Live VM Backup and Recovery: Design a system that can take real-time backups of VMs and ensure quick recovery, all while maintaining a strong security posture

Submitted in partial fulfilment of the **CAPSTONE PROJECT** in VIRTUALIZATION TECHNOLOGY, which is a part of

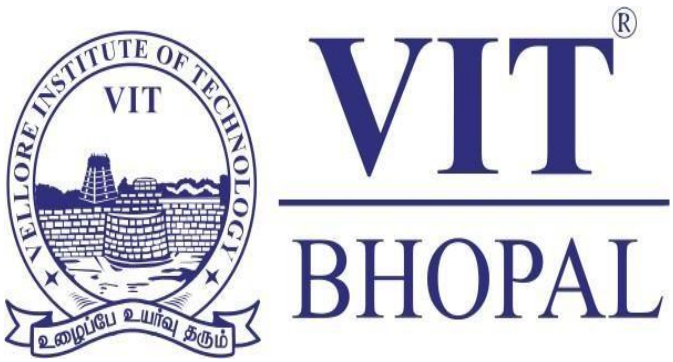
Integrated M. Tech. in Cybersecurity

By

Seyan Michael	Shraddha Pandey	Narendra Kumar Patel	Khushbu Dadhe	Apporv Kumar
20MEI10020	20MEI10029	20MEI10039	20MEI10041	20MEI100058

Submitted to

Dr. Hemraj S. Lamkuche



School of Computing Science and Engineering,VIT Bhopal University, Madhya Pradesh India

October 2023

Motivation

Securely In the context of cloud computing, VM migration is critical. For starters, it reduces the risk of being compromised by external threats. When we migrate a VM file from one server to another or from one internet to another, we need a security posture to secure it. There is one solution to this problem: use encryption and decryption. We intended to use both types of encryption and decryption processes in this project at the same time.
Thanks!

Capstone Project Approval

This is to certify that the Integrated M. Tech. Capstone Project report titled" **Live VM Backup and Recovery: Design a system that can take real-time backups of VMs and ensure quick recovery, all while maintaining a strong security posture."** By **Seyan Michael** (**20MEI10020) Shraddha Pandey (20MEI10029), Narendra Kumar Patel (20MEI10039), Khushbu Dadhe (20MEI10041), Apoorv Kumar (20MEI10058)** is approved for the degree of **Integrated M. Tech. in Cybersecurity**.

Dr. Hemraj S. Lamkuche
(Course Coordinator)

Date: 23-10-2023
Place: Bhopal

Declaration

We members of Group 7 declare that this written submission represents our ideas in our own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any ideas, data, facts or sources in our submission. We understand that any violation of the above will bethe cause of disciplinary action by the institute and evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Date:10-10-2023
Place: Bhopal

Author(s): Seyan Michael, Shraddha Pandey, Narendra Kumar Patel, Khushbu Dadhe, Apoorv Kumar

Registration number(s) 20MEI10020 20MEI10029, 20MEI10039, 20MEI10041, 20MEI10058

Abstract

Securely VM migration is important in the context of cloud computing. For starters, it reduces the risk of being compromised by external threats. When we migrate a VM file from one server to another or from one internet to another, we need a security posture to secure it. There is one solution to this problem: use encryption and decryption. We intended to use both types of encryption and decryption processes in this project at the same time. Moving VM files between systems exposes us to numerous security threats and attacks. The goal of this project is to develop an application that encrypts VM files using double encryption, which includes symmetric and asymmetric components, at the sender end before sending it to the receiver, where it can be decrypted and used in a similar fashion. For achieving this goal, we are using the RSA algorithm for asymmetric encryption and the AES (Advanced Encryption Standard) algorithm for symmetric encryption. As a result, we successfully created the application we have created a working application that can conduct double encryption and decryption using asymmetric and symmetric algorithms, and we can transfer it over the intranet in a secure manner. We are now intending to create an application that will provide security so that we can send it from one internet to another.

Table of Contents

List of Figures

Chapter 1

Introduction

Introduction: When we are migrating a VM file from one server to another, we must do so securely so that we do not encounter any problems. In this section, we will refresh our memories with definitions such as-

1.1.1 What is Virtual Machine?

A virtual machine (VM) is a virtual environment that works as a virtual computer system with its own CPU, memory, network interface, and storage, generated on a physical hardware system (located off- or on-premises). It makes use of hypervisor software, which separates the machine's resources from the hardware and properly configures them for use by the VM. The hypervisor views compute resources—such as CPU, memory, and storage—as a pool of resources that can be easily relocated between existing guests or to new virtual machines, and virtualization is a technology that allows you to create useful IT services using resources that were previously bound to hardware. It enables you to exploit a physical machine's full capability by distributing its capabilities across multiple users or settings.

