Memory Forensics in Multi-Tenant Cloud Environment

By

Hamaad Saeed

00000328827

Submitted to the Faculty of Department of Information Security Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Information Security

July 2022

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Hamaad Saeed**, Registration No. **00000328827**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor Dr. Mian M Waseem Iqbal

Date: 11/8/23

Signature (HOD): _____

HoD
Information Security
Military College of Sigs

Date: 11/8/23

Signature (Dean/Principal) _____

Date: 11/8/23

Brig
Dean, MCS (NUST)
(Asif Masood, Phd)

Declaration

I certify that this research work titled "Memory forensics in multi-tenant cloud environment" is my own work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged.

Hamaad Saeed
July 2023

Dedication

This thesis is dedicated to my Family, Teachers, and Friends

for their unconditional love, endless support, and continuous encouragement.

Acknowledgement

I would like to convey my gratitude to my supervisor, Dr. Mian Muhammad Waseem Iqbal for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis work are major contributions to the success of this research. Also, I would thank my committee members Dr. Faisal Amjad, Asst. Prof Waleed bin Shahid and Dr. Imran Makhdoom for their guidance and support.

I am also grateful to Saad Bin Khalid and Kamran Arshad who helped me to carry out my research work with ease.

Abstract

This research study aims to explore and analyze existing forensics techniques applicable to cloud computing, evaluate the security posture of a cloud service provider (CSP), and identify suitable security controls for multi-tenant cloud architectures. Forensic techniques are critical for investigating security incidents and cybercrimes in cloud environments, necessitating an understanding of their application, limitations, and challenges. Additionally, assessing the CSP's security posture involves evaluating current security controls, identifying vulnerabilities, and ensuring compliance with industry standards. The study focuses on multi-tenant cloud architecture, which presents unique security challenges due to shared resources and data across tenants. The identification and implementation of appropriate security controls, such as access controls, encryption, network segmentation, and regular security assessments, are essential to mitigate risks and safeguard data for each tenant. Conducting experiments revealed significant findings concerning system security and resource management. Non-compliance with access control measures for user accounts, the presence of Certificate Service Providers (CSP), and known vulnerabilities in the Open Source Xen hypervisor were identified. Resource availability limitations were also noted, impacting system performance and availability. As a recommendation, adopting a proprietary hypervisor across all instance classes is

proposed to ensure a consistent and secure virtualization environment. Addressing these findings and implementing necessary improvements can lead to enhanced system security, resource management, and overall performance. While capturing memory images from the cloud, integrity verification remains an unresolved challenge. Future research is encouraged to propose methods for ensuring the integrity of memory images in cloud forensics investigations.

Contents

1 Introduction **1**

1.1 Introduction 1

1.1.1 Cloud Architecture 2

1.2 Background 3

1.3 Problem Statement 4

1.4 Objectives 5

1.5 Relevance to National needs 5

1.6 Advantages 6

1.7 Delimitations 6

1.8 Areas of Application 6

1.9 Organization of Thesis 7

2 Literature Review **8**

2.0.1 Preliminary Knowledge 9

2.0.2 Related Work 13

3 Proposed Research Methodology **15**

3.1 Proposed System Architecture 16

3.1.1 Security Concerns 16

3.1.2 NIST 800-210 19

3.1.3 ISO/IEC 27017 19

3.1.4 ISO/IEC 27040 20

3.1.5 Memory Images Acquired 21

4 Experiments for Security Assessment of Cloud Memory **23**

4.1 Security Analysis 23

4.1.1 Tools Used 24

4.1.2 Case Studies 24

4.1.3 Purpose 29

4.1.4 Artifacts Recovered 29

5 Conclusion and Future Work **40**

5.0.1 Future Work 41

References **42**

List of Figures

3.1 Multi-tenant Cloud Architecture 17

3.2 Experiment Conducted 22

4.1 Overall Flow 30

List of Tables

4.1 Public Certificates Recovered 32

4.2 Ports Information Recovered 34

4.3 Instance Information 36

4.4 Access Logs 38

List of Abbreviations and Symbols

Abbreviations

AWS	Amazon Web Services
EC2	Elastic Compute Cloud
SSH	Secure Shell
DoS	Denial of Service
AVML	Acquire Volatile Memory for Linux
WinSCP	Windows Secure Copy
IT	Information Technology
IoT	Internet of Things
ISO	International Organization for Standardization
CAGR	Compound Annual Growth Rate
CSP	Cloud Service Provider

IEC	International Electrotechnical Commission
RBAC	Role-based access control
CVE	Common Vulnerabilities and Exposures
Att	Attacker
HTTP	Hyper Text Transfer Protocol
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
NIST	National Institute of Standards and Technology

Chapter 1

Introduction

1.1 Introduction

Cloud computing has emerged as a paradigm-shifting technology that is revolutionizing the way businesses and individuals' access and utilize computing resources. It has transformed the traditional approach of owning and managing on-premises hardware and software by providing access to computing resources and services through the internet. Cloud computing has brought a new level of flexibility, scalability, cost-efficiency, and agility to computing, enabling users to deploy and use services on-demand, pay-as-you-go, and with minimal upfront costs.

Cloud computing has become an essential technology for businesses and individuals, providing numerous benefits and advantages that have transformed the way we access, store, and use computing resources. The IT industry has been rapidly moving towards cloud computing in recent years, with a growing number of organizations adopting cloud-based solutions to drive innovation, agility, and cost-efficiency. Here are some

statistics that demonstrate the trend towards cloud adoption.

- According to Gartner, worldwide public cloud spending is expected to reach $332.3 billion in 2021, representing a 23.1% increase from 2020.
- A survey by Flexera found that 94% of organizations are using cloud services, with 87% using a multi-cloud strategy.
- The same survey found that 49% of cloud users spend over $1.2 million on cloud services annually.
- A report by IDC predicts that public cloud spending will grow at a compound annual growth rate (CAGR) of 22.3% from 2020 to 2025, reaching $500 billion by 2023.
- According to a survey by RightScale, 96% of respondents reported using cloud-based services, with 81% of enterprises operating a multi-cloud strategy.

These statistics demonstrate the rapid growth of cloud computing in the IT industry, as more organizations look to leverage cloud-based solutions to drive innovation, agility, and cost-efficiency. The trend towards multi-cloud adoption also indicates that organizations are seeking to take advantage of the unique features and benefits offered by different cloud providers to optimize their IT infrastructure.

1.1.1 Cloud Architecture

Multi-tenant and single-tenant are two cloud architecture models that define how resources are allocated and shared among users or tenants.

