MODULE 4

11.1 SECURITY: THE TOP CONCERN FOR CLOUD USERS

Some believe that moving to the cloud eliminates security concerns, as experts handle cloud security. However, this is not entirely true.

Key Concerns:

- **New Security & Privacy Risks:** Outsourcing computing to the cloud introduces security risks, and Service Level Agreements (SLAs) do not provide full legal protection.
- **Trust & Control Issues:** Organizations used to operate within a secure corporate firewall. Now, they must trust the Cloud Service Provider (CSP), which is a difficult shift. Surveys confirm that security is a top concern.
- **Unauthorized Access & Data Theft:** Data is more vulnerable in storage than during processing. Risks include threats from rogue employees of CSPs. Insider attacks are a major concern since CSP hiring policies are not transparent.
- **Data Lifecycle Control:** Users cannot verify if deleted data is permanently removed. CSPs create backups without user consent, which may expose data to accidental loss or attacks.
- **Lack of Standardization:** No interoperability standards exist. Questions remain, such as:
    - What happens if CSP services are interrupted?
    - How can critical data be accessed during a blackout?
    - What if CSPs raise prices drastically?
    - How difficult is switching to another CSP?
    - Auditing and compliance remain unresolved challenges.
- **Future Technology Risks:** Emerging technologies, such as autonomic computing, may introduce new security risks. These self-managing systems make it harder to track actions and identify threats.

- **Multi-Tenancy Risks:** Multi-tenancy allows multiple users to share cloud resources, reducing costs but increasing risks. In **SaaS**, a security breach can expose private user data like names, phone numbers, and credit card details.
- **Legal Uncertainties:** Laws regarding cloud security and privacy lag behind technology. Issues include:
    - CSP data centers in different countries—Which country's laws apply?
    - CSP outsourcing data handling—How can users enforce security when outsourcing crosses multiple countries?
    - CSPs may be legally required to share user data with law enforcement.

Reducing Security Risks:
Cloud users should:

1. Evaluate **CSP security policies** and enforcement mechanisms.
2. Analyze the **sensitivity of stored data**.
3. Ensure contractual clarity on:
    - CSP obligations regarding sensitive information and privacy laws.
    - CSP liabilities for data mishandling.
    - Data ownership rules.
    - Geographic limits on data storage.
4. Avoid storing **sensitive data** on the cloud when possible. Google's **Secure Data Connector** protects data behind a firewall, but this solution isn't always feasible. If storing sensitive data is unavoidable, **encryption** should be used.

11.2 CLOUD SECURITY RISKS

Cloud services are widely used, but many users do not fully understand the security risks. One major concern is that cloud platforms can be misused for cyberattacks.

Preventing Cloud Misuse

To prevent malicious activities in the cloud, service providers must:

- **Enforce strong authentication** to stop unauthorized access.
- **Monitor and detect suspicious activities** in real-time.

- **Follow security regulations** and work with authorities to prevent cybercrime.

Main Security Risks in Cloud Computing

Cloud security risks can be grouped into three categories:

1. Traditional Security Threats

- **Amplified Risks:** Due to the vast cloud resources and large user base, attacks can have a major impact.
- **User Responsibilities:** Users must secure their own devices and networks when connecting to the cloud.
- **Authentication Issues:** Organizations need proper access control based on user roles.
- **Common Attacks:**
    - **DDoS Attacks:** Overloading cloud services to disrupt access.
    - **Phishing:** Tricking users into revealing sensitive information.
    - **SQL Injection:** Injecting malicious queries to steal or modify database data.
    - **Cross-Site Scripting (XSS):** Inserting harmful scripts into websites to bypass security.

Challenges in Attack Tracing:

- Multi-tenancy (sharing resources among users) makes tracking attacks difficult.
- Traditional digital forensics does not work well in dynamic cloud environments.

2. System Availability Risks

- **Service Downtime:** Power failures, system crashes, or cyberattacks can cause disruptions.
- **Data Lock-In:** Organizations may struggle to retrieve data if a provider shuts down.
- **Reliability Issues:** Users cannot always verify if cloud services return accurate results.

3. Third-Party Control Risks

- **Lack of Transparency:** Users have limited control over how providers manage data.
- **Risky Subcontracting:** Cloud providers may outsource services to untrusted third parties, increasing security concerns.

- **Cloud Provider Espionage:** Some providers may access and misuse customer data.
- **Liability Issues:** Cloud contracts often place full responsibility on users for data security.
- **Lack of Auditability:** Users cannot easily verify if cloud providers handle data correctly.

Top Cloud Security Threats (CSA Report 2010)

A 2010 Cloud Security Alliance (CSA) report highlights the top threats to cloud security:

1. **Abuse of cloud resources** – Attackers use cloud services for malicious activities.
2. **Insecure APIs** – Weak interfaces expose user data.
3. **Malicious insiders** – Employees at cloud providers could exploit their access.
4. **Shared technology vulnerabilities** – Multi-tenant systems pose security risks.
5. **Account hijacking** – Cybercriminals steal credentials to gain control.
6. **Data loss or leakage** – Cloud data is at risk due to system failures or attacks.
7. **Unknown risk profiles** – Users may not fully understand cloud security risks.