1.1.2 VM Architecture:

Figure 1: VM Architecture

1.1.3 Types of Virtual Machine:

Virtual machines are classified into two groups based on their functions: system virtual machines and process virtual machines.

i. **System Virtual Machines:** These VMs allow complete virtualization. These will provide functionalities to execute a whole operating system by acting as a substitute for the real machine. Hardware resources are shared and managed, resulting in the formation of several environments on the host system. These environments are separate but live on the same physical host. As a result, these enable time-sharing among many single-tasking operating systems. Memory pages with the same content can be shared among many virtual machines running on the same physical host. This is very helpful for read-only pages.

ii. **Process Virtual Machines (VM):** This sort of VM operates as a standard application within the host's operating system, supporting a single process. It is

produced at the start of the process and destroyed when the procedure is completed. It is used to give the process with a platform-independent programming environment, allowing it to run on any of the other platforms. All operating system services are available to the application running on these VMs. These virtual machines (VM) include the parallel virtual machine and the message passing interface.

1.1.4 How does virtualization function?

Hypervisors in virtualization software separate physical resources from virtual environments—the entities that use those resources. Hypervisors divide our physical resources so that virtual environments can utilise them, and they can be partitioned from the real environment to the various virtual environments as needed. Users interact with the virtual environment (also known as a guest computer or virtual machine) and conduct calculations within it. The virtual machine is implemented as a single data file. And, like any digital file, it may be transferred from one computer to another, opened in either, and expected to function the same way. When a user or program issues an instruction that requires additional resources from the physical environment, the hypervisor relays the request to the physical system and caches the changes—all at close to native speed (especially if the request is sent through an open-source hypervisor based on KVM, the Kernel-based Virtual Machine).

1.1.5 Types of virtualizations:

i. **Data Virtualization:** Data virtualization enables businesses to approach data as a dynamic supply, allowing them to combine data from numerous sources, readily adapt new data sources, and alter data based on user requirements.

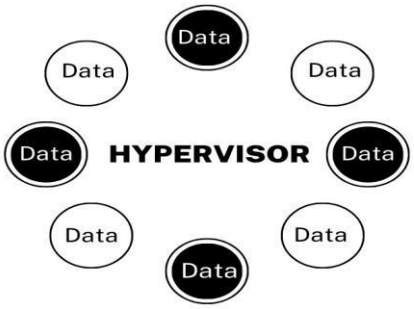


Figure 2: Data Virtualization

ii. **Desktop Virtualization:** Desktop virtualization enables a central administrator (or automated administration tool) to distribute simulated desktop environments to hundreds of actual workstations at the same time.

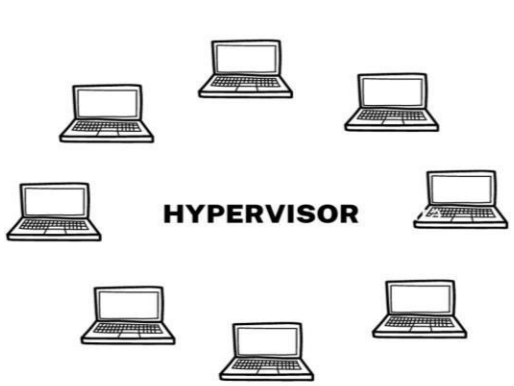


Figure 3: Desktop Virtualization

iii. **Server virtualization:** Servers are computers that are meant to perform a high volume of certain operations efficiently so that other computers, such as laptops and desktops, can perform a range of other jobs. Virtualizing a server allows it to perform more of those specialized functions by splitting it so that the components can fulfil numerous roles.

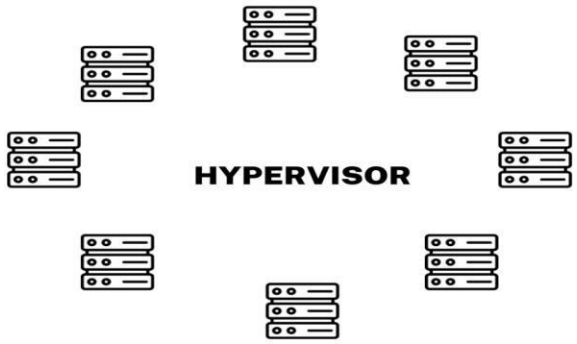


Figure 4: Server Virtualization

iv. **Operating System Virtualization:** Operating system virtualization occurs in the kernel, which is the central task manager of operating systems. It is a convenient technique to run Linux and Windows environments concurrently.

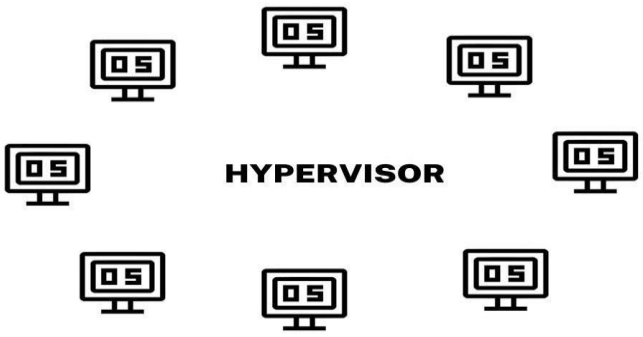


Figure 5: OS Virtualization3

v. **Network Function Virtualization:** Network functions virtualization (NFV) separates the main functions of a network (such as directory services, file sharing, and IP setup) so that they can be spread across environments. Virtualizing networks minimizes the number of physical components required to construct several, independent networks, such as switches, routers, servers, cables, and hubs, and it is especially popular in the telecommunications industry.