1.1.1.1 Multi-tenant Cloud Architecture

Multi-tenant cloud architecture is a model where multiple users, or tenants, share the same computing resources and infrastructure provided by a cloud service provider. In this model, each tenant has its own isolated environment within the shared infrastructure, and their data is segregated from other tenants. Multi-tenant architecture provides cost efficiencies, scalability, and flexibility to the users, as they pay only for the resources they use and can easily scale up or down as per their requirements. However, it also poses challenges related to security, privacy, and performance, as tenants share the same infrastructure.

1.2 Background

With the advancement of modern technology, the terms such as cloud, big data, and IoT emerging in every field of life. As cloud services increase, networking also changes and software-defined networks emerged. In contemporary networks, data and control planes are coupled together and we cannot integrate new network requirements (such as bandwidth utilization, quality of services, resiliency, security, and reliability) easily to provide flexibility and elasticity to different users. In traditional networks, devices (routers, switches) are closed configured and have the following drawbacks:

- Complicated network protocols are integrated within devices.
- Devices are exclusively manufactured so it is tedious to update or add functionality to them.

- Difficult to manage the requirement of integrating new devices.

With the evolution of cloud services, the facts listed above traditional networks are incapable of providing reliability, flexibility, and elasticity to the users that have been brought due to the IoT and Cloud services.

1.3 Problem Statement

The purpose of the study is to identify existing forensics techniques on the cloud, analyze the existing security posture of the cloud service provider (CSP), and determine which controls can be applied in multi-tenant cloud architecture.

Forensic techniques are essential for investigating security incidents, data breaches, and other types of cybercrimes that may occur in cloud environments. Therefore, it is important to identify the existing forensics techniques that are applicable to cloud computing, as well as any limitations or challenges that may be encountered when using them.

In addition, the study aims to analyze the existing security posture of the CSP. This includes evaluating the effectiveness of the security controls that are currently in place, identifying any vulnerabilities or gaps in the security architecture, and assessing the CSP's compliance with industry standards and best practices.

Finally, the study seeks to determine which controls can be applied in multi-tenant cloud architecture to ensure the security and privacy of data belonging to different tenants. Multi-tenant architecture presents unique security challenges due to the sharing of resources and data across multiple tenants. Therefore, it is important to identify and

implement appropriate security controls that can mitigate these risks and protect the data of each tenant.

Some of the controls that may be applied in multi-tenant cloud architecture include access controls, encryption, network segmentation, monitoring, and regular security assessments and audits. By identifying and implementing these controls, CSPs can improve the security posture of their cloud environments and provide greater assurance to their tenants that their data is being protected.

1.4 Objectives

Following are the objectives of this research:

- Literature review of current forensic techniques in cloud memory.
- Forensic analysis of the running cloud instances in multi-tenancy model to recover artifacts.

1.5 Relevance to National needs

The future of IT Industry will be entirely cloud-based, and under Pakistan's new cloud policy, all information pertaining to its residents must be stored there. This would require robust, highly available and especially secure cloud infrastructure designs. This research would help in understanding the cloud related security issues and would support in mitigating the issues before they arise.

1.6 Advantages

Some of the advantages of the proposed scheme are as follows:

- Detection of zero-day cloud security issues pertaining to memory.
- Proposing a solution to properly manage and secure a cloud's infrastructure memory.

1.7 Delimitations

Previous research has focused on cloud auditing using event logs, management of cloud logs, and identification of corresponding threats, but no research has been done on cloud memory analysis to the best of our knowledge. This study is solely based on detecting breaches of privacy and privileges in a multi-tenant cloud model by analyzing its memory.

1.8 Areas of Application

This proposed authentication scheme would assist all business sectors that may be impacted by cyber-attacks or targeted by cybercriminals.

- IT Sector
- Public Sector
- Government Sector

- Banking Sector

1.9 Organization of Thesis

- **Chapter 1:** is composed of the Introduction and background of the research.
- **Chapter 2:** consists of a literature review of the related studies.
- **Chapter 3:** comprises the proposed research methodology discussing the system architecture.
- **Chapter 4:** consists of the experiment conducted and their results.
- **Chapter 5:** comprises concluding remarks and future directions for research.

Chapter 2

Literature Review

Due to the significance of cloud computing, it is frequently targeted by cyber-attackers. Most cyber-attacks and data breaches in cloud infrastructure are due to human errors and misconfiguration vulnerabilities. While Cloud Service Providers (CSP) often provide several techniques to help manage cloud configuration. Misconfiguration of cloud resources remains the most widespread cloud vulnerability and can be exploited to access cloud data and services. The rapid pace of CSP innovation creates new functionality but it also adds complexity to securely configure an organization's cloud resources. Since many components comprising large-scale cloud data centers have a great number of configuration parameters, therefore, it gets difficult to keep consistencies in the configuration parameters. According to VMware [1], 49 percent of breaches are caused by system glitches and human errors, which prove that humans are the weakest link. Shared tenancy in the cloud is the ability to host multiple tenants on the same physical resources, by sharing physical storage, memory, and networks. Since users' data is stored in a shared machine in a shared tenancy model of CSPs, so the main focus of

this study aims to apply the forensic techniques on the shared machines to analyze the shared resources by extracting the artifacts and to evaluate the shared tenancy model of CSP, by analyzing the memory of an instance that is managed by CSPs between different tenants.

2.0.1 Preliminary Knowledge

2.0.1.1 Cloud Computing

Cloud computing is a technology that allows users to access and use computing resources, such as servers, storage, databases, applications, and services, over the internet. These resources are hosted on remote servers and are provided to users on a pay-as-you-go basis, meaning users only pay for what they use. Cloud computing is a way to provide users with access to computing resources without requiring them to invest in expensive hardware, software, or infrastructure. Instead, users can simply access these resources from the cloud provider over the internet, allowing them to scale their usage up or down based on their needs. Overall, cloud computing provides numerous benefits, including cost-efficiency, scalability, flexibility, reliability, and security, making it a popular choice for businesses and individuals alike.

2.0.1.2 Multi-Tenant Architecture

Multi-tenant cloud architecture is a model where multiple users, or tenants, share the same computing resources and infrastructure provided by a cloud service provider. In this model, each tenant has its own isolated environment within the shared infrastruc-

ture, and their data is segregated from other tenants. Multi-tenant architecture provides cost efficiencies, scalability, and flexibility to the users, as they pay only for the resources they use and can easily scale up or down as per their requirements. However, it also poses challenges related to security, privacy, and performance, as tenants share the same infrastructure.