Types of Cloud Attacks (CSA Report 2011)

A 2011 CSA report categorizes cloud attacks based on three main actors:

- **User attacks:** SSL spoofing, phishing, and browser cache exploitation.
- **Service attacks:** Buffer overflow, SQL injection, and privilege escalation.
- **Cloud infrastructure attacks:** Exploiting vulnerabilities in cloud management systems.

Top 12 Cloud Security Threats (Student-Friendly Notes)

The 2016 Cloud Security Alliance (CSA) report highlights the most critical cloud security risks.

1. Data Breaches

- Breaches involving **financial, health, trade secrets, or intellectual property** data are most damaging.
- Organizations are responsible for protecting data.
- **Prevention:** Use **multi-factor authentication (MFA)** (e.g., one-time passwords, phone-based authentication, smart cards) and **encryption**.

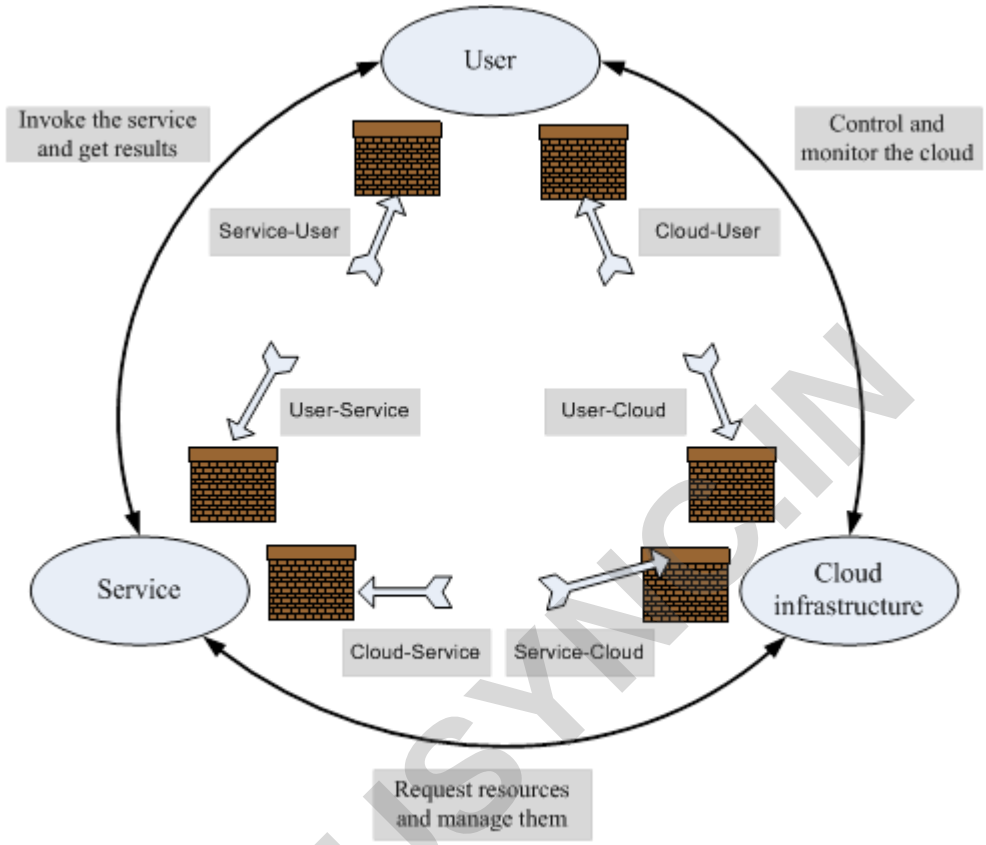


Fig 11.1 Surfaces of attacks in a cloud computing environment.

2. Compromised Credentials & Broken Authentication

- Weak passwords and poor key management make cloud accounts vulnerable.
- **Prevention:** Enforce strong authentication policies.

3. Hacked Interfaces & APIs

- Weak APIs expose services and credentials to attacks.
- **Prevention:** Secure APIs and limit third-party access.

4. Exploited System Vulnerabilities

- Multi-tenancy and shared resources create new attack surfaces.
- **Prevention:** Regular security updates and vulnerability patching.

5. Account Hijacking

- Attackers steal credentials to gain control of accounts.
- **Prevention:** Monitor accounts and track transactions to specific users.

6. Malicious Insiders

- Insiders (employees or admins) can misuse their privileges.
- **Prevention:** Enforce **role segregation**, log activities, and conduct security audits.

7. Advanced Persistent Threats (APTs)

- Long-term targeted attacks that infiltrate networks undetected.
- **Prevention:** Use **network monitoring** and advanced threat detection.

8. Permanent Data Loss

- Data can be lost due to accidental deletion, system failures, or attacks.
- **Prevention:** Regular **data backups** and redundancy.

9. Inadequate Diligence

- Organizations may fail to properly assess cloud risks before migrating.
- **Prevention:** Conduct **security assessments** and follow best practices.

10. Cloud Service Abuse

- Attackers misuse cloud services for spam, malware distribution, or cyberattacks.
- **Prevention: Monitor cloud usage** and restrict malicious activities.

11. Denial of Service (DoS) Attacks

- Attackers overload cloud services, making them unavailable.
- **Prevention:** Use **DoS protection tools** and scalable infrastructure.

12. Shared Technology Issues

- Vulnerabilities in shared resources (e.g., hypervisors) can affect multiple users.
- **Prevention:** Strengthen **isolation mechanisms** between tenants.

