.57	258.02
32	2	23.86	238.71	262.57
33	0	23.03	253.47	276.5

Table 5.11: 10K Read Operations in 100Kb DU – CSP2

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	14.85	0.1	14.95
1	1	15.16	0.1	15.26
2	2	15.49	0.1	15.59
3	0	14.81	14.95	29.76
4	1	15.16	15.26	30.43
5	2	15.46	15.59	31.05
-	-	-	-	-
-	-	-	-	-
28	1	15.13	136.37	151.5
29	2	15.46	139.26	154.72
30	0	14.81	148.24	163.05
31	1	15.13	151.5	166.63
32	2	15.46	154.72	170.18
33	0	14.81	163.05	177.86

Table 5.12: 10K Read Operations in 100Kb DU – CSP2

- **CSP 3**
- **CSP 4**

5.2.2.2 Mb Data Unit Output for Read & Write Operation in Depsky Multi Cloud Model

- **CSP 1**
- **CPS2**
- **CSP 3**
- **CSP 4**

5.2.2.3 10 Mb Data Unit Output for Read & Write Operation in Depsky Multi Cloud Model

- **CSP 1**

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	22.27	0.1	22.37
1	1	22.67	0.1	22.77
2	2	23.14	0.1	23.24
3	0	22.26	22.37	44.63
4	1	22.67	22.77	45.43
5	2	23.07	23.24	46.31
-	-	-	-	-
-	-	-	-	-
28	1	22.66	204.09	226.75
29	2	23.07	207.77	230.83
30	0	22.27	222.75	245.02
31	1	22.67	226.75	249.42
32	2	23.07	230.83	253.9
33	0	22.27	245.02	267.29

Table 5.13: 10K Read Operations in 100Kb DU – CSP3

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	14.42	0.1	14.52
1	1	14.74	0.1	14.84
2	2	15.05	0.1	15.15
3	0	14.42	14.52	28.94
4	1	14.74	14.84	29.57
5	2	15.05	15.15	30.2
-	-	-	-	-
-	-	-	-	-
28	1	14.74	132.73	147.46
29	2	15.05	135.57	150.62
30	0	14.42	144.3	158.73
31	1	14.74	147.46	162.2
32	2	15.05	150.62	165.67
33	0	14.42	158.73	173.15

Table 5.14: 10K Write Operations in 100Kb DU – CSP3

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	21.55	0.1	21.65
1	1	21.93	0.1	22.03
2	2	22.38	0.1	22.48
3	0	21.55	23.66	43.2
4	1	21.93	24.07	43.97
5	2	22.32	24.47	44.8
-	-	-	-	-
-	-	-	-	-
28	1	21.99	197.51	219.5
29	2	22.32	201.05	223.37
30	0	21.55	215.57	237.12
31	1	21.93	219.5	241.43
32	2	22.32	223.37	245.69
33	0	21.55	237.12	258.66

Table 5.15: 10K Read Operations in 100Kb DU – CSP4

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	14.05	0.1	14.25
1	1	14.36	0.1	14.56
2	2	14.67	0.1	14.87
3	0	14.05	14.25	28.3
4	1	14.36	14.56	28.92
5	2	14.67	14.87	29.53
-	-	-	-	-
-	-	-	-	-
28	1	14.36	129.42	143.78
29	2	14.67	132.19	146.86
30	0	14.05	140.71	154.76
31	1	14.36	143.78	158.14
32	2	14.67	146.86	161.53
33	0	14.05	154.76	168.81

Table 5.16: 10K Write Operations in 100Kb DU – CSP4

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	40.81	0.1	40.91
1	1	41.46	0.1	41.56
2	2	42.19	0.1	42.29
3	0	40.73	23.66	81.64
4	1	41.46	24.07	83.02
5	2	42.19	24.47	84.49
-	-	-	-	-
-	-	-	-	-
28	1	41.46	373.25	414.71
29	2	42.19	379.92	422.11
30	0	40.73	407.48	448.21
31	1	41.46	414.71	456.17
32	2	42.19	422.11	464.3
33	0	40.73	448.21	488.94

Table 5.17: 10K Read Operations in 1Mb DU – CSP1

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	16.93	0.1	17.03
1	1	17.28	0.1	17.38
2	2	17.65	0.1	17.75
3	0	16.91	14.25	33.95
4	1	17.28	14.56	34.67
5	2	17.65	14.87	35.41
-	-	-	-	-
-	-	-	-	-
28	1	17.28	155.65	172.93
29	2	17.65	158.98	176.63
30	0	16.91	169.25	186.16
31	1	17.28	172.93	190.22
32	2	17.65	176.63	194.29
33	0	16.91	186.16	203.07