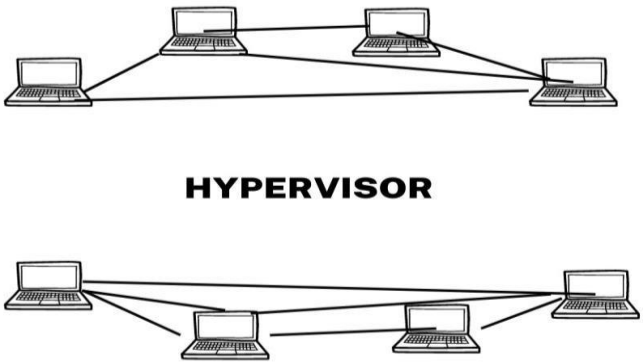


Figure 6: Network Function Virtualization

1.1.6 Common Vulnerabilities in VM:

Some virtual machine, or VM, assaults are variations on traditional threats such as denial of service. Others are still entirely hypothetical, but they are likely to become a reality as hype and resources grow. Keep a look out for the following key flaws:

i. **VM sprawl:** As VMs are simple to deploy, many organizations regard them as hardware-like tools that do not require formal policies. This has resulted in VM sprawl, or the unintentional proliferation of VMs. Attackers can exploit poorly monitored resources. More deployments entail more failure points; therefore, sprawl can cause issues even when there is no malice involved.

ii. **Hyper jacking:** It takes control of the hypervisor to obtain access to the VMs and their data. It is primarily launched against type 2 hypervisors that run on a host OS, while type 1 assaults are potentially viable. Due to the difficulty of directly accessing hypervisors, hyper jackings are uncommon. However, hype jacking is a real-world issue, and administrators should go on the offensive and prepare for it.

iii. **VM escape:** A guest OS breaks free from its VM encapsulation to connect directly with the hypervisor. This grants the attacker access to all VMs and, if guest privileges are high enough, the host machine as well. Although few if any incidents are recorded, experts believe VM escape to be the most danger to VM security.

iv. **Denial of service attacks:** Denial of service attacks, which range from overwhelming a network with traffic to clever exploitation of a host's own resources, are common. The availability of botnets makes it easier for attackers to launch campaigns against specific servers and applications to disrupt the target's online services.

v. **Incorrect VM isolation:** To be secure and exchange resources effectively, VM must be isolated from one another. Inadequate control over VM deployments can result in isolation breaches when VMs communicate. This virtual drawbridge can be used by attackers to obtain access to many guests and possibly the host.

vi. **Unsecured VM migration:** Unsecured VM migration occurs when a VM is moved to a new host without security policies and settings being changed to reflect the change. The host and any visitors may become more susceptible as a result. Attackers have an edge because administrators are likely ignorant that they have introduced vulnerabilities and will not be on the lookout for them.

vii. **Vulnerabilities caused by hosts and guests:** Host and guest interactions can amplify system vulnerabilities at numerous points. Their operating systems, particularly Windows, are likely to be riddled with flaws. They, like other computers, are vulnerable to flaws in email, Web surfing, and network protocols. However, because of virtual interconnections and the co-hosting of many data sets, a severe attack on a virtual environment is especially harmful.

1.1.7 Securing the VM:

i. **VM Traffic Monitoring:** It is vital to be able to monitor VM backbone network activity. Because VM traffic is controlled by internal soft switches, conventional approaches will not discover it. However, hypervisors provide effective monitoring tools that should be enabled and evaluated.

ii. **Administrative control:** Secure access can be jeopardized owing to VM sprawl and other factors. Ensure that authentication, identity management, and logging procedures are foolproof.

iii. **Customer Security:** Outside of the VM, ensure that customer-facing interfaces such as websites are protected.

iv. **VM segregation:** In addition to standard isolation, functional segregation can help to improve VM security. Consider building different security zones for desktops and servers. The purpose is to minimize junction points as much as possible.

1.1.8 What is VM migration?

The task of migrating a virtual machine from one physical hardware environment to another is known as virtual machine migration. It is part of managing hardware virtualization systems and is something that providers consider when offering virtualization services.

1.2 Objective of Our Project:

Nowadays, moving VM files between systems exposes us to numerous security threats and attacks. The goal of this project is to develop an application that encrypts VM files using double encryption, which includes symmetric and asymmetric components, at the sender end before sending it to the receiver, where it can be decrypted and used in a similar fashion. In this project, we are using the RSA algorithm for asymmetric encryption and the AES (Advanced Encryption Standard) algorithm for symmetric encryption.

1.3 Context of Problem:

The context of the problem is that a strong encryption and decryption mechanism is required when migrating the VM file from one server or system to another. This project accomplishes that goal at the intranet level.

Chapter 2
Literature Review

Literature Review:

Through the internet, the entire world is being digitalized. And cloud computing rules the internet due of its simplicity and user-satisfying quality of service. Handling such many users while providing uninterrupted services is only possible with live virtual machine migration (before and post copy). Live Virtual Machine (VM) migration is a remnant of server virtualization in cloud computing.

