Cloud Security: Risks, Top concern for cloud users, privacy impact assessment, trust, OS security, VM Security, Security Risks posed by shared images and management OS.

		Module-4			
Q. 07	a	Explain operating system security and virtual machine security.	L1,L2,L3	3, 4	10
	b	Explain the security risks posed by shared images and management os.	L1,L2,L3	3, 4	10
		OR			
Q. 08	a	Explain the concept of privacy impact assessment and its importance in cloud computing.	L1,L2,L3	3, 4	10

	b	Explain the following associated with cloud computing i) cloud security risks ii)Security: the top concern for cloud users.	L1,L2,L3	3, 4	10

Cloud Security Risks

Cloud computing introduces significant security risks, which users often underestimate due to the ease of access and lack of understanding of cloud operations. These risks can be broadly classified into three categories: traditional threats, system availability threats, and third-party data control threats.

1. Traditional Security Threats:

- Traditional threats, such as phishing, SQL injection, and cross-site scripting, are amplified in the cloud due to the scale of resources and shared infrastructure.
- **Authentication and Authorization Issues:** Cloud services require nuanced access controls for organizational use, making it challenging to adapt internal security policies to the cloud.
- **Multitenancy Risks:** Virtual Machine Monitors (VMMs) supporting multiple virtual machines (VMs) can be exploited to compromise shared environments.
- Investigating cloud security incidents is complex due to shared resources and the rapid overwrite of logs, which limits forensic capabilities.

2. System Availability Threats:

- **Service Interruptions:** Power outages, system failures, and catastrophic events can disrupt cloud services, potentially locking businesses out of critical data.

- **Data Accuracy Concerns:** Users cannot always be assured that cloud-hosted applications will return correct results.
- **Phase Transition Risks:** Complex cloud systems are prone to phenomena that can impact availability, as discussed in advanced studies.

3. Third-Party Data Control Risks:

- **Transparency Issues:** Cloud providers often subcontract services to third parties with unknown trust levels, leading to data mishandling.
- **Espionage Risks:** Providers may access proprietary data, creating risks of espionage and privacy breaches.
- **Contractual Limitations:** Cloud providers often limit their liability for data loss or security incidents, placing full responsibility on users.
- **Audit Challenges:** Lack of transparency makes verifying data handling practices and proving data deletion difficult.

4. Specific Threats Identified by CSA (Cloud Security Alliance):

- **Abuse of Cloud Resources:** Malicious users can exploit cloud services for launching large-scale attacks, such as Distributed Denial of Service (DDoS).
- **Insecure APIs:** Poorly designed APIs can expose users during authentication, monitoring, and runtime operations.
- **Malicious Insiders:** Providers' hiring practices may leave systems vulnerable to insider threats.
- **Data Loss or Leakage:** Cloud data replication failures combined with storage media failures can lead to permanent data loss.
- **Account Hijacking:** Credential theft poses a significant risk to user accounts and services.
- **Unknown Risk Profiles:** Many users underestimate the risks involved, leading to unintentional exposure.

---

5. Preventive Measures and Mitigation

For Users:

1. Evaluate the security policies and mechanisms of Cloud Service Providers (CSPs).
2. Clearly define contractual obligations with providers, covering:

- Secure data handling.
- CSP liability for breaches or data loss.
- Data ownership and storage geography.

3. Avoid processing sensitive data on public clouds unless necessary.
4. Encrypt sensitive data in storage and transit.

For Providers:

1. Strengthen API security with robust access control and monitoring.
2. Enforce strict hiring and personnel screening policies.
3. Improve transparency with subcontractor and hardware supplier relationships.

---

1. Attack Surfaces

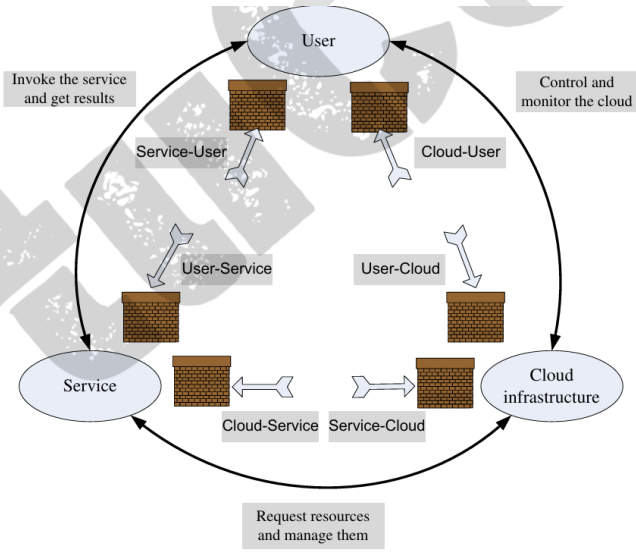

FIGURE 9.1
Surfaces of attacks in a cloud computing environment.