2.0.1.3 NIST 800-210

NIST 800-210 is a special publication from the National Institute of Standards and Technology (NIST) titled "General Access Control Guidance for Cloud Systems". It provides guidance and recommendations for implementing access controls in cloud-based systems.

The publication is designed to help organizations that are migrating their IT systems and applications to the cloud to maintain the confidentiality, integrity, and availability of their information. It focuses specifically on access controls, which are a critical component of any information security program.

NIST 800-210 provides an overview of the access control concepts and principles that are applicable to cloud systems. It covers topics such as:

- Authentication and authorization
- Role-based access control (RBAC)
- Access control policies and procedures
- Network segmentation and isolation

- Monitoring and logging

The publication also provides guidance on how to implement these access control concepts in the cloud environment. It provides recommendations for cloud service providers (CSPs) and cloud customers, and includes examples of access control architectures and best practices.

Overall, NIST 800-210 is a valuable resource for organizations that are planning to implement cloud-based systems, or that are looking to improve their existing cloud security posture.

2.0.1.4 ISO/IEC 27017

ISO/IEC 27017 is a standard that provides guidelines for information security controls applicable to cloud computing. It is a part of the ISO/IEC 27000 family of standards, which are international standards that provide a framework for information security management.

ISO/IEC 27017 is designed to help organizations that are using cloud services to protect the confidentiality, integrity, and availability of their information. It provides guidance on the implementation of security controls that are specific to cloud computing, such as those related to virtualization, data segregation, and access control.

The standard covers a wide range of topics, including:

- Information security policies and procedures for cloud computing
- Managing risks associated with cloud computing

- Separation of duties between cloud service providers and cloud customers
- Monitoring and auditing of cloud services
- Business continuity and disaster recovery planning for cloud services

ISO/IEC 27017 is intended to be used in conjunction with other ISO/IEC 27000 standards, such as ISO/IEC 27001 (Information Security Management System) and ISO/IEC 27018 (Code of Practice for Protection of Personally Identifiable Information).

2.0.1.5 ISO/IEC 27040

ISO 27040 is an international standard that provides guidelines for the management of information security incidents and events. It is part of the larger ISO/IEC 27000 family of standards that covers various aspects of information security management systems.

The ISO 27040 standard provides a systematic approach to managing information security incidents, from the detection and analysis of incidents, through to their containment, eradication, and recovery. The standard outlines a set of processes, procedures, and guidelines for managing security incidents in a way that minimizes their impact and helps organizations to recover quickly and effectively.

The standard covers various aspects of incident management, including:

- Incident management policies and procedures
- Incident detection and analysis
- Incident response planning and implementation

- Containment and eradication of incidents
- Recovery and post-incident activities
- Incident reporting and documentation

By following the guidelines set out in ISO 27040, organizations can establish an effective incident management framework that helps to protect their information assets and minimize the impact of security incidents. The standard is applicable to organizations of all sizes and across all industry sectors, and can be used as a basis for developing and implementing an incident management program that is tailored to the specific needs and risks of the organization.

2.0.2 Related Work

Several digital forensic frameworks have been proposed by researchers and forensic practitioners. Various researchers have refined previously published processes and frameworks, as well as proposing new ones, resulting in a diverse set of digital forensic process models and terminology. According to a study which proposed and built a cloud data collection and rendering mechanism using the Hadoop file system. Saibharath et al. performed the pre-processing of the evidence files using log and VM disc drive clustering. It aided in reducing the time required for forensic inquiry [2]. Moreover, the correlation function between drives assisted investigators in performing cross drive analysis. Study addressed the issue of cloud evidence credibility, which occurs when evidence obtained in the cloud is untrustworthy due to its multi-tenancy and the various players in the forensic process. Fei et al [3] In this study, they proposed a new Cloud Forensics

Tamper-Proof Framework (TamForen) for cloud forensics that may be employed in an untrusted and multi tenancy cloud environment. Ameer [4]. addressed the challenges faced while gathering evidence from cloud.As the utilization of cloud computing continues to grow, new threats specific to the cloud environment have surfaced. The nature of cloud computing sets it apart from traditional systems, leading to distinct differences in cloud forensics. Over the past decade of research, several forensics challenges have been brought to the forefront, including issues related to trust, network forensics, evidence collection, privacy, and data provenance[5]. "Given the potential risks of data breaches in cloud-based applications, the current study aims to investigate and analyze residual registry artifacts left by the widely used cloud storage application, OneDrive, specifically on Windows 11 operating systems[6]. This research explores the existing practices in cloud forensics, fog forensics, edge forensics, and legal aspects, emphasizing the crucial role of cloud computing in digital forensics. Furthermore, we address the technical obstacles, limitations, and potential future advancements in this field[7]. An original proposal introduces a secure architecture for cloud forensics chain-of-custody investigations using Hyperledger Sawtooth. The concept involves establishing a private block-based ledger network among collaborators aiming to exchange and digitally sign various components of a forensics investigation. Additionally, the proposal suggests the implementation of chain codes to facilitate automated transactions within the chain of custody[8].

Chapter 3

Proposed Research Methodology

The study we're conducting is an experimental case study. The main objective of this section is to analyze the Multi-Tenant Cloud Architecture. Specifically, we want to uncover the truth about maintaining privacy in a cloud environment. We will be examining multiple aspects of cloud security. A multi-tenant cloud environment is a type of cloud computing architecture where multiple users or tenants share a single set of computing resources, such as servers, storage devices, and networks. Each tenant is typically isolated from the others, meaning that they have their own separate applications, data, and access controls. Multi-tenant cloud environments are commonly used for hosting Software-as-a-Service (SaaS) applications, where multiple customers use the same application and underlying infrastructure. By sharing resources, multi-tenant environments can provide significant cost savings and flexibility, as well as scalability and availability benefits. However, multi-tenant cloud environments also present unique security challenges, particularly with respect to data privacy and security. Because multiple tenants share the same resources, there is a risk that one tenant's data or

activity could be accessed or compromised by another tenant. Therefore, it is important for cloud service providers to implement strong security measures, such as access controls, encryption, and monitoring, to protect the privacy and security of their tenants' data. Additionally, tenants must also take responsibility for protecting their own data by implementing appropriate security controls and monitoring their own applications and systems.

3.1 Proposed System Architecture

Multi-tenancy is a cloud computing architecture where multiple customers, known as tenants, share computing resources such as servers, storage, and networking infrastructure provided by a cloud service provider (CSP). Each tenant's data and applications are logically isolated from other tenants, but they coexist on the same physical infrastructure

The architecture diagram for the proposed system is represented in Figure 3.1.