Table 5.18: 10K Write Operations in 1Mb DU – CSP1

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	39.29	0.1	39.39
1	1	40	0.1	40.1
2	2	40.7	0.1	40.8
3	0	39.29	23.66	78.68
4	1	40	24.07	80.1
5	2	40.7	24.47	81.51
-	-	-	-	-
-	-	-	-	-
28	1	40	360.08	400.08
29	2	40.7	366.44	407.14
30	0	39.29	393.02	432.31
31	1	40	400.08	440.08
32	2	40.7	407.14	447.85
33	0	39.29	432.31	471.6

Table 5.19: 10K Read Operations in 1Mb DU – CSP2

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	16.6	0.1	16.7
1	1	17.04	0.1	17.14
2	2	17.39	0.1	17.49
3	0	16.61	16.7	33.31
4	1	16.97	17.14	34.11
5	2	17.33	17.49	34.83
-	-	-	-	-
-	-	-	-	-
28	1	16.97	152.89	169.86
29	2	17.33	156.15	173.48
30	0	16.6	166.15	182.76
31	1	16.97	169.86	186.83
32	2	17.33	173.48	190.82
33	0	16.61	182.76	199.36

Table 5.20: 10K Write Operations in 1Mb DU – CSP2

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	37.11	0.1	37.21
1	1	37.78	0.1	37.88
2	2	38.44	0.1	38.54
3	0	37.11	37.21	74.32
4	1	37.78	37.88	75.65
5	2	38.44	38.54	76.98
-	-	-	-	-
-	-	-	-	-
28	1	37.78	340.09	377.86
29	2	38.44	346.08	384.53
30	0	37.11	371.19	408.3
31	1	37.78	377.86	415.64
32	2	38.44	384.53	422.97
33	0	37.11	408.3	445.41

Table 5.21: 10K Read Operations in 1Mb DU – CSP3

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	16.12	0.1	16.22
1	1	16.47	0.1	16.57
2	2	16.82	0.1	16.92
3	0	16.12	16.22	32.33
4	1	16.47	16.57	33.04
5	2	16.82	16.92	33.75
-	-	-	-	-
-	-	-	-	-
28	1	16.47	148.33	164.8
29	2	16.82	151.5	168.33
30	0	16.12	161.27	177.39
31	1	16.47	164.8	181.27
32	2	16.82	168.33	185.15
33	0	16.12	177.39	193.5

Table 5.22: 10K Write Operations in 1Mb DU – CSP3

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	35.16	0.1	35.26
1	1	35.79	0.1	35.89
2	2	36.42	0.1	36.52
3	0	35.16	35.26	70.41
4	1	35.79	35.89	71.68
5	2	36.42	36.52	72.94
-	-	-	-	-
-	-	-	-	-
28	1	35.79	322.19	357.98
29	2	36.42	327.87	364.29
30	0	35.16	351.67	386.82
31	1	35.79	357.98	393.76
32	2	36.42	364.29	400.71
33	0	35.16	386.82	421.98

Table 5.23: 10K Read Operations in 1Mb DU – CSP4

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	15.66	0.2	15.86
1	1	16	0.2	16.2
2	2	16.34	0.2	16.54
3	0	15.66	15.86	31.51
4	1	16	16.2	32.2
5	2	16.34	16.54	32.89
-	-	-	-	-
-	-	-	-	-
28	1	16	144.19	160.19
29	2	16.34	147.28	163.62
30	0	15.66	156.76	172.42
31	1	16	160.19	176.19
32	2	16.34	163.62	179.96
33	0	15.66	172.42	188.08

Table 5.24: 10K Write Operations in 1Mb DU – CSP4

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	79.52	0.1	79.62
1	1	80.95	0.1	81.05
2	2	82.37	0.1	82.47
3	0	79.52	79.62	159.14
4	1	80.95	81.05	161.99
5	2	82.38	82.47	164.85
-	-	-	-	-
-	-	-	-	-
28	1	80.95	728.64	809.58
29	2	82.38	741.5	823.88
30	0	79.52	795.28	874.8
31	1	80.95	809.58	890.53
32	2	82.38	823.88	906.26
33	0	79.52	874.8	954.32

Table 5.25: 10K Read Operations in 1Mb DU – CSP1

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	26.86	0.1	26.96
1	1	27.45	0.1	27.55
2	2	28.04	0.1	28.14
3	0	26.86	26.96	53.82
4	1	27.45	27.55	55
5	2	28.04	28.14	56.18
-	-	-	-	-
-	-	-	-	-
28	1	27.45	247.15	274.6
29	2	28.04	252.49	280.53
30	0	26.86	268.72	295.58
31	1	27.45	274.6	302.05
32	2	28.04	280.53	308.56
33	0	26.86	295.58	322.44