- **Cloud Computing Attack Surface**
- The attack surface in cloud computing refers to all the potential points where an attacker could exploit vulnerabilities to compromise the system. Since cloud environments are complex, the attack surface is larger compared to traditional IT systems and includes three key areas: User, Service, and Cloud Infrastructure.

1. User-Specific Attack Surface

- These attacks target the end-user who interacts with cloud services, often through user devices like laptops or mobile phones.
- **SSL/TLS Certificate Spoofing:**
  Attackers impersonate a legitimate cloud service by spoofing its SSL certificate, allowing them to intercept or manipulate user data.
- Impact: Man-in-the-middle attacks, data theft.
- **Phishing:**
  Fake entities trick users into revealing sensitive information like login credentials or financial data.
- Impact: Account compromise, identity theft.
- **Browser Cache Attacks:**
  Sensitive data like session tokens or passwords stored in a browser's cache can be stolen by attackers.
- Impact: Account hijacking, data leakage.

2. Service-Specific Attack Surface

- These attacks focus on vulnerabilities within the cloud services themselves, such as APIs or applications hosted in the cloud.
- **Buffer Overflow:**
  Attackers exploit programming flaws in cloud services to execute arbitrary code.
- Impact: Data corruption, system compromise.
- **SQL Injection:**
  Malicious SQL commands are inserted into web forms or applications, manipulating backend databases.
- Impact: Data theft or alteration.
- **Privilege Escalation:**
  Attackers exploit flaws to gain higher access levels than authorized, compromising the cloud service.
- Impact: Full system access, unauthorized operations.

3. Cloud Infrastructure-Specific Attack Surface

- This area refers to the underlying cloud infrastructure, such as virtual machines (VMs), networking components, and storage systems, where security vulnerabilities can be exploited.
- **Resource Exhaustion (DDoS):**
  Overloading cloud resources (e.g., CPU, memory) to prevent legitimate users from accessing services.
- Impact: Service disruption or downtime.
- **VMM Vulnerabilities:**
  Virtual Machine Monitors (VMMs) that manage VMs may have flaws allowing attackers to break out of one VM and access another or the host system.
- Impact: Cross-VM attacks, unauthorized data access.
- **Side-Channel Attacks:**
  Exploiting shared resources (like CPUs) to infer sensitive data being processed in other VMs.
- Impact: Data leakage between tenants.

Security: The Top Concern for Cloud Users

Security remains the primary concern for cloud users, who are used to having full control over their systems where sensitive information is stored and processed. In traditional IT environments, users operate within secure perimeters, typically protected by corporate firewalls. In contrast, cloud computing requires users to extend trust to Cloud Service Providers (CSPs) in exchange for the economic benefits of utility computing. This transition is challenging but necessary for the future of cloud adoption.

---

1. Major User Concerns

- **Unauthorized Access & Data Theft:**
  - Users are concerned about their data being vulnerable in the cloud, especially when it's stored for extended periods. While data is exposed to threats during processing, the risks of data theft are greater when the data is stored.
  - **Key Focus Areas:**
    - Security of storage servers.
    - Data in transit.

        - Protecting against rogue employees within CSPs.

- **Data Deletion Issues:**
    - Users cannot be certain that their data is completely deleted after use. Even if data is deleted, it's not guaranteed that the media was wiped clean, allowing future users to recover confidential data.
    - **CSP Backups:**
        - CSPs perform seamless backups without user consent, which could lead to data loss, accidental deletion, or exposure to attackers.