Designing a solution for live VM (Virtual Machine) backup and recovery while maintaining a solid security posture is a vital part of current IT architecture. The goal is to achieve near-zero data loss and rapid recovery.

A variety of VM migration strategies have been developed to achieve effective VM migration while meeting the quality of service-driven customer criteria.

There are various AI-based and traditional load balancing, energy-aware, SLA-aware, and network-aware live VM migration strategies that explores the most significant components of traditional and AI-driven live VM migration strategies.

So, we can say that VM migration is a fundamental technology that used in cloud architecture to relocate running virtual machines (VMs). When the memory transfer rate exceeds the network bandwidth, pre copy migration impairs application performance. Furthermore, due to excessive page faults, post-copy migration is unable to provide optimal performance. To ensure optimal performance during VM migration, offers a hybrid VM migration methodology that combines the pre copy and post copy methods and optimal performance during VM migration in cloud data centres, a hybrid VM migration technique combining pre-copy and post-copy methodologies is proposed. This transfer VMs efficiently, the methodology employs **"push and pull"** approaches between highly loaded and less laden servers.

Simulations and comparisons with existing migration approaches demonstrate the proposed approach's usefulness in various settings because of the cloud's multi-tenant nature and the availability of resources in the form of virtual machines (VMs), there is an urgent need to evaluate the usefulness of prior backup and recovery methodologies in cloud platforms with virtual machine-based design. VM-Saver, a proposed backup and recovery framework, enables flexible and scalable backup and recovery models for virtualized physical servers within a multi-tenant cloud. VM-Saver incorporates numerous hypervisors' basic state saving methods and gives various methodologies and situations for providing virtualized system backup and recovery. This framework is versatile, reconfigurable, and compatible with several hypervisors, making it perfect for today's infrastructure clouds and the effective live VM migration approach can only be used to provide better computing capabilities, handle huge numbers of cloud users, and

save time and energy on cloud data centres. The modern cloud computing architecture is mostly based on live VM migration. Data centres have grown in importance as the use of cloud services has grown. Because of the increased business competitiveness to create cloud data centers, energy consumption in these data centers has increased. One of the major issues that needs to be addressed is how to reduce energy use. Even though many academics have provided graph solutions for difficulties like as load monitoring and load balancing, there are two variables that are critical in the migration process: how to create a green cloud and how to create a fault-tolerant cloud. Requests for resources can occur concurrently in a cloud environment, and these requests are then routed to the appropriate and accessible resources. One significant topic that has gotten a lot of attention over the last decade is resource utilization. Different load prediction approaches for load balancing during VM migrations have been presented utilizing the ideas of neural network, automata, or machine learning, but their combination remains a key difficulty in the domain of cloud server consolidation.

It is vital that any VMs at the time of transmission are not lost if VM migration fails, which it frequently does**. V-Recover** is a mechanism introduced to recover VMs in the event of migration failure due to source, destination, or network difficulties and to manage various failure scenarios during live migration, the approach employs forward incremental checkpointing and reverse incremental checkpointing procedures evaluation shows that V-Recover recovers VMs effectively while incurring acceptable overheads in migration metrics and application performance.

The significance of VM live migration in simplifying workload scheduling amongst remote cloud hubs to maximize server resource usage. By coordinating migration groups based on the I/O request pattern of VMs, a Live Scheduling Scheme (LSS) is presented to limit I/O interference in VM migration and improve migration efficiency. When compared to previous methodologies, the scheme is shown to dramatically enhance VM performance and migration effectiveness. It underlines the importance of effective migration procedures to deal with the growing number of users and workload. Additionally, the migration of operating system instances in data centers and clusters, emphasizing the advantages of live migration in terms of hardware-software separation, fault management, load balancing, and low-level system maintenance.

The design alternatives for migrating operating systems with liveness limitations are investigated, and a high-performance OS migration implementation based on the Xen VMM is provided. Another way for increasing the efficiency of VM live storage migration in cloud data centres. This solution called Snapping is given to improve migration efficiency while minimizing performance effect on user applications by utilizing existing VM snapshots in backup servers. This method reduces migration durations and increases VM performance, particularly when several migrations are taking place at the same time.

It is also underlined the significance of regular disaster recovery testing and the use of cloud-based backup systems. Several research have been conducted to investigate how

machine learning and artificial intelligence might be utilized to improve backup and recovery operations.

Chapter 3
Proposed Methodology

3.1 Proposed Methodology: In this project we are introducing an application that perform the double encryption by using the RSA asymmetric and AES symmetric, for that we have used the following tools and technologies:

3.1.1 Tools: To support the development of the application that encrypts VM files using double encryption with the RSA and AES algorithms, we employed a variety of tools and libraries.

Here is a list of tools and libraries that we have used:

3.1.1.1 **Windows Operating System**

3.1.1.2 **Virtualization software such as VMWare, Virtual Machine**

3.1.1.3 **Programming Languages:**

i. **Python:** We used the Python programming language for the programming purpose because it has extensive libraries for encryption and decryption purpose.