3.1.1 Security Concerns

Multi-tenancy is a cloud computing architecture where multiple customers, known as tenants, share computing resources such as servers, storage, and networking infrastructure provided by a cloud service provider (CSP). Each tenant's data and applications are logically isolated from other tenants, but they coexist on the same physical infrastructure.

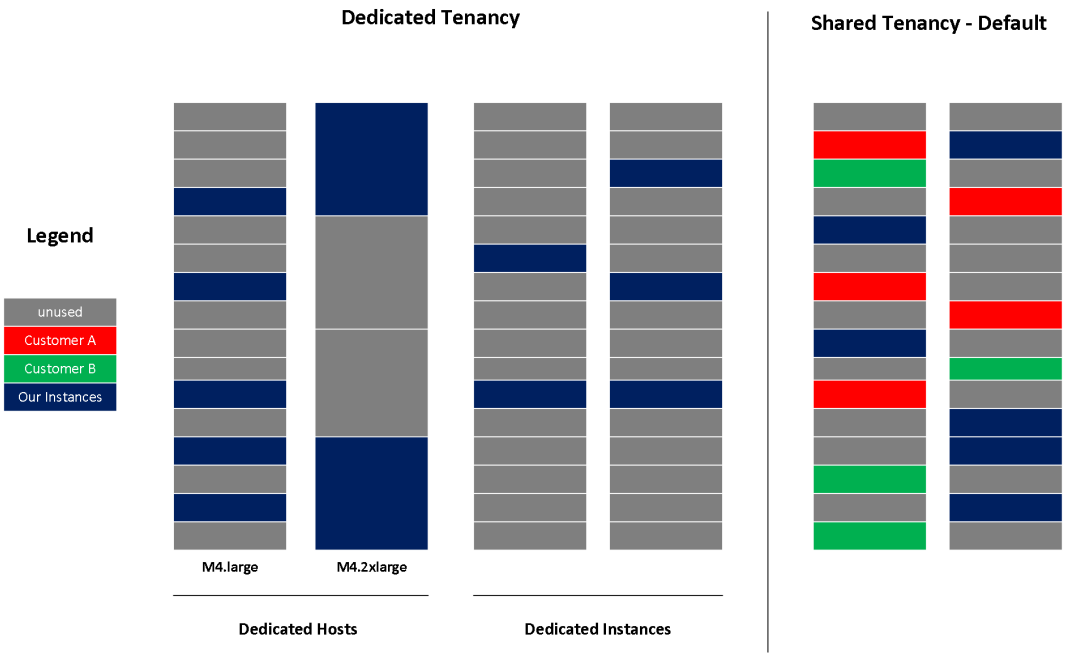

Figure 3.1: Multi-tenant Cloud Architecture

- Data Confidentiality: In a multi-tenant environment, there is a risk of unauthorized access to sensitive data by other tenants or malicious insiders. Strong access controls, encryption, and isolation mechanisms must be in place to protect the confidentiality of data.

- Data Segregation: Tenants' data should be properly segregated to prevent data leakage or accidental exposure. The CSP should implement robust mechanisms to ensure that tenant data remains isolated and that one tenant cannot access another tenant's data.

- Multi-Tenant Privilege Escalation: Unauthorized access or privilege escalation within the multi-tenant environment can lead to one tenant gaining access to another tenant's resources. Adequate isolation mechanisms and access controls must be implemented to prevent such incidents.

- Vulnerability Exploitation: If a vulnerability is discovered in the underlying infrastructure or shared components, it can potentially impact multiple tenants. The CSP should promptly patch vulnerabilities and implement strong security measures to minimize the risk of exploitation.

- Compliance and Regulatory Requirements: Different tenants may have specific compliance requirements, such as industry regulations or data protection laws. The CSP must ensure that their architecture and security controls comply with the relevant regulations and provide necessary compliance features to tenants.

- Denial of Service (DoS) Attacks: Malicious tenants or external attackers may attempt to launch DoS attacks, targeting shared resources to disrupt services for other tenants. Robust network monitoring, traffic isolation, and DoS prevention mechanisms should be implemented to mitigate such attacks.

- Insufficient Resource Allocation: Improper allocation of resources to tenants may result in resource contention and performance degradation. CSPs must carefully allocate and manage resources to ensure fair and efficient utilization among tenants.

To address these security concerns, CSPs must implement strong security measures, including network segregation, access controls, encryption, regular security audits, and monitoring. Tenants should also take responsibility for securing their applications and data within the multi-tenant environment by implementing proper access controls, encryption, and security best practices. It's important to note that while multi-tenancy introduces some security challenges, reputable cloud service providers invest heavily in

security measures to ensure the protection of their tenants' data and resources.

In light of the literature review, the following are the compliance requirements applicable to securing our architecture.

3.1.2 NIST 800-210

NIST 800-210, titled 'General Access Control Guidance for Cloud Systems,' is a special publication by the National Institute of Standards and Technology (NIST). This publication offers valuable guidance and recommendations for the implementation of access controls in cloud-based systems.

The primary purpose of this publication is to assist organizations in securely migrating their IT systems and applications to the cloud while ensuring the preservation of information confidentiality, integrity, and availability. It specifically emphasizes the significance of access controls as a crucial element within any comprehensive information security program.

3.1.3 ISO/IEC 27017

ISO/IEC 27017 is an internationally recognized standard within the ISO/IEC 27000 family of standards. It offers comprehensive guidelines for information security controls that are specifically tailored for cloud computing environments.

This standard is specifically designed to support organizations leveraging cloud services in safeguarding the confidentiality, integrity, and availability of their information. It provides valuable guidance on implementing security controls that are unique to cloud

computing, including areas such as virtualization, data segregation, and access control.

ISO/IEC 27017 serves as an essential framework for organizations seeking to establish robust security practices within their cloud-based operations, ensuring that appropriate measures are in place to address the specific challenges and risks associated with cloud computing.

3.1.4 ISO/IEC 27040

ISO 27040 is a globally recognized standard within the ISO/IEC 27000 family of standards, focusing on the management of information security incidents and events. This standard offers comprehensive guidelines for effectively handling and responding to security incidents.

As a part of the broader ISO/IEC 27000 family, ISO 27040 provides organizations with a structured approach to manage information security incidents throughout their lifecycle. From initial detection and analysis, to containment, eradication, and recovery, the standard establishes a systematic framework.

By outlining a set of processes, procedures, and best practices, ISO 27040 assists organizations in managing security incidents in a manner that minimizes their impact and ensures a swift and efficient recovery. It serves as a valuable resource to enhance incident response capabilities and strengthen overall information security management systems.