Table 5.26: 10K Write Operations in 1Mb DU – CSP1

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	74.22	0.1	74.32
1	1	75.55	0.1	75.65
2	2	76.88	0.1	76.98
3	0	74.22	74.32	148.54
4	1	75.55	75.65	151.2
5	2	76.89	76.98	153.87
-	-	-	-	-
-	-	-	-	-
28	1	75.55	680.06	755.61
29	2	76.89	692.16	769.05
30	0	74.22	742.38	816.61
31	1	75.55	755.61	831.16
32	2	76.88	769.05	845.93
33	0	74.22	816.61	890.83

Table 5.27: 10K Read Operations in 1Mb DU – CSP2

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	26.11	0.1	26.21
1	1	26.67	0.1	26.77
2	2	27.24	0.1	27.34
3	0	26.09	26.21	52.3
4	1	26.67	26.77	53.43
5	2	27.24	27.34	54.57
-	-	-	-	-
-	-	-	-	-
28	1	26.66	240.09	266.75
29	2	27.24	245.29	272.52
30	0	26.09	261.05	287.15
31	1	26.67	266.75	293.42
32	2	27.24	272.52	299.76
33	0	26.09	287.15	313.24

Table 5.28: 10K Write Operations in 1Mb DU – CSP2

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	66.8	0.1	66.9
1	1	67.99	0.1	68.09
2	2	69.2	0.1	69.3
3	0	66.8	66.9	133.69
4	1	68	68.09	136.09
5	2	69.2	69.3	138.49
-	-	-	-	-
-	-	-	-	-
28	1	68.1	612.07	680.17
29	2	69.2	622.86	692.05
30	0	66.8	668.05	734.85
31	1	68	680.17	748.17
32	2	69.2	692.05	761.25
33	0	66.8	734.85	801.65

Table 5.29: 10K Read Operations in 1Mb DU – CSP3

- **CSP 2**
- **CSP 3**
- **CSP 4**

5.3 Assessment of VMbSC Attack

5.3.1 Implementation of VMbSC Attack

For the implementation of VMbSC attack, we utilized the same environment of Single Cloud and Multi Cloud Model with an additional entity named as "Global Broker". The purpose of Global Broker is to initiate the placement of Malicious VM along with the images of legitimate VM in a particular CSP environment. Once successfully implanting the malicious VM in Cloud environment, the malicious VM sets its priority of accessing the Read/Write operations high and downgrading the priority of legitimate VM as low. The DU selected to perform this analysis is 1Mb. Now when there are instructions called upon for accessing the resources in order to perform Read/Write operations the malicious VM acquires the Read/Write operations on priority for a specific amount time and after completing the cycle

Read Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	60.73	0.1	60.83
1	1	61.82	0.1	61.92
2	2	62.9	0.1	63
3	0	60.72	60.83	121.55
4	1	61.81	61.92	123.73
5	2	62.91	63	125.91
-	-	-	-	-
-	-	-	-	-
28	1	61.81	556.44	618.26
29	2	62.91	566.25	629.16
30	0	60.76	607.41	668.16
31	1	61.92	618.26	680.17
32	2	63.01	629.16	692.16
33	0	60.72	668.16	728.89

Table 5.30: 10K Read Operations in 1Mb DU – CSP4

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	23.83	0.1	23.93
1	1	24.35	0.1	24.45
2	2	24.87	0.1	24.97
3	0	23.83	23.93	47.75
4	1	24.35	24.45	48.79
5	2	24.87	24.97	49.84
-	-	-	-	-
-	-	-	-	-
28	1	24.35	219.22	243.57
29	2	24.87	223.92	248.79
30	0	23.82	238.35	262.18
31	1	24.35	243.57	267.92
32	2	24.87	248.79	273.65
33	0	23.82	262.18	286

Table 5.31: 10K Write Operations in 1Mb DU – CSP4

Write Op ID	VM ID	Time to Complete Operation	Start Time (ms)	Finish Time (ms)
0	0	24.98	0.1	25.08
1	1	25.45	0.1	25.55
2	2	26	0.1	26.1
3	0	24.91	25.08	49.99
4	1	25.45	25.55	51.01
5	2	26	26.1	52.1
-	-	-	-	-
-	-	-	-	-
28	1	25.45	229.18	254.63
29	2	26	234.09	260.09
30	0	24.91	249.25	274.16
31	1	25.45	254.63	280.09
32	2	26.02	260.09	286.11
33	0	24.91	274.16	299.06

Table 5.32: 10K Write Operations in 1Mb DU – CSP3

of malicious VM, the remaining operations are assigned to legitimate VM's. The specific amount of time is discussed in next section based on the scenarios.

5.3.2 Simulation Environment for VMbSC Attack on Single and Depsky Multi Cloud Model

There are two cloud models that we have utilized in order to create a comparison on the impact of VMbSC attack on these models. We have used the same simulation runs of both cloud models during normal operations as explained in Section 5.2 for the purpose of analysis of VMbSC attack. All results are obtained with the confidence of 93%. Results are obtained based on three scenarios.