3.1.1.4 **Cryptographic Libraries**

3.1.1.5 Development Environment

3.1.1.6 **Integrated Development Environment (IDE):** To develop the program, we utilized the IDE "Visual Studio Code

3.1.1.7 **RSA Encryption**

3.1.1.8 **AES Encryption**

3.1.1.9 **File Handling:** To handle the file, we used Python's built-in **"os"** and **"shuntil"** modules, which allow us to read, write, and move VM files.

3.1.1.10 **Networking:**

i. **User Interface:** We designed a user-friendly interface for our program by utilizing the "**Tkinter framework**."

ii. **Security Best Practices:** Throughout the development process, we adhered to security best practices such as secure key management, sensitive data handling, and frequent security audits.

iii. **Operating System Compatibility:** We guaranteed that our application is compatible with the operating system.

3.1.2 Techniques: To construct an application that encrypts "**VM.iso**" files using double encryption (symmetric and asymmetric encryption) with the RSA and AES algorithms, we used a variety of approaches and best practices, including:

3.1.2.1. Requirement Analysis: The project requirements, including the file encryption procedure, key management, and communication between sender and recipient computers, have been properly stated.

3.1.2.2. Key Management: To produce, store, and exchange encryption keys, we have implemented a secure key management system. To generate keys, we used powerful, cryptographically safe random number generators.

3.1.2.3. Double Encryption: We used the RSA (asymmetric) and AES (symmetric) algorithms to accomplish double encryption.

3.1.2.4. Encryption Process: On the sender's end, we used the following stages to execute the encryption process:

i. For AES encryption, we produced a random symmetric key.
ii. Next, we used RSA encryption using the receiver's public key to encrypt the VM file.
iii. Following the asymmetric encryption, we utilized the symmetric encryption algorithm AES key to encrypt the VM file.
iv. Finally, we send the encrypted file along with the key.

3.1.2.5 Decryption Process: Make use of the following steps to implement the decryption process on the receiver's end:

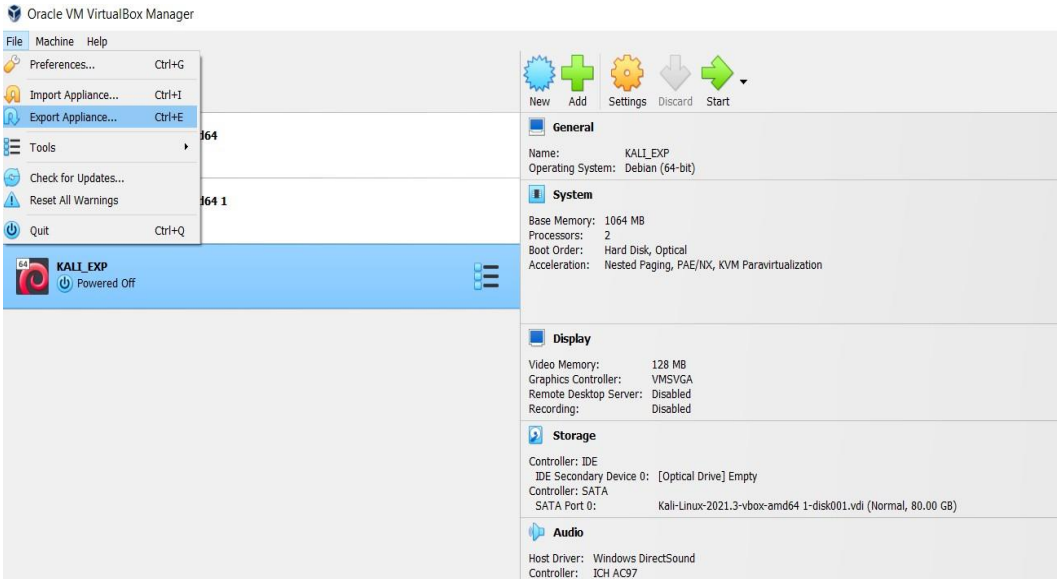
i. Using an AES-encrypted symmetric key, decrypt the VM file.
ii. Then, using the receiver's private key, decrypt it with the RSA-encrypted asymmetric key.
iii. After that, it will conduct the required file activity, such as saving the decrypted file.