Additional Cloud Security Concerns

- **Cloud Controls Matrix**: Provides guidelines on cloud security measures.

- **Reported Threats (2014-2018)**:
    - **Hardware failures, natural disasters, malware, poor infrastructure planning.**
    - **POS intrusions, cyber-espionage, insider privilege misuse, web attacks, theft/loss.**

  Cloud security requires **strong policies, regular monitoring, and advanced security measures** to protect against these threats.

Here's a condensed version of the content while maintaining the original wording for student-friendly notes:

11.3 PRIVACY AND PRIVACY IMPACT ASSESSMENT

Privacy refers to the right of individuals, groups, or organizations to keep personal or proprietary information from being disclosed. Many nations recognize privacy as a basic human right. The **Universal Declaration of Human Rights, Article 12**, states that no one should face arbitrary interference with their privacy, family, home, or correspondence.

While the **U.S. Constitution** does not explicitly mention privacy, the **Bill of Rights** protects aspects of it. The **UK guarantees privacy** through the **Data Protection Act**, and the **European Court of Human Rights** has defined various privacy rights. However, privacy is limited by laws such as taxation requirements. Privacy rights also vary across countries.

The **digital age** presents new privacy challenges, like identity theft from stolen or misused online data. Some nations are more proactive in addressing these issues. The **EU**, for example, has strict data protection laws and introduced the **"right to be forgotten"**, allowing individuals to remove online personal information.

Cloud computing adds complexity to privacy concerns as **data is stored on servers owned by Cloud Service Providers (CSPs)**, often in unencrypted form. Users **lose control** over their data's exact location and storage duration. **Gmail's privacy policy** shows how companies collect and use personal data, including sharing non-personally identifiable data with third parties.

Key cloud privacy concerns include:

- **Lack of user control** – Users cannot determine where or how long data is stored.
- **Unauthorized secondary use** – Data may be used for advertising or analytics without consent.
- **Data proliferation** – Data spreads across multiple locations.

- **Dynamic provisioning** – Cloud providers may outsource data storage, making it unclear who has access to the data.

Legislative Needs & Privacy Impact Assessment (PIA)

Privacy laws must evolve to address digital concerns. The **Federal Trade Commission (FTC)** suggests four **Fair Information Practices** for websites handling personal data:

1. **Notice** – Clear disclosure of data collection, use, and sharing practices.
2. **Choice** – Users must have options for how their data is used beyond the initial purpose.
3. **Access** – Users should be able to review, correct, or delete their personal data.
4. **Security** – Websites must take reasonable steps to protect collected information.

There is a need for **Privacy Impact Assessment (PIA) tools** to identify privacy risks in information systems. As of **2017, no international PIA standards exist**, though different countries require PIA reports.

An example is the legal assessment of the **UK-US Safe Harbor** process, which allows **US companies to comply with European data protection laws**. A **proactive privacy approach**—embedding privacy rules into new systems from the start—is better than making difficult changes later.

A proposed **web-based PIA tool** requires users to provide project details, privacy risks, and stakeholders. The system generates a **PIA report** covering risk analysis, security, transparency, and data flows across borders. An **expert system** evaluates user inputs, applies rules, and prioritizes findings.

11.5 CLOUD DATA ENCRYPTION

Governments, corporations, and individual users question whether it is safe to store sensitive data on public clouds. **Encryption** is the primary solution, and cloud providers offer encryption services. For example, **AWS Key Management Service (KMS)** enables clients to create and manage encryption keys for securing their data. KMS integrates with **EBS, S3, RDS, Redshift**, and other AWS services.

Homomorphic Encryption

While **strong encryption** keeps data secure in storage, **decryption for processing** creates vulnerabilities. The idea of **homomorphic encryption** allows operations on encrypted data

without decryption. This follows the mathematical concept of **homomorphism**, where encrypted operations produce the same result as plaintext operations after decryption.

Fully Homomorphic Encryption (FHE) was introduced by **Craig Gentry (2009)** and allows **general computations on encrypted data**. However, **FHE is impractical** due to extreme processing overhead—initial implementations required **minutes per operation**, though improvements have reduced this to **about one second** in some cases.

Searching Encrypted Databases

Cloud databases store vast amounts of **encrypted data**, but searching them efficiently is difficult. Standard encryption methods cause **performance issues** because they prevent the use of **database indexing (e.g., B-trees)**.

Order Preserving Encryption (OPE)

OPE helps encrypt **numeric data** while preserving order, allowing efficient range queries. It works by mapping numbers to a **larger and sparse range** using a function based on the **Negative Hypergeometric Distribution (NHG)**.

OPE uses a **binary search encryption process** with a **secret key (KEncrypt, KH)**:

- **KEncrypt** encrypts values normally.
- **KH** applies an order-preserving hash.
- The encrypted value consists of **Encrypt(KEncrypt, x) || H(KH, x)**.

Searchable Symmetric Encryption (SSE)

SSE enables **secure searches** on encrypted cloud databases. The client stores only a **cryptographic key** and performs searches by:

1. **Encrypting the query** before sending it to the database.
2. **Receiving encrypted search results** from the server.
3. **Decrypting the results** with the cryptographic key.