2. Other Concerns

- **Lack of Standardization:**
    - There are no interoperability standards, leaving many questions unresolved, such as:
        - What happens if a CSP's service is interrupted?
        - How can critical data be accessed in a blackout?
        - What if the CSP raises prices drastically?
        - How expensive is it to migrate to another CSP?
- **Auditability Challenges:**
    - Maintaining a full audit trail on the cloud is practically infeasible due to the distributed nature of cloud environments.
- **Emerging Threats (Autonomic Computing):**
    - As cloud computing evolves, technologies like autonomic computing (self-organization, self-repair) could introduce new threats.
    - It will become harder to track actions within such systems, making it difficult to pinpoint the source of an attack or data loss.
- **Multitenancy Risks:**
    - **Shared Resources:**

- In multi-tenant cloud environments, multiple users share resources. If security is compromised on one server, multiple users are affected, especially when sensitive data like credit card numbers or addresses are stored together.
- **Processing Time Risks:**
  - Threats from multitenancy are not limited to storage; data can also be compromised during processing.

3. Legal and Regulatory Concerns

- **Legal Framework:**
  - Cloud technology has outpaced security and privacy legislation, causing confusion about which laws apply when data crosses national borders.
  - **Outsourcing Issues:**
    - CSPs may outsource data handling to other countries or companies, complicating the enforcement of security and privacy laws.
    - CSPs may also be required by law to share data with law enforcement agencies.
- **User Rights:**
  - Users face difficulties in defending their rights and understanding the applicable laws, especially when their data is stored or processed in multiple countries.

---

4. Mitigating Security Risks

To minimize the risks associated with cloud computing, users can take the following steps:

1. **Evaluate CSP Security Policies:**
   - Carefully analyze the security mechanisms that the CSP has in place to enforce its policies.
2. **Contractual Obligations:**
   - Contracts between users and CSPs should clearly address:
     - CSP's responsibility for securing sensitive information.
     - CSP liabilities for mishandling data or data loss.
     - Ownership rules for data.
     - Geographical regions where data and backups can be stored.

3. **Encrypt Sensitive Data:**
    - Whenever possible, encrypt sensitive data stored or processed in the cloud to protect it from unauthorized access.
    - **Challenges with Encryption:**
        - Encryption can make data difficult to index and search.
        - **Options:**
            - Fully Homomorphic Encryption: Allows encrypted data to be processed without decrypting it.
            - Secure Two-Party Computations: Enables secure data processing between two parties without revealing private data.

---

5. Other Recommendations

- **Avoid Storing Sensitive Data on Public Clouds:**
    - If possible, users should avoid storing sensitive data on public clouds. For highly sensitive applications (e.g., medical records), using private or hybrid cloud solutions is preferable.
- **Secure Data Connector (e.g., Google's Solution):**
    - Tools like Secure Data Connector analyze data structures and protect data with firewalls before accessing cloud services.

Privacy and Privacy Impact Assessment

Privacy refers to an individual's or organization's right to protect personal or proprietary information from being disclosed without consent. It is considered a fundamental human right in many nations, as stated by the **Universal Declaration of Human Rights** (Article 12), which ensures protection against arbitrary interference with privacy. However, privacy rights can conflict with other legal obligations, such as taxation laws or freedom of speech. Privacy laws vary by country, and the digital age has raised significant privacy challenges, including identity theft due to data misuse.

1. Privacy in the Digital Age

- **Emerging Threats:**
    - Personal information shared online can be misused or stolen, leading to identity theft.

- The **EU** has introduced strict privacy laws and the **"right to be forgotten"**, aiming to give individuals more control over their online information.

- **Public Clouds and Privacy:**
  - In public cloud environments, data often resides on unencrypted servers owned by Cloud Service Providers (CSPs). This increases the risk of unauthorized access or misuse of personal data.
  - The owner of the data has limited control over the exact location and retention of the data once stored on the CSP's servers.

---

2. Privacy Concerns in Cloud Computing

- **Lack of User Control:**
  - Once data is stored on a CSP's servers, users lose control over its location, retention, and accessibility. For example, Gmail users cannot control where their emails are stored or how long they remain in backups.
- **Secondary Data Usage:**
  - CSPs may use user data for unauthorized purposes, such as targeted advertising, without users' explicit consent.
  - **Dynamic Provisioning Risks:**
    - Subcontracting by CSPs raises questions about data ownership and rights, especially during mergers, acquisitions, or bankruptcy.