3.1.2.6 Secure Communication: This program is designed to deliver VMs over the intranet.

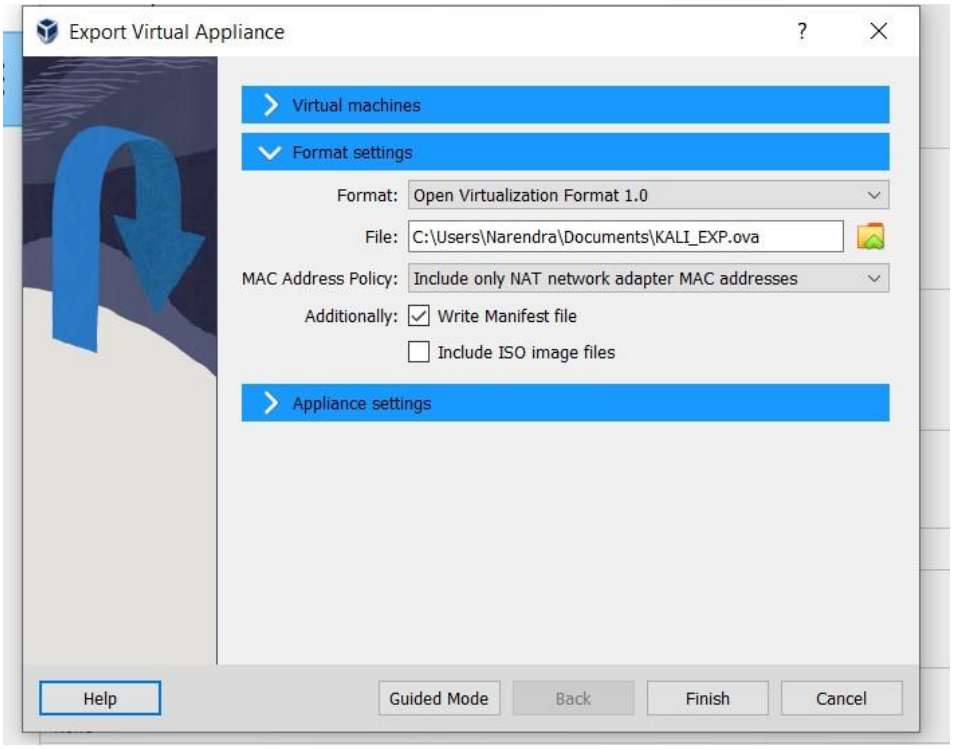
3.1.3 Complete Process of Application:

3.1.3.1 Encryption and Decryption Process with the help of available tools: Initially we did the encryption and decryption with the help of available tools

- Launch the Oracle Virtual Box.



- Select the VM which we want to migrate and export the virtual machine for backup as .ova file.

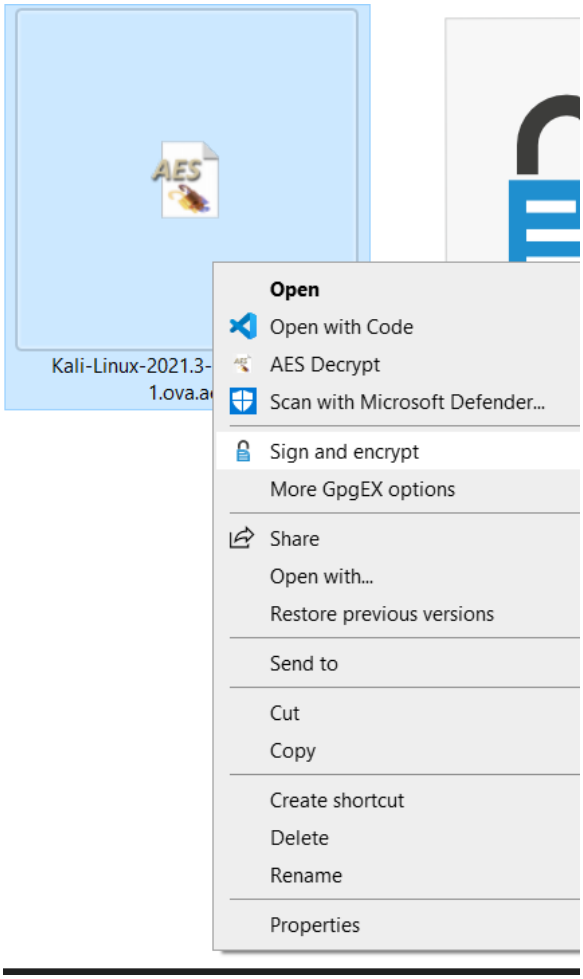


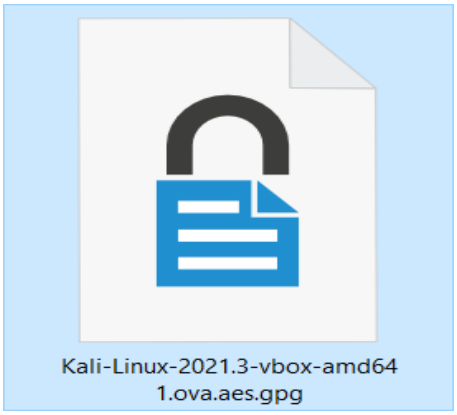
- Install the AES crypt tool and PGP encryption tool. Here We have used AES Crypt tool for Symmetric Encryption and PGP Kleopatra for Asymmetric Encryption.

- Encrypting the VM backup file in following order
  - **AES Encryption:** It will add (.aes) extension in our backup file.