SSE prevents explicit **data leaks** but may reveal **query patterns**. A scalable **SSE protocol** supporting **Boolean, phrase, range, substring, wildcard, and ranked searches** has been developed, even working efficiently on **large databases like Wikipedia**.

Cloud Data Security Threats

- **Public Clouds:** Attackers can target encrypted data when it is decrypted for processing.

- **Private Clouds:** Outsiders face **firewall protection**, but **insider threats** remain. Insiders with access to **log files** can **identify database hotspots** and selectively steal sensitive data.

To **mitigate insider risks**, **protection rings** should **limit staff access** to specific database sections.

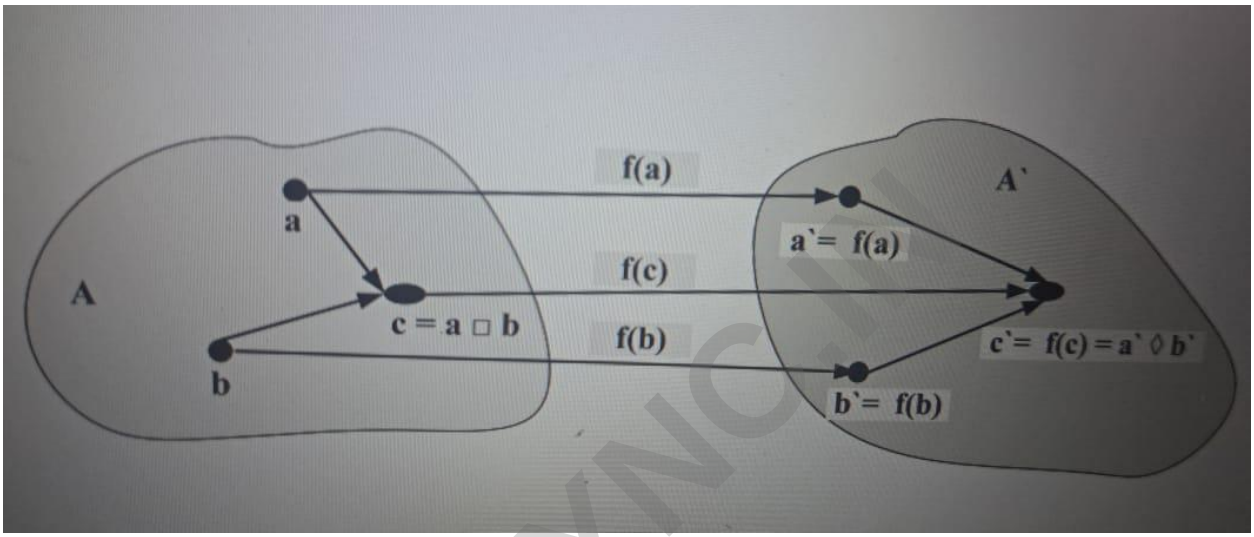


Fig 11.2 A homomorphism f : A → A is a structure-preserving map between sets A and A with the composition operations and ♦, respectively. Let a,b,c ∈ A with c = ab and a ,b ,c ∈ A with c = a ♦b . Let a = f (a),b = f (b),c = f (c) be the results of the mapping f (·). If f is a homomorphism, then the composition operation ♦ in the target domain A produces the same result as mapping the result of the operation applied to the two elements in the original domain A: f (a)♦f (b) = f (ab).

11.6 SECURITY OF DATABASE SERVICES

Cloud users delegate control of their data to **Database-as-a-Service (DBaaS)**, raising security concerns. DBaaS security is evaluated based on **data owners, users, CSPs, and third-party auditors (TPAs).**

Key Security Concerns

1. **Integrity, Confidentiality, and Availability**
    - Data loss occurs due to **poor authentication, authorization, and accounting** mechanisms.

- **Unencrypted data** is vulnerable to bugs, errors, and attacks.
- **Insider threats** arise from superusers misusing unlimited privileges.

2. **External Attacks**
   - Malicious attackers use **spoofing, sniffing, man-in-the-middle attacks, side-channeling,** and **illegal transactions** to launch **DoS attacks**.
   - **Data recovery from storage devices** is possible if CSPs do not perform **thorough scrubbing** after deletion.
   - **Data in transit** is at risk and should be **encrypted before transmission**.
3. **Data Provenance & Transparency Issues**
   - **Tracking data origins** using metadata is essential but computationally expensive.
   - Cloud users do not know their data's **physical location**, making it hard to track security breaches.
   - **Limited control** over remote execution environments prevents users from detecting illegal operations.
4. **Replication & Backup Challenges**
   - **Ensuring data consistency** across replicas is difficult.
   - **Timely backups** are essential for disaster recovery.
   - **Auditing and monitoring** help detect issues but introduce security risks when handled by TPAs.
5. **Legal & Compliance Risks**
   - **Privacy laws** in **Europe and South America** prohibit storing data outside the country of origin.
   - **Conventional auditing** requires knowledge of network infrastructure and storage locations, leading to **privacy concerns**.

Threats to DBaaS Security

- **Data Availability Risks**:
  - **Resource exhaustion** due to poor specification of user needs.
  - **Failures in consistency management** causing **inconsistent views of user data**.

    - **Monitoring and auditing failures** affecting security oversight.
- **Data Confidentiality Risks**:
    - **Insider & outsider attacks, access control issues, illegal data recovery, network breaches,** and **third-party access**.
    - **Inability to verify data provenance** compromises trust in data security.