---

3. Privacy and Cloud Delivery Models

- **SaaS (Software as a Service) Example:**
  - Gmail's privacy policy shows that user data, such as personal information, location data, and device information, is collected and shared with third parties under certain conditions (e.g., legal obligations, advertising).
  - **Privacy Concerns:**
    - Lack of user control over stored data.
    - Potential unauthorized secondary uses, such as advertising.

- **Privacy Issues Differ by Model:**
    - **IaaS (Infrastructure as a Service)** and **PaaS (Platform as a Service)** also face similar concerns, but users have more control over data storage and processing compared to SaaS.

---

4. Privacy Legislation and Consumer Rights

- **Federal Trade Commission's Fair Information Practices:**
  The U.S. FTC recommends four core practices to protect consumer privacy on commercial websites:
    1. **Notice:** Clear and visible information on what data is collected, how it is used, and if it will be shared.
    2. **Choice:** Offering consumers options about how their personal data is used beyond its initial purpose.
    3. **Access:** Allowing consumers to access, review, and correct their personal data.
    4. **Security:** Taking reasonable steps to protect the collected data's security.
- **Privacy Legislation Challenges:**
    - Privacy laws vary between countries, making it difficult to enforce privacy protections when data crosses borders.

---

5. Privacy Impact Assessment (PIA)

- **What is PIA?**
    - A **Privacy Impact Assessment** is a process that helps identify privacy risks in information systems and ensures that privacy policies are followed.
    - **PIA Tools** help assess and mitigate privacy risks in cloud computing systems. They include:
        - A **questionnaire** for project details, privacy risks, and stakeholders.
        - A **knowledge base** managed by domain experts to analyze privacy rules and generate compliance reports.
- **Benefits of PIA:**
    - Helps identify and address privacy issues proactively, ensuring privacy is embedded in new systems rather than applying changes to existing systems that could affect functionality.

- Tools like the proposed PIA tool automate the process of generating PIA reports, including a risk summary, transparency, security, and cross-border data flow analysis.

---

6. Need for Legislation and Tools

- **Privacy Legislation:**
  There is a growing need for comprehensive legislation addressing privacy in the digital age, as current laws struggle to keep up with the rapid growth of cloud computing.
- **PIA Tool Implementation:**
  Tools capable of performing Privacy Impact Assessments (PIAs) are necessary to proactively identify and mitigate privacy risks. These tools use templates to generate questions for users and produce compliance reports, ensuring that privacy concerns are properly addressed in cloud services.

Trust in Cloud Computing

Trust is a critical concept in cloud computing, as it governs the confidence users have in cloud service providers (CSPs) and their ability to securely store and process sensitive data. Trust is also essential for online interactions in general, where the identities of parties involved are often obscured, and security mechanisms are necessary to ensure reliability and accountability.

---

1. Traditional Concept of Trust

According to the **Merriam-Webster Dictionary**, trust is defined as "assured reliance on the character, ability, strength, or truth of someone or something." Trust is essential for cooperation, reducing conflicts, and promoting organizational effectiveness. It lowers transaction costs and helps in crisis management. For trust to develop, two conditions must exist:

- **Risk:** There is a possibility of loss or failure, making trust necessary to mitigate that risk.
- **Interdependence:** One entity's success depends on the actions or cooperation of another entity.

Trust progresses in three phases:

1. **Building Phase:** Trust is formed.
2. **Stability Phase:** Trust is established and maintained.
3. **Dissolution Phase:** Trust declines, often due to violations.

---

2. Types of Trust

- **Deterrence-based Trust:**
  Based on the belief that penalties for breach of trust exceed the benefits of opportunistic behavior.
- **Calculus-based Trust:**
  Derived from the belief that actions align with the self-interest of the parties involved.
- **Relational Trust:**
  Builds over time based on repeated interactions and dependability.

---

3. Trust in Online Activities

- **Challenges in Online Trust:**
  In online environments, especially in cloud computing, the traditional elements of trust—such as personal identity and relationship—are often absent.
  - **Anonymity:** Users can conceal their identity, which causes mistrust due to the lack of accountability.
  - **Opacity:** Online entities lack clear roles, and it's difficult to verify the person behind a transaction.

To address these issues, mechanisms for **access control**, **identity transparency**, and **surveillance** are needed. These include:

- **Access Control:** Prevents unauthorized users from gaining access.
- **Identity Transparency:** Uses methods like biometric identification, digital signatures, and certificates to verify identities.
- **Surveillance:** Involves intrusion detection systems or logging and auditing to monitor actions and verify accountability.