3.1.5 Memory Images Acquired

In a digital forensics analysis process, memories acquired from different states of a computing system can provide important insights into the system's behavior and state.

The four different scenarios that are commonly used to acquire memory data are:

- Fresh Machine: In this scenario, memory acquisition is performed on a newly created machine that has not been started or used before. This allows for the collection of a baseline memory image of the system before any other changes have been made.

- Stopping then running the instance: This scenario involves stopping an instance of a computing system, making changes, and then starting it again. Memory acquisition in this scenario would be used to capture the state of the system before and after changes have been made. This allows for the comparison of the two states and the identification of any differences or potential issues that may have arisen.

- Terminating the instance and creating a new instance: In this scenario, the original instance of the computing system is terminated, and a new instance is created. Memory acquisition in this scenario would be used to capture the state of the original instance before it is terminated and the state of the new instance after it has been created. This can be useful in identifying any changes or differences between the two instances.

- After running a process and restarting the instance: In this scenario, a process is

run on the computing system, and then the instance is restarted. Memory acquisition in this scenario would be used to capture the state of the system before and after the process has run. This can be useful in identifying any changes made by the process or any potential issues that may have arisen as a result of the process.

Overall, acquiring memory data in these different scenarios can help forensic analysts to identify potential security issues or malicious activities that may have occurred on the system. By analyzing the data from these different memory acquisitions, analysts can build a comprehensive understanding of the system's behavior and the events that have occurred on it.

The architecture diagram for the proposed system is represented in Figure 3.2.

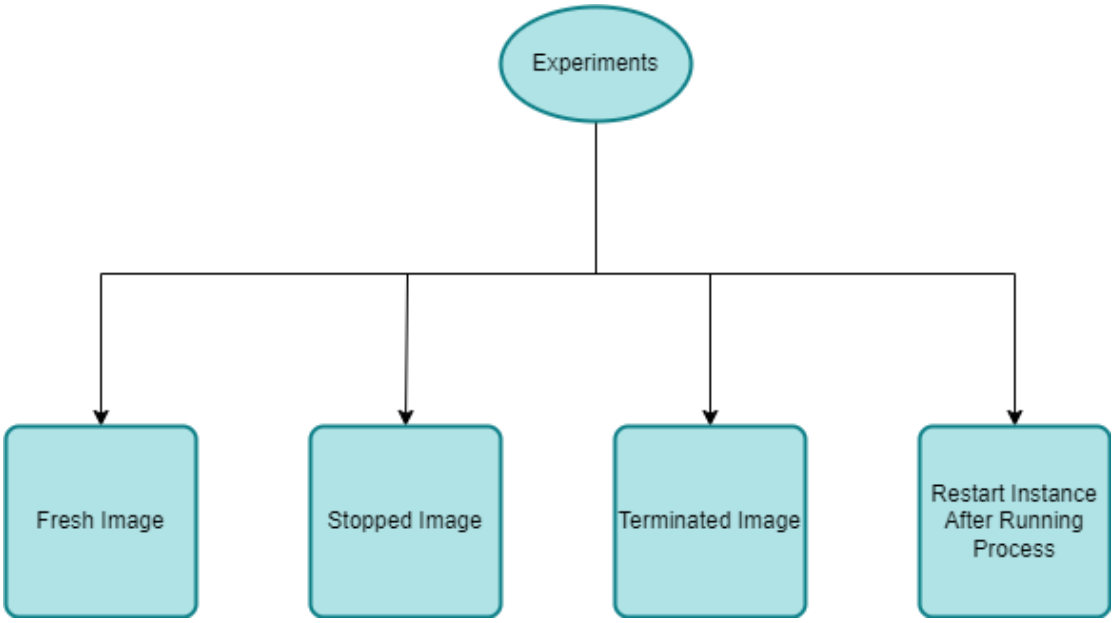

Figure 3.2: Experiment Conducted

Chapter 4

Experiments for Security Assessment of Cloud Memory

In this chapter, we present the experimental framework and methodology employed for assessing the security of cloud memory. Cloud computing has revolutionized the way data is stored, processed, and accessed, offering scalability and flexibility. However, the unique characteristics of cloud environments raise concerns regarding the security of sensitive information, particularly when it comes to memory storage.

4.1 Security Analysis

The primary objective of this research chapter is to conduct a comprehensive assessment of security measures implemented in cloud memory, focusing on potential vulnerabilities and associated risks. Through a series of controlled experiments, we aim to evaluate the effectiveness of existing security mechanisms, identify potential weaknesses,

and propose recommendations to enhance the protection of cloud memory.

4.1.1 Tools Used

- AVML (Acquire Volatile Memory Linux): This is a tool used to launch and manage virtual machines (VMs) for forensic analysis. It can be used to create VMs from forensic images or disk images, and to manage virtual networks and storage.
- Autopsy: This is a digital forensics platform that can be used to conduct a comprehensive analysis of a disk image. It includes a wide range of forensic tools and features, such as file carving, keyword searching, and hash matching.
- Coldsnap: This is a tool used to create snapshots of running virtual machines. It can be used to create forensic images of virtual machines in a multi-tenant cloud environment, which can then be analyzed using other forensic tools.
- WinSCP: This is an open-source FTP client and SFTP client that can be used to securely transfer files between systems. It can be used to transfer forensic images or data from a cloud service provider to a forensic analyst's system for analysis.

4.1.2 Case Studies

4.1.2.1 Fresh Instance Memory

our experiment began by creating a fresh AWS account. Once the account was set up, we proceeded to log in to the AWS Management Console. Within the console, we created a new EC2 (Elastic Compute Cloud) instance, which is a virtual server in the AWS

infrastructure. After creating the instance, we took a snapshot of it without accessing the instance itself. This snapshot captured the state of the instance at that particular moment. We used a tool called "coldsnap" to download the snapshot to our local system. Next, we performed an analysis of the snapshot using a forensic tool called "Autopsy." This analysis aimed to gather various types of evidence from the snapshot, providing insights into the instance's activities and configurations. In the subsequent step, we accessed the EC2 instance using the secure shell (SSH) protocol, which allowed us to establish a secure connection to the instance. Once connected, we used a tool called "AVML" to capture a complete image of the Random Access Memory (RAM) of the instance. The RAM image contains volatile data, such as running processes and data in memory, which can be valuable for forensic analysis. To facilitate further analysis, we downloaded the captured RAM image from the instance to our local system using the "WinSCP" tool. This image was then analyzed once again using the "Autopsy" tool, which enabled us to extract and examine additional evidence from the RAM data. By following these steps, we aimed to comprehensively investigate the instance and gather relevant evidence from both the snapshot and the captured RAM image for further analysis and forensic examination.