11.7 OPERATING SYSTEM SECURITY

An **Operating System (OS)** allows multiple applications to share hardware resources while enforcing security policies. It must protect against **unauthorized access, tampering, and spoofing**. Even **single-user devices** like PCs, tablets, and smartphones can be vulnerable, especially when importing malicious code from **Java applets or harmful websites**.

Mandatory OS Security

- Defined by **system security policy administrators**.
- Includes **access control, authentication, and cryptographic usage policies**.
- OS security components must be **tamper-proof** and **non-bypassable**.
- Applications should operate within a **unique security domain**.

Trusted Applications & Security Policies

- Applications with **special privileges** must operate with **minimal privileges**.
- **Type enforcement** restricts trusted applications to **only necessary permissions**.
- **Discretionary security** (user-controlled) can lead to **security breaches**, while **mandatory security** (admin-controlled) prevents unauthorized changes.

Security Weaknesses in Commercial OS

- **Lack of multi-layered security**: OS often only distinguishes between **fully privileged** and **completely unprivileged** users.
- Some OS (e.g., **Windows NT**) allow programs to **inherit all privileges** of the invoking program.

Trusted Path Mechanisms

- **Prevent malicious software from impersonating trusted applications**.

- Solutions include decomposing mechanisms into **separate enforcer and decider components**:
    - **Enforcer**: Collects user and object information.
    - **Decider**: Determines access permissions.
    - **Enforcer** executes the decision.

Protecting Against Malicious Mobile Code

- **Java Security Manager** prevents unauthorized actions using a **sandbox** but is still vulnerable to **JVM bytecode manipulation**.
- **File system integrity** is crucial for securing Java class code.
- **Digitally signed applets** from trusted sources still have risks due to **all-or-nothing security models**.
- **Confining a browser to a separate security domain** can improve security.

Specialized vs. Open-Box Platforms

- **Closed-box platforms** (e.g., ATMs, game consoles, mobile phones) use **embedded cryptographic keys** for authentication.
- **Open-box platforms** (e.g., traditional PCs) **lack built-in identity verification** mechanisms.

Limitations of OS Security

- **OS security alone is insufficient**; application-specific security (e.g., digital signatures in e-commerce) is also needed.
- **OS complexity** (millions of lines of code) makes it **vulnerable to various attacks**.
- Weak isolation between applications: **Compromising one app can compromise the entire system**.
- Poor **authentication mechanisms**: Applications cannot reliably **authenticate one another**.
- No **trusted path between users and applications**, making it easier for **malicious programs to impersonate legitimate ones**.

Conclusion

- **Commodity OS offer low security assurance**.

- A compromised application can **endanger the entire platform**.
- These **weaknesses pose challenges** in distributed computing, **affecting financial transactions, user authentication, and data integrity**.

11.8 VIRTUAL MACHINE SECURITY

This discussion focuses on **traditional system VM security**, where a **hypervisor** manages hardware access. **Hybrid and hosted VM models** expose the system to OS vulnerabilities and are not analyzed.

Virtual Security Services

- **Hypervisor-based security**: The hypervisor provides security services.
- **Dedicated security VM**: A separate VM handles security functions.
- **Trusted Computing Base (TCB)**: If compromised, **the entire system is at risk**.

Hypervisor Security & VM Isolation

- Hypervisors provide **better VM isolation** than traditional OS process isolation.
- **Privileged operations** like memory, disk, and network access are controlled by the hypervisor.
- Hypervisors are **simpler and better structured** than traditional OS, making them more resilient to security attacks.

Guest VM Security & Cloning

- The **hypervisor can save, restore, clone, and encrypt VM states**.
- **Cloning helps identify malicious applications** by testing their behavior in a duplicate VM.
- Moving **guest VM files to a dedicated VM** can enhance security.
- **Inter-VM communication is faster** than between two physical machines, making this approach feasible.

VM Fingerprinting & Log Protection

- Attackers can **fingerprint VMs** to bypass honeypots.

- **VM log files** must be **securely protected** to prevent unauthorized access to sensitive data.

Cost of Virtualization Security

- **Higher hardware costs** (more CPU, memory, disk, and network bandwidth required).
- **Development costs** for hypervisors and OS modifications (in **paravirtualization**).
- **Virtualization overhead** due to hypervisor intervention in privileged operations.