- **Attack – For – 40%:** In this pattern of attack, malicious VM acquires the Read/Write operations for the initial 40% of simulation run and the legitimate VM's acquire these operations for the remaining 60% of simulation run.
- **Attack – For – 60%:** In this pattern of attack, malicious VM acquires the Read/Write operations for the initial 60% of simulation run and the legitimate VM's acquire these operations for the remaining 40% of simulation run.
- **Attack – For – 80%:** In this pattern of attack, malicious VM acquires the Read/Write operations for the initial 80% of the simulation run and the

legitimate VM's acquire these operations for the remaining 20% of simulation run.

5.4 Assessment of Single Cloud and Depsky Multi Cloud Model on VMbSC Attack

Presence of VMbSC attack exploits the properties of virtual entities i.e. legitimate VM's. In VMbSC attack, the malicious VM changes the priority of legitimate VM as low which results in acquiring the Read/Write operations on highest priority. Figure 5.3 represents the flow chart of different VMbSC attack patterns for SC and Depsky MC Model.

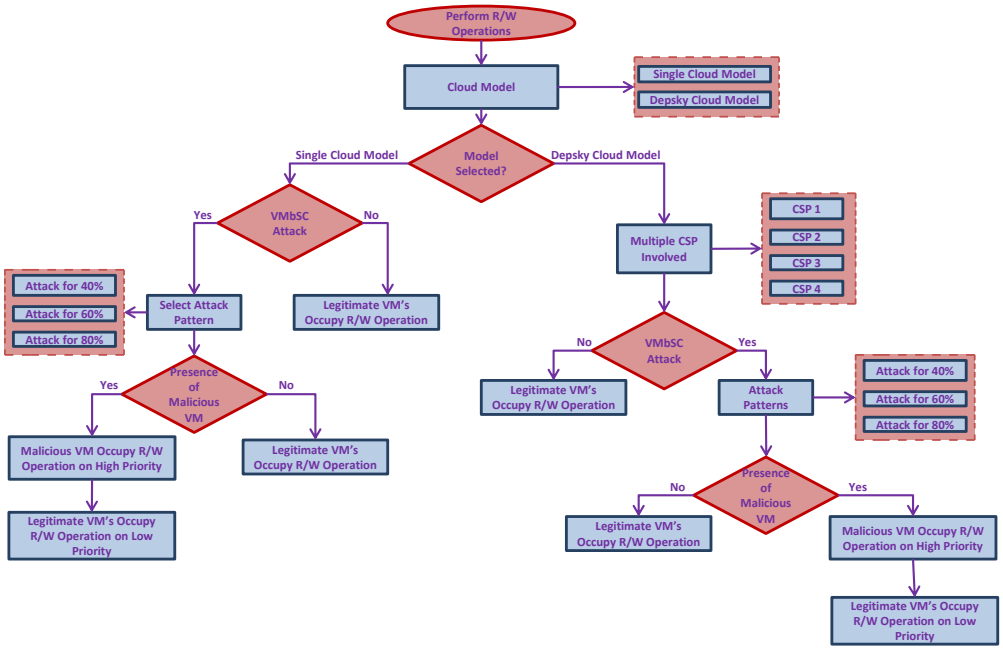

Figure 5.3: Flow VMbSC Attack for SC and Depsky MC Model

Following are the impact of VMbSC Attack on SC and Depsky MC Model.

5.4.1 Single Cloud Model with VMbSC Attack

5.4.1.1 10K Read and Write Operations

In Single Cloud model, there is only one CSP involved that is providing services to the client. Graph represents three attack scenarios for Read and Write operations under VMbSC attack. As shown in graph attack for 40% pattern, the initial 40% of the operations are consumed by malicious VM and last 60% are assigned to the legitimate VM's. In attack for 60% pattern, legitimate VM's occupy Read and Write operations for 40% only whereas initial 40% are assigned to malicious VM. In attack for 80% pattern, large chunk of Read and Write operations are consumed by malicious VM whereas only 20% is assigned to legitimate VM's.