4.1.2.2 Restarting the Instance

In this case study, the focus was on examining the impact of stopping and restarting an AWS instance on the forensic analysis process. The following steps were performed:

- Initially, an instance was created in the AWS environment, similar to the previous case.

- After the instance was created, researchers executed the "stop" operation to temporarily halt the instance's execution. They then waited for a brief period to ensure the instance was completely stopped.

- Subsequently, the instance was restarted, resuming its normal operation.

- Once the instance was running again, researchers established an SSH connection to access the instance remotely.

- With SSH access established, researchers utilized the "AVML" tool to capture a RAM image of the running instance. This step aimed to extract volatile data stored in the instance's memory, including running processes and other valuable information.

- The captured RAM image was downloaded from the running instance to the researchers' local system using the "WinSCP" tool. This facilitated secure transfer of the image for subsequent analysis.

- Finally, the downloaded RAM image was subjected to analysis using the "Autopsy" tool, allowing researchers to delve into the contents of the RAM data and extract relevant evidence.

The objective of Case study was to investigate how stopping and restarting an instance might impact the forensic analysis process. By performing these specific actions and capturing a RAM image after the instance had been stopped and restarted, researchers could assess any potential changes or differences in the acquired evidence compared to the previous case. The analysis of the RAM image using "Autopsy" enabled re-

searchers to identify and extract additional evidence, providing insights into the state of the instance after the restart. This evaluation contributes to the understanding of the implications of instance operations on the forensic investigation process, aiding in the development of more comprehensive and accurate forensic methodologies in cloud computing environments.

4.1.2.3 Terminating the Instance

In this case study, the objective was to examine the impact of terminating an AWS instance and creating a new one on the forensic analysis process. The following steps were carried out:

- Initially, an instance was created in the AWS environment, similar to the previous cases.
- After the instance was created and had undergone the necessary operations, the researchers proceeded to terminate (delete) the instance. They waited for a brief period to ensure the termination process was completed.
- Following the termination of the earlier instance, researchers created a new instance in the AWS environment.
- Once the new instance was created, researchers took a snapshot of the instance without accessing it directly. This snapshot captured the state of the instance at that particular moment.
- The researchers utilized the "coldsnap" tool to download the snapshot of the new

instance to their local system. This allowed them to obtain an offline copy of the snapshot for subsequent analysis.

- The downloaded snapshot was then analyzed using the "Autopsy" tool. This analysis aimed to gather various forms of evidence from the snapshot, such as file system information, user activity, and system configurations.

- Researchers then established an SSH connection to the new instance, enabling them to access it remotely.

- With SSH access established, researchers employed the "AVML" tool to capture a RAM image of the running instance. The RAM image contained volatile data, including active processes and data stored in the instance's memory.

- The captured RAM image was downloaded from the running instance to the researchers' local system using the "WinSCP" tool, ensuring secure transfer for subsequent analysis.

- Finally, the downloaded RAM image was analyzed once again using the "Autopsy" tool. This analysis allowed researchers to extract and examine additional evidence from the RAM data.

The purpose of Case Study was to assess the implications of terminating an instance and creating a new one on the forensic analysis process. By examining the snapshots and capturing RAM images from the new instance, researchers could investigate any potential differences or variations in the obtained evidence compared to previous cases. This analysis contributes to understanding the impact of instance life cycle events on

forensic investigations in cloud computing environments, facilitating the development of more robust and accurate forensic methodologies.

The architecture diagram for the proposed system is represented in Figure 4.1.

4.1.3 Purpose

The experiments allows researchers to examine the challenges and opportunities associated with forensic analysis in cloud environments, with specific emphasis on AWS. It offers insights into the methods and tools used to gather and analyze evidence, assess the impact of instance operations (such as stopping, restarting and terminating), and evaluate the effectiveness of different tools in extracting and interpreting data. Through this research case study, researchers can contribute to the advancement of forensic techniques in cloud computing, identify potential limitations or improvements in existing methodologies, and provide recommendations for enhancing the forensic investigation process in cloud-based infrastructures. The findings from this case study can serve as a valuable reference for practitioners and organizations involved in digital forensics and cloud security.

4.1.4 Artifacts Recovered

During a comprehensive analysis of a RAM dump, a total of 1662 artifacts were successfully recovered, shedding light on various aspects of the system's activities. Notably, it is important to highlight that all recovered artifacts originated from volatile memory, as no items were retrieved from the system's disk storage. The artifacts en-