---

4. Credentials and Reputation

- **Credentials:**
  These are used to verify the identity of an entity. For instance, a doctor's diploma is a credential proving their qualification. Similarly, a **digital signature** acts as a credential in cloud applications.

- **Policies:**
  Trust is governed by **policies**, which specify the conditions for trust and the actions to take when conditions are met. Policies ensure credentials are verified and trusted.
- **Reputation:**
  Reputation builds based on the history of interactions or observations of an entity. It can be assessed through recommendations or decisions made by others based on their trust in the entity.

---

5. Trust in Cloud Services

In the context of cloud computing, trust is defined as the measurable belief that a cloud service provider (CSP) will behave dependably over a specified period, in relation to the services offered. This includes ensuring:

- **Persistent Trust:**
  Built over time based on reliable service delivery and continuous interaction.
- **Dynamic Trust:**
  Context-specific trust that adapts to changes in the service environment or technological developments.

---

6. Establishing Trust in Cloud Computing

- **Policies and Reputation Systems:**
  Trust in cloud services can be determined through policies that define the conditions for establishing trust. Reputation systems track the history of interactions and feedback from users to assess reliability and service quality.
- **Measuring Trust:**
  In a cloud context, trust between a user (party A) and a service provider (party B) for a specific service (X) is the belief that the service provider will consistently deliver the service in a dependable manner, in line with agreed terms.

An operating system (OS) allows multiple applications to share hardware resources securely while protecting them from threats like unauthorized access, tampering, and spoofing. Even single-user systems, such as PCs and smartphones, are vulnerable to attacks through malicious Java applets or compromised web data.

Mandatory security policies in an OS are defined and controlled by system administrators. These policies include access control to regulate resource access, authentication mechanisms to verify identities, and cryptographic mechanisms to protect data integrity and confidentiality. These subsystems must be tamper-proof and enforceable, ensuring that applications operate within unique security domains.

Trusted applications perform security-specific functions and are granted minimal privileges necessary for their tasks. Type enforcement is a mandatory security mechanism that limits the privileges of these applications. However, discretionary security mechanisms, which rely on user-defined controls, can lead to vulnerabilities due to user errors or malicious intent. Unlike discretionary policies, mandatory policies can only be modified by system administrators, providing a more robust security framework.

Commercial operating systems often lack multilayered security and distinguish only between fully privileged and unprivileged domains. For instance, Windows NT allows programs to inherit privileges from their invokers, regardless of the trust level. This approach makes systems vulnerable to privilege escalation and security breaches. Additionally, the absence of trusted paths in some OSs allows malicious software to impersonate trusted applications, compromising user interactions.

To enhance security, the decomposition of mechanisms into well-defined components, such as enforcers and deciders, is recommended. Enforcers gather and validate access requests, while deciders evaluate these requests against security policies. Trusted paths are crucial to preventing tampering with policy rules and object attributes. For example, cryptographic mechanisms should be safeguarded through such trusted paths to ensure data integrity.

Mobile code, such as Java applets, poses additional security risks. While the Java Security Manager restricts unauthorized actions using type safety in a sandbox environment, the Java Virtual Machine (JVM) can still accept invalid byte code. This limitation makes it susceptible to tampering by other applications, highlighting the need for stronger OS protections.

Commodity operating systems face inherent weaknesses due to their complexity, often comprising millions of lines of code. They lack strong application isolation, making the entire system vulnerable if one application is compromised. Additionally, weak authentication mechanisms and the absence of trusted paths hinder secure interactions between applications and users. This is especially challenging in distributed computing environments where robust authentication is essential.

Virtual Machine Security

Virtual machine (VM) security primarily concerns the traditional system VM model, where the Virtual Machine Monitor (VMM) controls access to hardware. The hybrid and hosted VM models are excluded as they depend on the security of the host operating system, introducing additional vulnerabilities.

Role of VMM in Security:

- The **VMM** provides virtual security services and controls privileged operations, enforcing memory isolation, and managing disk and network access.
- A secure **Trusted Computing Base (TCB)** is essential; compromising the TCB affects the entire system's security.
- **Dedicated Security Services VMs** can be used for enhanced protection, isolating sensitive files and processes.