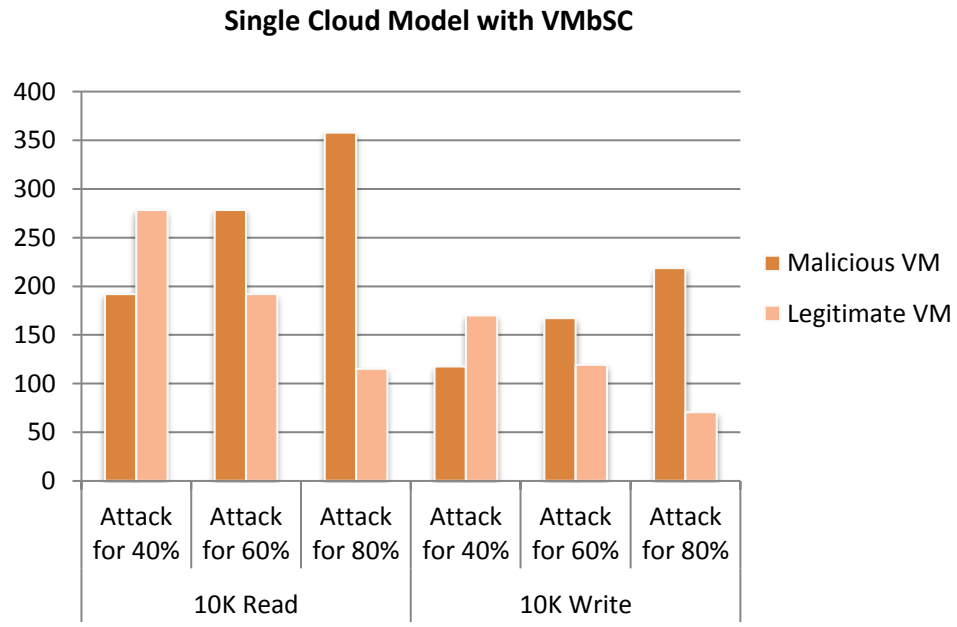

Figure 5.4: Impact VMbSC Attack Patterns on Single Cloud Model

5.4.2 Depsky Multi Cloud Model with VMbSC Attack

5.4.2.1 Read Operations

In Depsky Multi Cloud model, there are four CSP's involved that are providing services to the client at the same time. Each CSP has its own cloud environment

and are at distant locations. So, attack vector space of VMbSC attack for Depsky Multi Cloud Model is very big due to which placement of malicious VM is possible in only one CSP among the four CSP's. The Graph represents three attack scenarios for Read under VMbSC attack. The affected CSP with VMbSC attack in below mentioned graph is "CSP 1" whereas rest three CSP's operate under normal scenario and are not affected by VMbSC attack. As shown in graph attack for 40% pattern, the initial 40% of the Read operations are consumed by malicious VM and last 60% are assigned to the legitimate VM's in CSP 1 environment. In attack for 60% pattern, legitimate VM's occupy Read operations for 40% only whereas initial 40% are assigned to malicious VM in CSP 1 environment. In attack for 80% pattern, large chunk of Read operations are consumed by malicious VM whereas only 20% is assigned to legitimate VM's in CSP 1 environment.

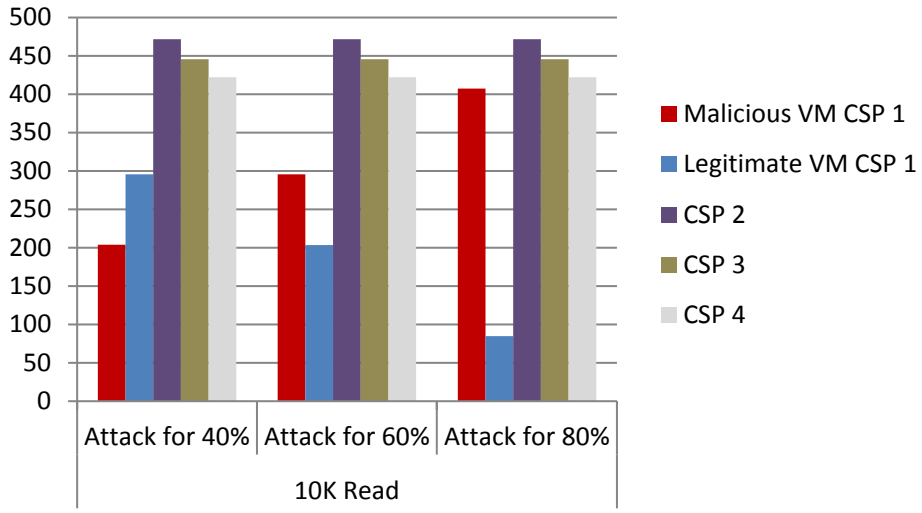

Figure 5.5: Impact VMbSC Attack Patterns on Depsky Multi Cloud Model with 10K Reads

5.4.2.2 Write Operations

The Graph represents three attack scenarios for Write operations under VMbSC attack. The affected CSP with VMbSC attack in below mentioned graph is "CSP 1" whereas rest three CSP's operate under normal scenario and are not affected by VMbSC attack. As shown in graph attack for 40% pattern, the initial 40% of the Write operations are consumed by malicious VM and last 60% are assigned to

the legitimate VM's in CSP 1 environment. In attack for 60% pattern, legitimate VM's occupy Write operations for 40% only whereas initial 40% are assigned to malicious VM in CSP 1 environment. In attack for 80% pattern, large chunk of Write operations are consumed by malicious VM whereas only 20% is assigned to legitimate VM's in CSP 1 environment.