VM-Based Intrusion Detection & Prevention

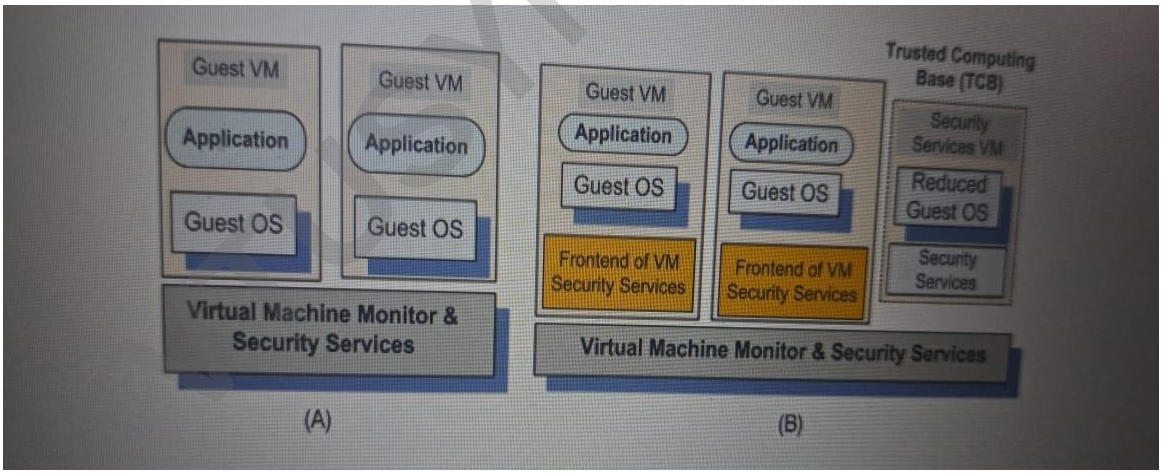
- **Intrusion detection systems** (IDS) like **Livewire** and **Siren** leverage VM capabilities for **isolation, inspection, and interposition**.
- **Intrusion prevention systems** (IPS) like **SVFS, NetTop, and IntroVirt** enhance VM security.
- **Terra** is a **VM-based trusted computing platform** that uses a **trusted hypervisor** for resource partitioning.
- 

Fig 11.3 (A) Virtual security services provided by the hypervisor/Virtual Machine Monitor; (B) A dedicated security VM.

Hypervisor-Based Threats (NIST Classification)

1. **Resource Starvation & Denial of Service (DoS)**
    - **Causes**:
        - Misconfigured **VM resource limits**.

        - A **rogue VM bypassing limits**.

2. **VM Side-Channel Attacks**
    - **Causes**:
        - **Misconfigured virtual network** leading to poor isolation.
        - **Packet inspection limitations** for high-speed traffic (e.g., video).
        - **Unpatched or insecure VM images**.
3. **Buffer Overflow Attacks**

VM-Based Threats

1. **Rogue or Insecure VM Deployment**
    - Unauthorized users may create **insecure instances** or modify existing VMs.
    - **Cause**: Poor access control on VM management tasks (e.g., creating, launching, suspending VMs).
2. **Tampered or Insecure VM Images**
    - **Causes**:
        - Lack of **access control in the VM image repository**.
        - No **integrity verification** (e.g., missing **digital signatures** on images).

11.10 SECURITY RISKS POSED BY SHARED IMAGES

Even if a cloud service provider is trustworthy, image sharing poses security risks, especially in the **IaaS cloud delivery model**. AWS users can choose from **Amazon Machine Images (AMIs)** available through Quick Start or Community AMI menus in EC2. First-time or less experienced users often select these AMIs without considering the security risks.

AMI Creation Process

- Starts from a **running system, another AMI, or a VM image**.
- **Bundling process**:
    1. Create an image
    2. Compress and encrypt the image

3. Split the image into segments and upload them to S3

- **Two procedures for AMI creation**:
    - ec2-bundle-image: Used for images as loopback files.
    - ec2-bundle-volume: Used for bundling running systems by copying file system data.

AMI Usage

- Users specify resources, provide credentials, configure firewalls, and choose a region.
- After instantiation, the **VM is available via a public DNS**.
- **Access methods**:
    - Linux: **SSH (port 22)**
    - Windows: **Remote Desktop (port 3389)**

Security Audit of Public AMIs

- **Study (Nov 2010 – May 2011)** analyzed **5,303 AMIs** from Amazon's public catalog.
- **Findings**:
    - **Sensitive data was easily recoverable**, including credentials and private keys.
    - Amazon acted promptly to mitigate threats.

Software Vulnerabilities

- **Windows AMIs**: 98% had critical vulnerabilities (**46 vulnerabilities per AMI**).
- **Linux AMIs**: 58% had critical vulnerabilities (**11 vulnerabilities per AMI**).
- **Old AMIs**:
    - 145, 38, and 2 Windows AMIs were **over 2, 3, and 4 years old**, respectively.
    - 1,197, 364, and 106 Linux AMIs were **over 2, 3, and 4 years old**, respectively.
- **Detection Tool**: Nessus classified vulnerabilities based on severity, focusing on **remote code execution**.

Security Risks

1. **Backdoors & Leftover Credentials**
    - **22% of Linux AMIs contained credentials** allowing remote login.

- **100 passwords, 995 SSH keys, and 90 instances with both were identified**.
- Malicious AMI creators could leave **their public keys** in the image, creating a backdoor.
- If **password-based authentication** is enabled, attackers can crack passwords with tools like **John the Ripper**.
- **Missing cloud-init script** leads to shared SSH keys, increasing **man-in-the-middle attack risks**.

2. **Unsolicited Connections**
   - Some **modified syslog daemons** forwarded logs (e.g., logins, web server requests) to external agents.
   - Distinguishing between **legitimate and malicious connections** is difficult.
3. **Malware**
   - **ClamAV scan** detected malware in **Windows AMIs**:
     - **Trojan-Spy (variant 50112)**: Keylogging, data theft, process monitoring.
     - **Trojan-Agent (variant 173287)**: Included a Firefox password recovery tool.