Key Features of VMM Security:

- Provides stricter isolation than traditional OS processes.
- Allows operations such as saving, restoring, cloning, and encrypting the state of guest VMs:
    - **Cloning:** Useful for testing potentially malicious applications.
    - **Inter-VM Communication:** Faster than physical machine communication, aiding security tasks.

Threats and Challenges:

1. **VMM-Based Threats:**
    - **Resource Starvation:** Improper resource limits or rogue VMs bypassing constraints.
    - **Side-Channel Attacks:** Exploit inter-VM traffic due to misconfigured networks or insecure VM instances.
    - **Buffer Overflow Attacks:** Target vulnerabilities in the VMM.
2. **VM-Based Threats:**
    - **Rogue/Insecure VMs:** Unauthorized users may create or modify insecure instances due to weak access controls.
    - **Tampered VM Images:** Lack of repository controls or mechanisms to verify image integrity, such as digital signatures.

Advantages of Virtualization for Security:

- Isolation, inspection, and interposition:
    - **Inspection:** VMM can review guest VM states.

- **Interposition:** VMM can trap and emulate privileged instructions.

- Supports intrusion detection/prevention systems, e.g., Livewire, Siren, and Terra.

Security Costs of Virtualization:

- Increased hardware requirements (CPU, memory, disk, bandwidth).
- Development and maintenance costs of VMMs.
- Performance overhead due to the VMM's role in privileged operations.

Security Risks Posed by Shared Images:

1. **Overview:**
   - Image sharing in cloud environments, particularly IaaS, introduces risks even when the cloud provider is trustworthy.
   - Users can select images like Amazon Machine Images (AMIs) from public repositories, often containing vulnerabilities.
2. **Risks Identified:**
   - **Sensitive Data Recovery:**
     - Credentials, private keys, and sensitive information can often be undeleted from shared AMIs using basic tools.
   - **Software Vulnerabilities:**
     - 98% of Windows AMIs and 58% of Linux AMIs analyzed were found with critical vulnerabilities, including remote code execution risks.
     - Older AMIs often lack updates and patches, increasing their exposure.
   - **Backdoors and Credentials:**
     - Malicious AMI creators may embed backdoors using SSH keys or password hashes, enabling unauthorized access.
     - Shared SSH host keys can lead to man-in-the-middle attacks.
   - **Unsolicited Connections:**

- Outgoing connections can leak privileged information, including IP addresses and logs, posing privacy risks.

- **Malware:**
  - Malware like Trojans and keyloggers were found in some AMIs, capable of stealing sensitive information.

3. **Impact on Image Providers:**
   - Providers risk exposing their private data (e.g., API keys, IP addresses, history files) stored in AMIs.
   - Recovery of deleted files from improperly wiped images exacerbates this risk.
4. **Mitigation Strategies:**
   - Use tools like shred, scrub, or wipe to ensure sensitive data is irretrievable.
   - Employ cryptographic verification of images and limit repository access.
   - Regularly update images to address known vulnerabilities.

Security Risks Posed by a Management OS:

1. **Overview of Management OS (Dom0):**
   - Dom0 in virtualized environments like Xen manages administrative tasks, including creating and managing VMs.
   - It interacts closely with the hypervisor and guest VMs (DomUs) for operations such as memory allocation and I/O handling.
2. **Risks Identified:**
   - **Vulnerabilities in Dom0:**
     - Most attacks target service components of Dom0, including buffer overflows and denial-of-service (DoS) attacks.
   - **Malicious Actions:**
     - Dom0 can manipulate guest VM configurations, such as altering kernel integrity, setting incorrect page tables, or refusing to release foreign memory mappings.

- **Insecure Communication:**
  - Runtime communication between Dom0 and DomU, especially involving I/O devices, can expose sensitive data.
- **XenStore Exploitation:**
  - Malicious VMs can deny access to critical XenStore elements or gain unauthorized access to DomU memory.

3. **Mitigation Strategies:**
   - Encrypt DomU's memory pages and CPU registers during Dom0 interactions.
   - Restrict specific hypercalls from Dom0 that could compromise DomU integrity.
   - Monitor and validate DomU integrity after critical hypercalls like state saving or restoring.
   - Use a secure runtime system that intercepts and controls hypercalls to ensure confidentiality and integrity.
4. **Performance Overhead:**
   - Enhanced security leads to increased resource usage, including longer domain build, save, and restore times (1.7x to 2.3x).