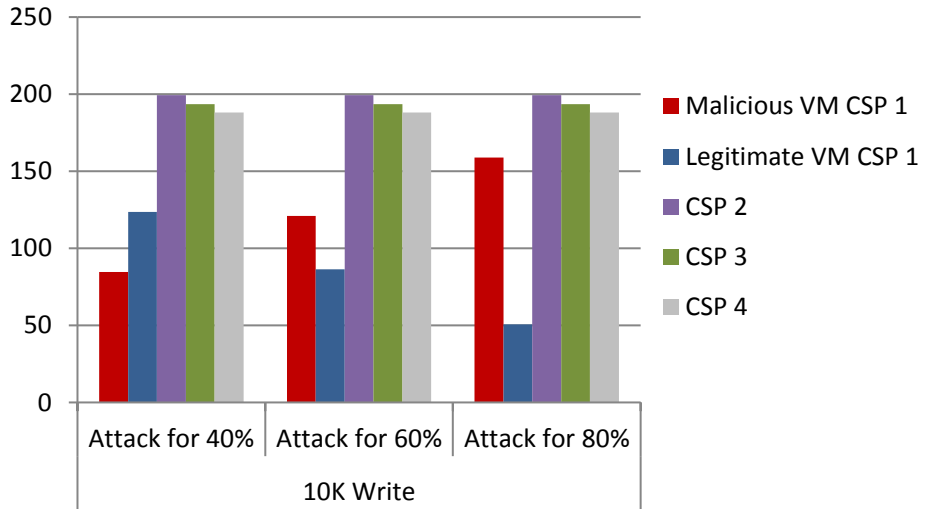

Figure 5.6: Impact VMbSC Attack Patterns on Depsky Multi Cloud Model with 10K Writes

5.5 Discussion

This chapter presents the implementation of Single Cloud Model, Depsky Multi Cloud Model and VMbSC attack. We analyzed the performance of Single Cloud and Depsky Multi Cloud Model under normal operations and we also analyzed the impact of VMbSC attack on these models. VMbSC attack completes affects and degrades the performance of Single Cloud Model in perspective of both CSP and client. Whereas in case of Depsky Multi Cloud Model only a particular CSP with presence of malicious entity in its environment get impacted with degraded performance, thus there is no impact on client side as information is readily available from other CSP's. Depsky Multi Cloud Model acts as a protective mechanism against virtualization layer attacks like VMbSC attack.

6 Conclusions and Future Work

In this chapter, we finally conclude the objectives of thesis that are functional for the analysis of VMbSC attack on Depsky Multi Cloud Model. In this section we will discuss about the achieved objectives and their generated results that are acquired through the implementation. Finally we will conclude the thesis with some future recommendations.

6.1 Discussion on objectives

CC helps to reduce the cost of procuring and managing the IT Infrastructure by providing a managed services platform in which CSP's are responsible for the operations and clients process their data. For CC, a secure environment is very important as confidential data is pooled with third parties. Therefore we established a comparison by utilizing two diverse models i.e. Single Cloud Model and Depsky Multi Cloud Model. Security is a major concern for CC environment. Due to external entities being involved to handle the confidential data, CC is more vulnerable to threats. VMbSC is one of the virtualization layer attacks that affect t and changes the properties of virtual entities on which the information is being stored. We implemented Single Cloud and Depsky Multi Cloud model in order to observe the impact of VMbSC attack on CC. we deduced form the simulation that VMbSC attack completely affects the operational performance of Single Cloud Model. Whereas in case of Depsky Multi Cloud model only a single CSP gets affected by this virtualization layer attack. Depsky model acts a protective mechanism against such attacks due to involvement of multiple CSP because if one CSP is down data is readily available from other CSP's.

6.2 Discussion on results

In this research, impact of VM based side channel attack on Depsky multi cloud model has been proposed. There are two models that have been implemented in this research i.e. Single Cloud Model and Depsky Multi Cloud Model in order to establish a comparison on the performance factors. In Single Cloud model there

is only one CSP involved that is providing services to the client end. Whereas in Depsky Multi Cloud model there is involvement of four CSP's which are providing services to client at the same time. Client confidential information is replicated on these four diverse CSP's and whenever there is a downtime at one particular CSP, the data is readily available to client from other CSP's, thus ensuring high availability. Security is major concern for CC. VMbSC attack is one of the attacks that affects the virtualization layer and thus impacting into degraded performance of CC. Three attack patterns have been discussed in this research to check the impact of VMbSC attack on Single Cloud and Multi Cloud model. For attack for 40% pattern, the initial 40% of the operations are consumed by malicious VM and last 60% are assigned to the legitimate VM's. In attack for 60% pattern, legitimate VM's occupy Read and Write operations for 40% only whereas initial 40% are assigned to malicious VM. In attack for 80% pattern, large chunk of Read and Write operations are consumed by malicious VM whereas only 20% is assigned to legitimate VM's. Our results show that VMbSC attack completely impacts the Single Cloud model whereas in case of Depsky Multi Cloud model, only a particular CSP with presence of malicious entity in its environment get impacted with degraded performance, thus there is no impact on client side as information is readily available from other CSP's. So Depsky Multi Cloud acts a protective mechanism against virtualization layer attacks like VMbSC attack.