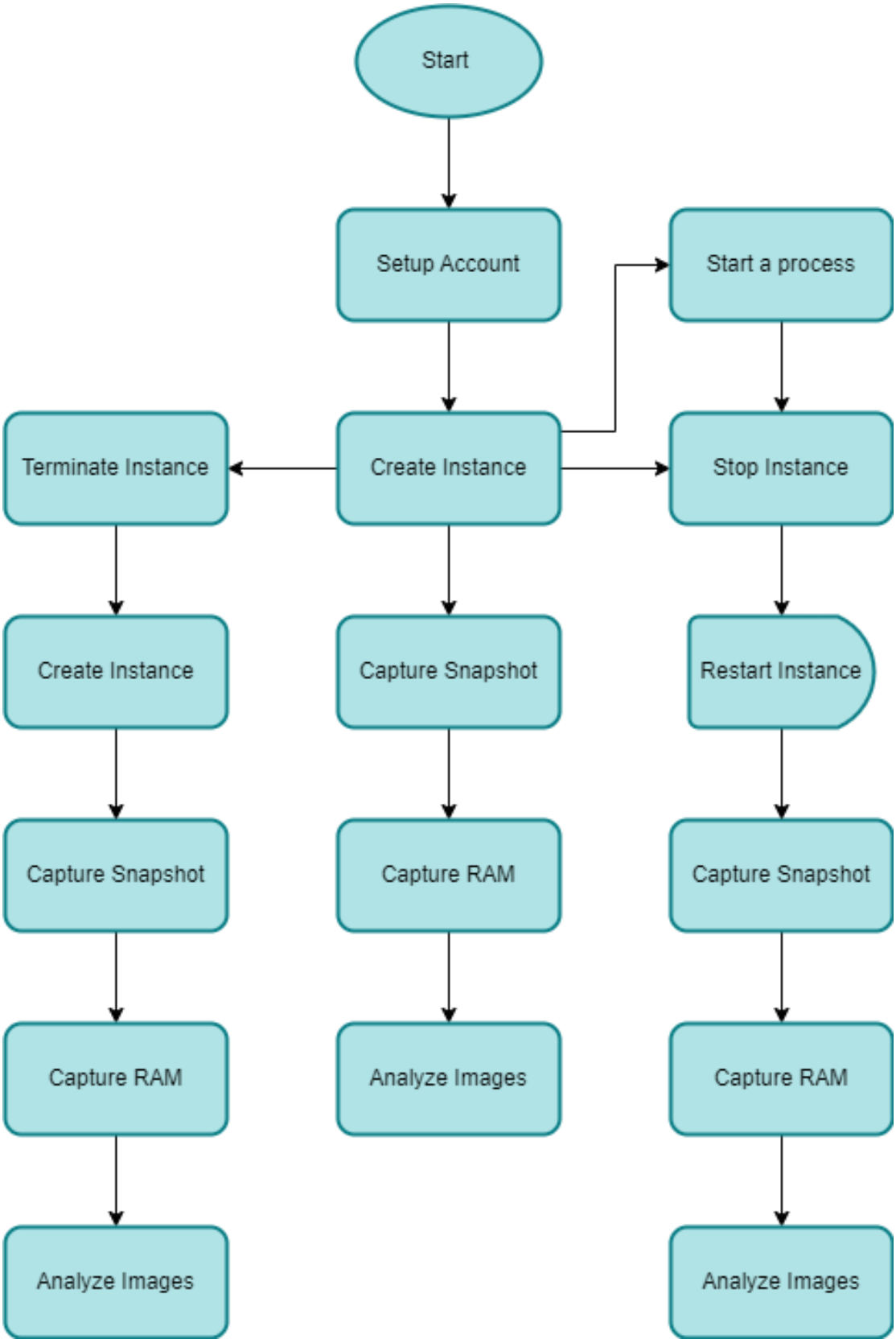

Figure 4.1: Overall Flow

compass three primary categories: Public Certificates, Access Logs, and Active Processes.

A substantial collection of public certificates was extracted from the RAM dump as shown in 4.1. These certificates, which are cryptographic documents used for secure communication and authentication, are indicative of the system's involvement in secure transactions, network communications, or cryptographic processes. Thorough analysis of these certificates may reveal insights into the system's network connections, security protocols, and potential third-party integrations.

File	File Path	Size	MD5 Hash
f1526530.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1526530.txt	3204	d78f06aa2ec4005079aad3071afe3b6b
f1286437.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1286437.txt	30272	f837d5eadbcf2fb6ec5eb565b22436c6
f1294819.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1294819.txt	31300	f7d95eb67e8178182598dc14dacd3502
f1296489.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1296489.txt	28227	2052438ba5672f570a2303c826ee43a5
f1303586.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1303586.txt	45652	a053eef5db2ed231af6210da1c19c897
f1304865.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1304865.txt	26890	c4defe22f93defeeffb78668b79e7223
f1526945.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1526945.txt	7747	4511537af7cdce445c16712c27f03707
f1527033.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1527033.txt	3648	8d0d212460501699a21ad1441d581700
f1527291.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1527291.txt	2624	d30477f08470d35e8e85acca34811e7d
f1527881.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1527881.txt	13460	dac84669f563fe9d9cc7f0dc4344425d
f1528545.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1528545.txt	32320	5fc1a044a0e825e8e4c7dfd3ff7763d7
f1538433.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1538433.txt	7744	efd7416d8deee0a8499d9f95f010f186
f1541765.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1541765.txt	5701	f82d63be603cbc61fc0c2f8d153d4150
f1541874.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1541874.txt	3200	a185f0308b8a63aea3aa1de0e783c6b2
f1547345.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1547345.txt	7746	8dd399ea4ed47dc80b9f1642f016c2b1
f1572105.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1572105.txt	11849	72d116d47b428a4b7c73855f18134528
f1575249.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1575249.txt	7744	44dcf7bb36611022afb896ef0eb8544c
f1576039.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1576039.txt	643	a693e223fc75675d1c30d15bff399168
f1576558.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1576558.txt	1088	879fd45e8f78ab130623a47f6e6ad85b
f1587937.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1587937.txt	14666	79cf7eae376e3546a8de2a7e29cbbdcb
f1606188.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1606188.txt	2112	dfbac9ddc7b7b5871e023bacd2ebf761
f1607772.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1607772.txt	2115	1a114bad9b214f4e4a90944227ca7d83
f1607800.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1607800.txt	4163	648954001c31da5fc30d28eeae0b349b
f1607827.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1607827.txt	2624	41e5fa861ac8b12909cbcc6a1c36ced7
f1608177.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1608177.txt	3648	b1da8c24a981585d05f2958927b61190
f1608193.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1608193.txt	3648	fd8a810734c2d92a3a06f47bc5ee1ce3

Table 4.1: Public Certificates Recovered

Among the recovered artifacts to active processes running within the system's memory as shown in 4.2. These processes represent the currently executing programs and applications at the time of the RAM dump. Studying these artifacts can offer a glimpse into the system's real-time activities, resource utilization, and potentially malicious activities. By identifying and examining these active processes, researchers can gain deeper insights into the system's functionality and potential vulnerabilities.

File	File Path	Size	MD5 Hash
f1555617.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1555617.txt	3821	62151b885d012af0b476cee0421f7ccb
f1561649.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1561649.txt	3648	3ebe6f87dbebd45aa1cecf10c986d2ff
f1561977.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1561977.txt	3650	fdb560cb6e567db39a92de4493ecd210
f1562105.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562105.txt	3648	0652bc78d3f62171a27235b4d594a880
f1567745.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1567745.txt	3713	422fab6d1e40c7e73f1bada6eb0b5b11
f1632329.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1632329.txt	7744	80a72f1c56a7cb1e742e53d896f2da6e
f1633609.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1633609.txt	3648	770c7935fd8fc132a8e4e90c334b7b60
f2034337.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2034337.txt	3712	a9d930da0c1daf5901bdb7d5958a5e2a
f2034545.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2034545.txt	15936	baa05d186306ace82b04be5fef8663e1
f2080145.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2080145.txt	7744	f8504507c35a9f9a101b2318f6b59f01
f2081697.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2081697.txt	7744	008eeff569b8dcb3b18f760fdcf37e4a
f2083153.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2083153.txt	3714	250786f5f1399156c94e950c65a29f20
f2084161.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2084161.txt	7747	ff3a562107eaad6b573b0f8ec9941850

Table 4.2: Ports Information Recovered

Within the analyzed RAM dump, a collection of artifacts pertaining to running virtual machine instances was discovered as shown in 4.3. These instances represent actively executing virtualized environments within the system's volatile memory. Each virtual machine instance artifact provides valuable insights into the system's utilization of virtualization technology and its impact on system operations.