Risks for AMI Providers

- **Private keys, IP addresses, browser & shell history, and deleted files** can be recovered.
- **AWS API keys** can be stolen and misused to run cloud applications at the original owner's expense.
- **Unprotected SSH keys** (54 out of 56 had no passphrase) allow unauthorized access.
- **Stored IP addresses** in databases like lastlog and lastb expose user information.
- **Recovered shell history** (from 612 AMIs) revealed 160,000 command lines, including **74 credentials**.
- **GET requests in logs** could expose passwords and credit card numbers.
- **Deleted file recovery**:
  - 98% of AMIs contained recoverable files.
  - Files recovered ranged from **6 to 40,000 per AMI**.
  - Tools like shred, scrub, zerofree, and wipe should be used to prevent recovery.

Conclusion

Both **AMI users and providers** must be aware of **serious security risks** posed by **shared images**. Proper security measures are **essential** to protect credentials, prevent backdoors, and avoid malware infections.

11.11 SECURITY RISKS POSED BY A MANAGEMENT OS

Virtualization is often considered secure because a **hypervisor** is smaller than a traditional OS. For example, the **Xen hypervisor** has about **60,000 lines of code**, significantly fewer than an OS.

A hypervisor provides strong **VM isolation**, but it still depends on a **management OS** for VM creation and data transfer.

Security Concerns

- The **Trusted Computing Base (TCB)** includes both the **hypervisor** and **management OS**.
- The **management OS** handles:
    - VM creation
    - Live migration
    - Device drivers & emulators

Xen Vulnerabilities

- **21 out of 23 attacks targeted the control VM (Dom0).**
- **11 attacks** exploited buffer overflow vulnerabilities.
- **8 attacks** were **denial-of-service (DoS) attacks**.

Security Risks of Dom0

- **During VM Creation**:
    - Dom0 could **refuse to start a VM** (DoS attack).
    - Modify the guest OS for **monitoring and control**.
    - Alter **page tables and virtual CPU registers**, compromising integrity.
    - Retain access to VM memory after launch.
- **VM Creation Steps**:

1. Allocate memory in Dom0 and load the guest OS kernel.
2. Allocate memory for the new VM and use **foreign mapping** to load the kernel.
3. Set up initial **page tables**.
4. Release the foreign mapping, configure **virtual CPU registers**, and launch the VM.

A secure **virtualization architecture** must ensure **confidentiality, integrity, and availability** while restricting **untrusted Dom0 interactions** with guest VMs.

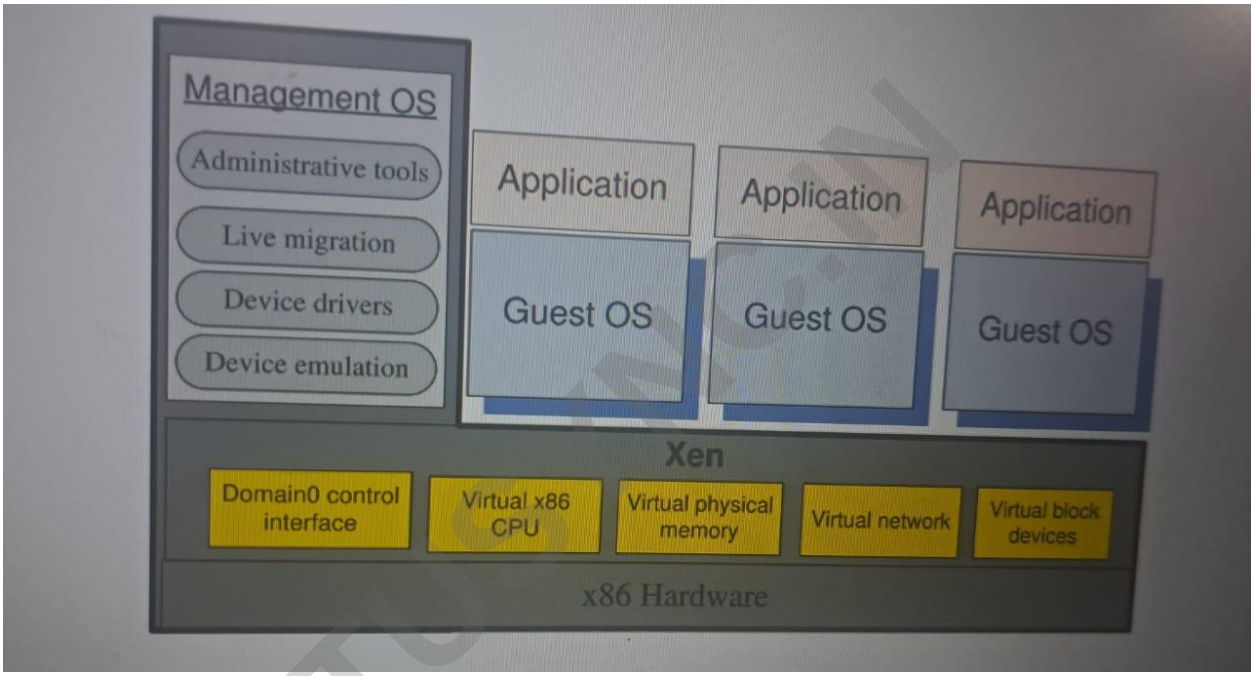


Fig 11.4 The trusted computing base of a Xen-based environment includes the hardware, Xen, and the management operating system running in Dom0. The management OS supports administrative tools, live migration, device drivers, and device emulators. A guest OS and applications running under it reside in a DomU.