6.3 Future Work

Although good results have been obtained, there is still scope for improvement in analysis of impact of VMbSC attack on Depsky multi cloud model. In future it would be interesting to propose a scheduler based defensive mechanism technique for detection and protection of virtual entities against VMbSC attack on CC model. In future we will try proposing a VM scheduling based algorithm to cater these types of virtualization layer attack.

Bibliography

[1] Ajey Singh and Maneesh Shrivastava. Overview of security issues in cloud computing. *International Journal of Advanced Computer Research (IJACR) Volume*, 2, 2012.

[2] Ahmet Cihat Baktır and Bilgin Metin. Cloud computing perception and success factors for information technology usage in turkey. In *Radioelektronika (RADIOELEKTRONIKA), 2016 26th International Conference*, pages 330–335. IEEE, 2016.

[3] Wenjun Wu, Wei Tek Tsai, Chao Jin, Guanqiu Qi, and Jie Luo. Proceedings-ieee 8th international symposium on service oriented system engineering, sose 2014. In *IEEE Computer Society*, 2014.

[4] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[5] Daryl C Plummer, Thomas J Bittman, Tom Austin, David W Cearley, and David Mitchell Smith. Cloud computing: Defining and describing an emerging phenomenon. *Gartner, June*, 17, 2008.

[6] Peter Mell, Tim Grance, et al. The nist definition of cloud computing. 2011.

[7] Anil Kumar Gupta and Manoj Kumar Gupta. A new era of cloud computing in private and public sector organization. *International Archive of Applied Sciences and Technology*, 3(2):80–85, 2012.

[8] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy H Katz, Andrew Konwinski, Gunho Lee, David A Patterson, Ariel Rabkin, Ion Stoica, et al. Above the clouds: a berkeley view of cloud. *Electrical Engineering and Computer Sciences, University of California at Berkeley*, 2009.

[9] Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1):1–11, 2011.

[10] Sumant Ramgovind, Mariki M Eloff, and Elme Smith. The management of security in cloud computing. In *Information Security for South Africa (ISSA), 2010*, pages 1–7. IEEE, 2010.

[11] Ian Foster. The grid: Computing without bounds.: Computing without bounds. *Scientific American*, 288(4):78, 2003.

[12] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6):599–616, 2009.

[13] Luis M Vaquero, Luis Rodero-Merino, Juan Caceres, and Maik Lindner. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 39(1):50–55, 2008.

[14] William Voorsluys, James Broberg, and Rajkumar Buyya. Introduction to cloud computing. *Cloud computing: Principles and paradigms*, pages 1–41, 2011.

[15] Bhaskar Prasad Rimal, Eunmi Choi, and Ian Lumb. A taxonomy and survey of cloud computing systems. *INC, IMS and IDC*, pages 44–51, 2009.

[16] Qi Zhang, Lu Cheng, and Raouf Boutaba. Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, 1(1):7–18, 2010.

[17] ESX VMware. Server http://www. vmware. com/products/esx/the manufacturers product catalog details the features and specifications of the product. *Also, white papers and case study discuss the advantages and application of the technology.*

[18] Dedicated Server. Managed hosting, web hosting by rackspace hosting.

[19] Tejaswi Redkar, Tony Guidici, and Todd Meister. *Windows azure platform*, volume 1. Springer, 2011.

[20] Alexander Zahariev. Google app engine. *Helsinki University of Technology*, pages 1–5, 2009.

[21] Cloud Hosting. Cloud computing and hybrid infrastructure from gogrid, 2012.

[22] Zubaida Alazawi, Saleh Altowaijri, Rashid Mehmood, and Mohmmad B Abdljabar. Intelligent disaster management system based on cloud-enabled vehicular networks. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 361–368. IEEE, 2011.

[23] Jiehan Zhou, Teemu Leppanen, Erkki Harjula, Mika Ylianttila, Timo Ojala, Chen Yu, Hai Jin, and Laurence Tianruo Yang. Cloudthings: A common architecture for integrating the internet of things with cloud computing. In *Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference on*, pages 651–657. IEEE, 2013.

[24] Sebnem Rusitschka, Kolja Eger, and Christoph Gerdes. Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 483–488. IEEE, 2010.

[25] Utpal Jyoti Bora and Majidul Ahmed. E-learning using cloud computing. *International Journal of Science and Modern Engineering*, 1(2):9–12, 2013.

[26] Bartosz Kryza, Dariusz Król, Michal Wrzeszcz, Lukasz Dutka, and Jacek Kitowski. Interactive cloud data farming environment for military mission planning support. *Computer Science*, 13:89–100, 2012.