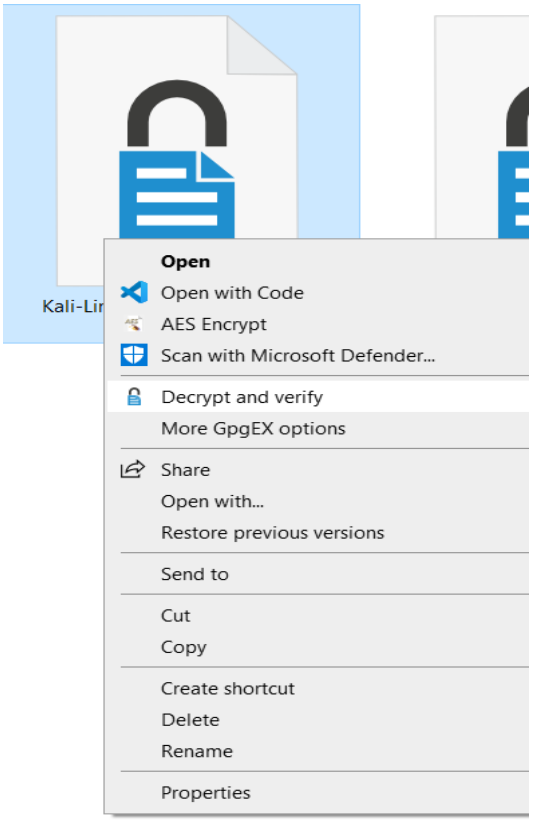
- **PGP Encryption:** It will add (.gpg) extension in our backup file with aes extension. Finally, File formate will be something – ABCD.ova.aes.gpg

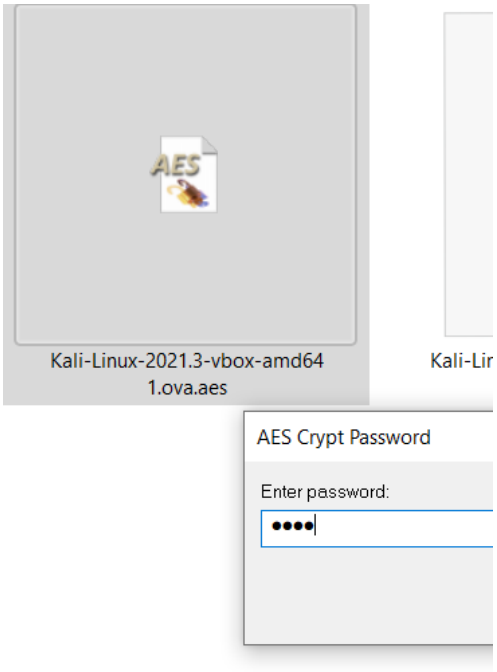

Kali-Linux-2021.3-vbox-amd64 1.ova
Kali-Linux-2021.3-
1.ova.a
AES Crypt Password
Enter password:
Confirm password:


Kali-Linux-2021.3-
1.ova.a
Open
Open with Code
AES Decrypt
Scan with Microsoft Defender...
Sign and encrypt
More GpgEX options
Share
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

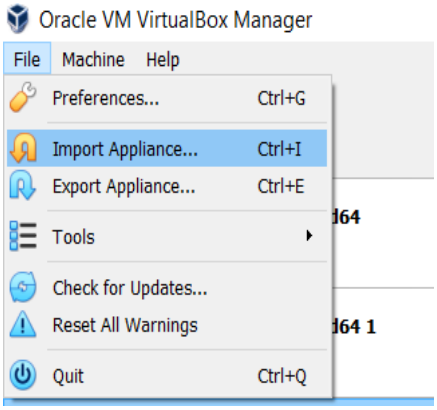


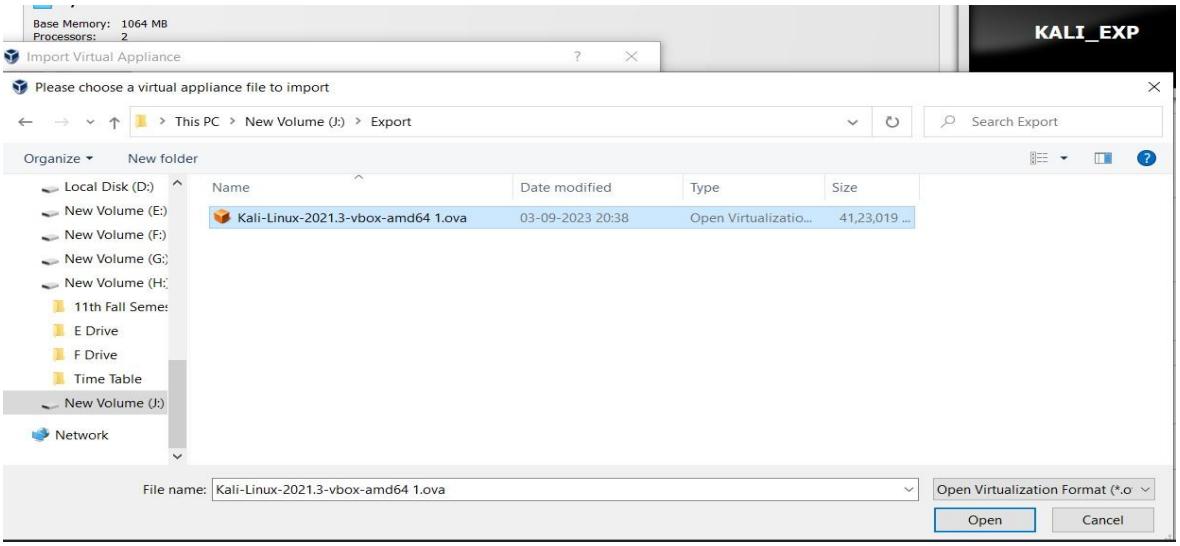
- Now share this final file to other system using Intranet or Share Using share folder. We can also share PGP Key and AES key but for the security reason we can also use other secure medium for sharing our keys.
- Now in the other system we will use LIFO Principal for decrypting key Using a public key to encrypt a VM aes encrypted file