File	File Path	Size	MD5 Hash
f1517401.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1517401.txt	2316	db6fdbeb6067b9a5f41b7c04f9f04c18
f1520249.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1520249.txt	3650	7ed235d94261e1b0b4e995583add5aa0
f1529649.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1529649.txt	2316	db6fdbeb6067b9a5f41b7c04f9f04c18
f1562705.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562705.txt	1104	acc3cd55a0650ae5aa05bd3a1a1c2e73
f1562708.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562708.txt	426	788cc371951d6a1e26b6b8b94919930a
f1562709.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562709.txt	1017	101f1227ca4157001ca8dc26f2348c16
f1562712.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562712.txt	131	48c3e43d618a9e35a9f8728d340ce13e
f1583349.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1583349.txt	129	a0ec06597327e63fe386fb0fc390fdf7
f1591545.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1591545.txt	3648	762779af93f3f612c1041e95c3b7b5d9
f1623033.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1623033.txt	1067	dae8278ad322041df3e67b5cb8fba415
f1623037.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1623037.txt	1603	01bf01f98400c44a96f1d8692e35308b
f1624001.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1624001.txt	2524	0c85ff0bcfd866d14deb6a73c0c6c5bf
f1624006.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1624006.txt	1155	7fafc88fc42131a93ed76661cac50ec9
f1634761.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1634761.txt	3649	de5735f5d6c5f3adf78215ea752216b0
f2032145.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2032145.txt	3713	165cb3dcf7c561a3974815c38ca83814
f2083001.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2083001.txt	3681	08f841dc2d0adde39741e741e396f4e3
f2084105.txt	/img_46.137.237.18.dmp/$CarvedFiles/f2084105.txt	3713	784b920f7a2dee9398fa7a3b422e26e6

Table 4.3: Instance Information

The RAM dump yielded a significant set of access log artifacts as shown in 4.4. These logs record instances of user or system interactions with various resources, applications, or services. Analysis of these access logs could provide a comprehensive overview of user activities, attempted unauthorized accesses, and patterns of system usage. Valuable insights into the operational history and potential security breaches may be derived from this collection.

File	File Path	Size	MD5 Hash
f1530361.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1530361.txt	3648	417aeea65cbf6acb98413d7b6a90eca1
f1530361.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1530361.txt	3648	417aeea65cbf6acb98413d7b6a90eca1
f1543905.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1543905.txt	3649	46e33e72886ceb78e36f17d1ca6f3f36
f1544649.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1544649.txt	1798	d1801d201a8e3b3ad8f645574ebef502
f1555148.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1555148.txt	2064	eb00a9a0b392690cf26fa4b9a3f384a9
f1562545.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1562545.txt	3712	388512192f558695e2bad6f75ad535ed
f1580273.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1580273.txt	133	46747b30a0c8de69dc65e157867eba32
f1580706.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1580706.txt	608	c25f22a1b9673f61b828aae6df06a927
f1581665.txt	/img_46.137.237.18.dmp/$CarvedFiles/f1581665.txt	934	f8efaa8595b4c0687f4f778020bf1117

Table 4.4: Access Logs

In conclusion, the analysis of the RAM dump yielded a rich array of 1662 artifacts, encompassing Public Certificates, Access Logs, and Active Processes. These artifacts provide a snapshot of the system's activities and may hold valuable information regarding network interactions, user behaviors, and potential security risks. Further in-depth examination of these artifacts is recommended to unveil a comprehensive understanding of the system's operational landscape and to facilitate potential security enhancements.

Chapter 5

Conclusion and Future Work

During my experiments, I made several significant findings regarding the system's security and resource management. Firstly, I discovered that Coldsnap is currently non-compliant with access control measures for user accounts, potentially posing a security risk. Additionally, while conducting an autopsy of the system, I came across certificates containing both public and private keys, indicating the presence of Certificate Service Providers (CSP).

In terms of resource allocation, I noticed that the CSP provides 100% resource availability for a specific time period. However, once the resources are fully utilized, the service halts for a certain duration, which could impact the system's performance and availability. Furthermore, I observed that the system uses Open Source Xen hypervisor whose source is available to everyone, which has known vulnerabilities (CVE), raising concerns about the overall security posture.

As a recommendation, I propose that AWS should adopt their own hypervisor across all instance classes to ensure a more consistent and secure virtualization environment. By

addressing these findings and implementing necessary improvements, the system can enhance its security, resource management, and overall performance, leading to a more robust and reliable infrastructure.

5.0.1 Future Work

In my current research, I have captured memory images from the cloud without physically access and addressed the challenges encountered during the analysis of these images on the cloud. However, there is currently no way to verify the integrity of these memory images. Future studies may propose methods to ensure the integrity verification of memory images.

References

[1] VMWare. Hybrid cloud architecture. https://www.vmware.com/topics/glossary/content/hybrid-clo 4:1583–1594, 2021.

[2] Geethakumari G. Saibharath, S. Cloud forensics: evidence collection and preliminary analysis. IEEE International Advance Computing Conference, 2015:464–467, 2015.

[3] Zheng Y. Fu X. Luo B. Du X. Guizani M. Ye, F. Tamforen: a tamper-proof cloud forensic framework. Transactions on Emerging Telecommunications Technologies, 33:3, 2022.

[4] Lazarescu M. Soh S. T Pichan, A. Cloud forensics: Technical challenges, solutions and comparative analysis. Digital investigation, 13:38–57, 2015.

[5] Sudha T. Bai, V. S. A systematic literature review on cloud forensics in cloud environment. International Journal of Intelligent Systems and Applications in Engineering, 11:565–578, 2023.

[6] Mishra S. Bajahzar, M. Cloud forensic artifacts: Digital forensics registry artifacts

discovered from cloud storage application. International Journal of Computing and Digital Systems, 14:1–xx, 2023.

[7] Shaikh A. A. Laghari A. A. Rind M. M. Khan, A. A. Cloud forensics and digital ledger investigation: a new era of forensics investigation. International Journal of Electronic Security and Digital Forensics, 15:1–23, 2023.

[8] Laghari A. A. Kumar A. Shaikh Z. A. Baig U. Abro A. A. Khan, A. A. Cloud forensics-enabled chain of custody: a novel and secure modular architecture using blockchain hyperledger sawtooth. International Journal of Electronic Security and Digital Forensics, 15:412–423, 2023.