[27] Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M Shamim Hossain, Abdulhameed Alelaiwi, and M Anwar Hossain. A survey on sensor-cloud: architecture, applications, and approaches. *International Journal of Distributed Sensor Networks*, 9(2):917923, 2013.

[28] Pankaj Deep Kaur and Inderveer Chana. Cloud based intelligent system for delivering health care as a service. *Computer methods and programs in biomedicine*, 113(1):346–359, 2014.

[29] Hiroshi Harada, Homare Murakami, Kentaro Ishizu, Stanislav Filin, Yoshia Saito, Ha Nguyen Tran, Goh Miyamoto, Mikio Hasegawa, Yoshitoshi Murata, and Shuzo Kato. A software defined cognitive radio system: cognitive wireless cloud. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pages 294–299. IEEE, 2007.

[30] Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya. A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, 40:325–344, 2014.

[31] Mazhar Ali, Samee U Khan, and Athanasios V Vasilakos. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305:357–383, 2015.

[32] Christian Cachin, Robert Haas, and Marko Vukolic. Dependable storage in the intercloud. Technical report, Research Report RZ, 3783, 2010.

[33] Axel Buecker, Ana Veronica Carreno, Norman Field, Christopher Hockings, Daniel Kawer, Sujit Mohanty, Guilherme Monteiro, et al. *Enterprise Security Architecture Using IBM Tivoli Security Solutions*. IBM Redbooks, 2007.

[34] Hussam Abu-Libdeh, Lonnie Princehouse, and Hakim Weatherspoon. Racs: a case for cloud storage diversity. In *Proceedings of the 1st ACM symposium on Cloud computing*, pages 229–240. ACM, 2010.

[35] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 85–90. ACM, 2009.

[36] Haider Ali Khan Khattak, Haider Abbass, Ayesha Naeem, Kashif Saleem, and Waseem Iqbal. Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure. In *E-health Networking, Application & Services (HealthCom), 2015 17th International Conference on*, pages 61–67. IEEE, 2015.

[37] Petr Kuznetsov and Rodrigo Rodrigues. Bftw 3: why? when? where? workshop on the theory and practice of byzantine fault tolerance. *ACM SIGACT News*, 40(4):82–86, 2010.

[38] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando Andr, and Paulo Sousa. Depsky: dependable and secure storage in a cloud-of-clouds. *ACM Transactions on Storage (TOS)*, 9(4):12, 2013.

[39] Dahlia Malkhi and Michael Reiter. Byzantine quorum systems. *Distributed computing*, 11(4):203–213, 1998.

[40] Subedari Mithila and P Pradeep Kumar. Data security through confidentiality in cloud computing environment. *Subedari Mithila et al,/(IJCSIT) International Journal of Computer Science and Information Technologies*, 2:1836–1840, 2011.

[41] Wenjun Luo and Guojing Bai. Ensuring the data integrity in cloud data storage. In *Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on*, pages 240–243. IEEE, 2011.

[42] Ari Juels and Alina Oprea. New approaches to security and availability for cloud data. *Communications of the ACM*, 56(2):64–73, 2013.

[43] Mohammed H Sqalli, Fahd Al-Haidari, and Khaled Salah. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, pages 49–56. IEEE, 2011.

[44] Ajey Singh and Dr Maneesh Shrivastava. Overview of attacks on cloud computing. *International Journal of Engineering and Innovative Technology (IJEIT)*, 1(4), 2012.

[45] Amin Panah, Amir Panah, Omid Panah, and Samere Fallahpour. Challenges of security issues in cloud computing layers. *Rep. Opin*, 4(10):25–29, 2012.

[46] Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pages 109–116. IEEE, 2009.

[47] Yinqian Zhang, Ari Juels, Alina Oprea, and Michael K Reiter. Homealone: Co-residency detection in the cloud via side-channel analysis. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 313–328. IEEE, 2011.

[48] Zhifeng Xiao and Yang Xiao. Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials*, 15(2):843–859, 2013.

[49] Eric Keller, Jakub Szefer, Jennifer Rexford, and Ruby B Lee. Nohype: virtualized cloud infrastructure without the virtualization. In *ACM SIGARCH Computer Architecture News*, volume 38, pages 350–361. ACM, 2010.

[50] Jakub Szefer, Eric Keller, Ruby B Lee, and Jennifer Rexford. Eliminating the hypervisor attack surface for a more secure cloud.

In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 401–412. ACM, 2011.

[51] Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar. Jackpot stealing information from large caches via huge pages. 2014.

[52] Gorka Irazoqui, Mehmet Sinan IncI, Thomas Eisenbarth, and Berk Sunar. Know thy neighbor: crypto library detection in cloud. *Proceedings on Privacy Enhancing Technologies*, 2015(1):25–40, 2015.