Kali-Linux-2021.3-vbox-amd64
1.ova.aes
Kali-Lir
AES Crypt Password
Enter password:
Kali-Lir
Open
Open with Code
AES Encrypt
Scan with Microsoft Defender...
Decrypt and verify
More GpgEX options
Share
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

- To facilitate migration, share the file from system-01 to system-02 via the intranet or a shared folder.
- Share the PGP and AES secret keys as well.
- Repeat the decryption and virtual machine running steps for the second system virtual box. multiple security layers, migration, and VM backup storage.





3.1.3.2 Encryption and Decryption Process with created application: We were inspired by the encryption and decryption that we performed with the help of tools and created an application that performs the same task and can be sent over the intranet.

Diagram:

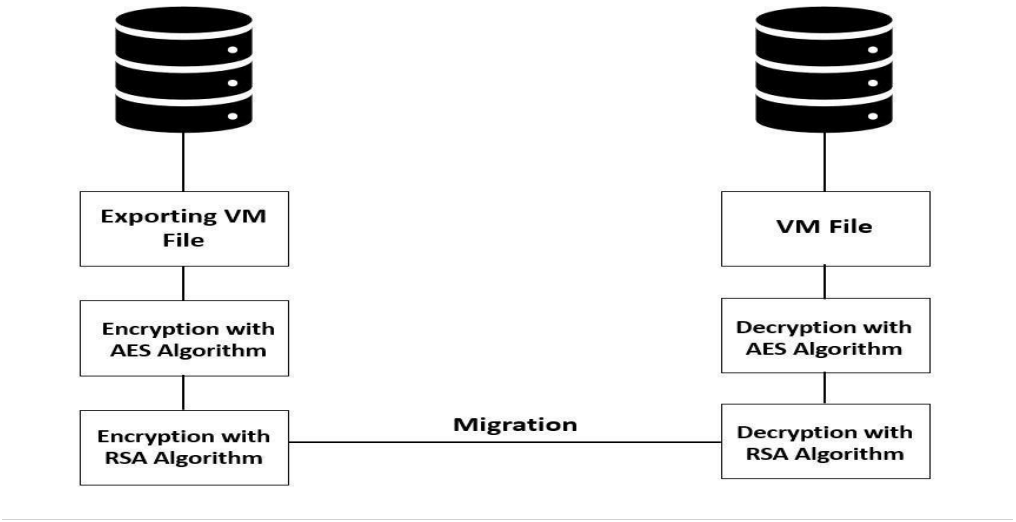


Figure 7: VM Migration Process

Chapter 4
Result

Results: The ultimate result of this project is that we have created a working application that can conduct double encryption and decryption using asymmetric and symmetric algorithms, and we can transfer it over the intranet in a secure manner.

Chapter 5
Conclusion

The conclusion of this project is that we successfully created the application we have created a working application that can conduct double encryption and decryption using asymmetric and symmetric algorithms, and we can transfer it over the intranet in a secure manner.

Chapter 6
Discussion

Discussion: We are now intending to create an application that will provide security so that we can send it from one internet to another.

References

[1] Wei Wang, Xiaoxin Wu, Ben Lin, Kai Miao, Xiaoyan Dang, “Secured VM Live Migration in Personal Cloud” January 2010.

[2] N. Nirmala Devi , S. Vengatesh Kumar, "PRE-COPY LIVE VM MIGRATION TECHNIQUES IN CLOUD COMPUTING USING HDWHM ALGORITHM" International Journal on Information Technologies & Security, № 1 (vol. 15), 2023

[3] Abhishek ku. Shakya (&), Deepak Garg, and Prakash Ch. Nayak, "Hybrid Live VM Migration: An Efficient Live VM Migration Approach in Cloud Computing" December 2018

[4] Prakash Ch. Nayak, Deepak Garg, Abhishek ku. Shakya, Poonam Saini, "A research paper of existing Live VM Migration and a Hybrid VM Migration approach in Cloud Computing" Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)

[5] Christopher Clark, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric Jul, Christian Limpach, Ian Pratt, Andrew Warfield, "Live Migration of Virtual Machine" 2018

[6] Anita Choudhary, Mahesh Chandra Govil, Girdhari Singh, Lalit K. Awasthi, Emmanuel S. Pilli & Divya Kapil, "A critical survey of live virtual machine migration techniques" Journal of cloud computing 2017

Acknowledgements

First and foremost, we would like to thank the Lord Almighty for His presence and immense blessings throughout the project work. We wish to express my heartfelt gratitude to Dr. H. Azath, Program Chair, Integrated MTech Cyber Security, School of Computing Science & Engineering, for much of his valuable support and encouragement in carrying out this work.

We would like to thank my internal guide Dr. Hemraj S. Lamkuche, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work. Last, but not least, we are deeply indebted to my parents who have been the greatest support while we worked day and night for the project to make it a success.

VIT University
Bhopal
October 10, 2023