A malicious Dom0 can play several nasty tricks at the time when it creates a DomU [302]:

• Refuse to carry out the steps necessary to start the new VM, an action that can be considered a denial-of-service attack.

• Modify the kernel of the guest OS in ways that will allow a third party to monitor and control the execution of applications running under the new VM.

• Undermine the integrity of the new VM by setting the wrong page tables and/or setup wrong virtual CPU registers.

• Refuse to release the foreign mapping and access the memory while the new VM is running.

11.12 XOAR – BREAKING THE MONOLITHIC DESIGN OF THE TCB

Xoar is a modified Xen version designed to enhance security. It assumes professional system management, restricting privileged access to administrators. Security threats come from guest VMs violating data integrity, confidentiality, or exploiting guest code, as well as bugs in the management VM's initialization code.

Xoar Design Principles

Xoar follows **microkernel** principles, ensuring modularity, reducing risk exposure, and enabling secure audit logging. Its goals include:

- Maintaining Xen functionality and transparency.
- Tight control of privileges, limiting each component's access.
- Reducing attack opportunities by limiting component runtime.
- Eliminating or explicitly managing sharing for better auditing.

Though modularity impacts performance, it minimizes the **Trusted Computing Base (TCB)** size, breaking Xen's monolithic design.

Xoar System Components

Xoar has four component types:

1. **Permanent** – XenStore-State maintains system state.
2. **Self-destructing** (used for booting) –
    - **PCIBack**: Virtualizes PCI bus access.
    - **Bootstrapper**: Coordinates system boot.
3. **Restarted on request** –
    - **XenStore-Logic**
    - **Toolstack**: Handles VM management.
    - **Builder**: Initiates user VMs.
4. **Restarted on timer** –

- **BlkBack**: Exports storage drivers.
- **NetBack**: Exports network drivers.

QEMU manages device emulation. **Bootstrapper and PCIBack** are destroyed after system initialization, while **Builder** (only 13,000 lines of code) remains.

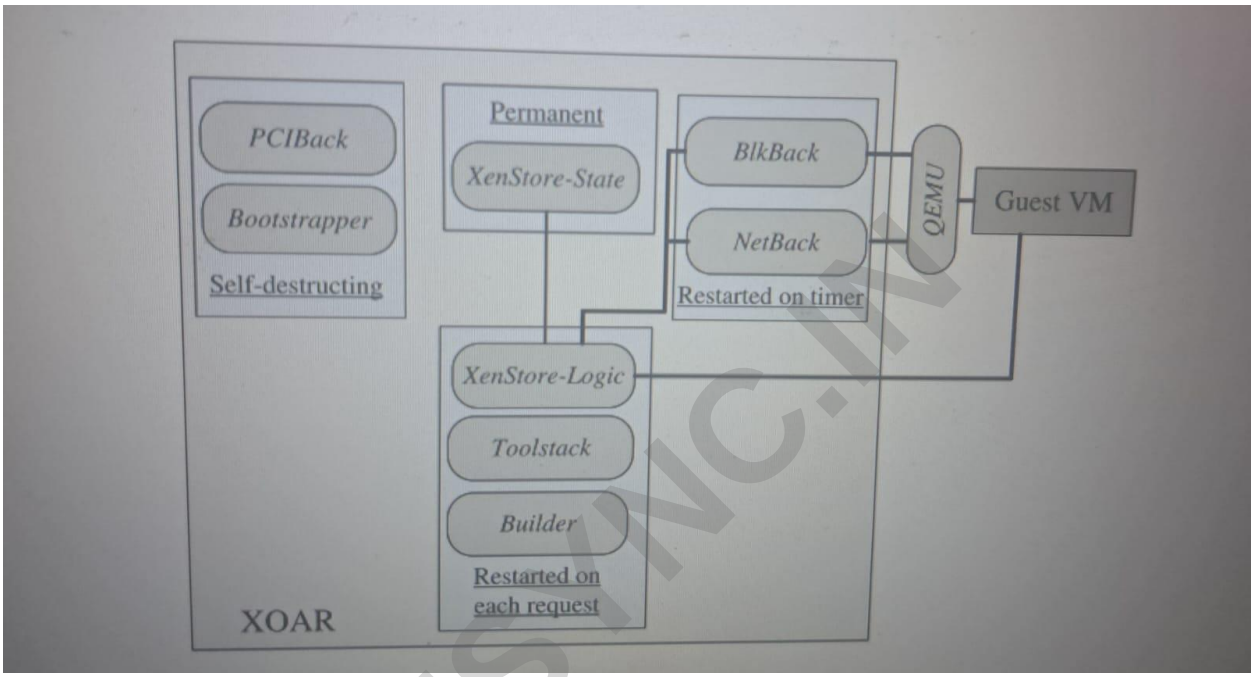


Fig 11.5 Xoar has nine classes of components of four types: permanent, self-destructing, restarted upon request, and restarted on timer. A guest VM is started using the Toolstack by the Builder and it is controlled by

Enhanced Security and Auditing

Xoar isolates shared service VMs, allowing users to control their access via device tags. Auditing is **secure and append-only**, with logs stored on a separate server.

Instead of rebooting, **snapshots** are used to restore a VM to a known good state, reducing overhead. Snapshots capture system states immediately after initialization, using **copy-on-write** to preserve modified pages.

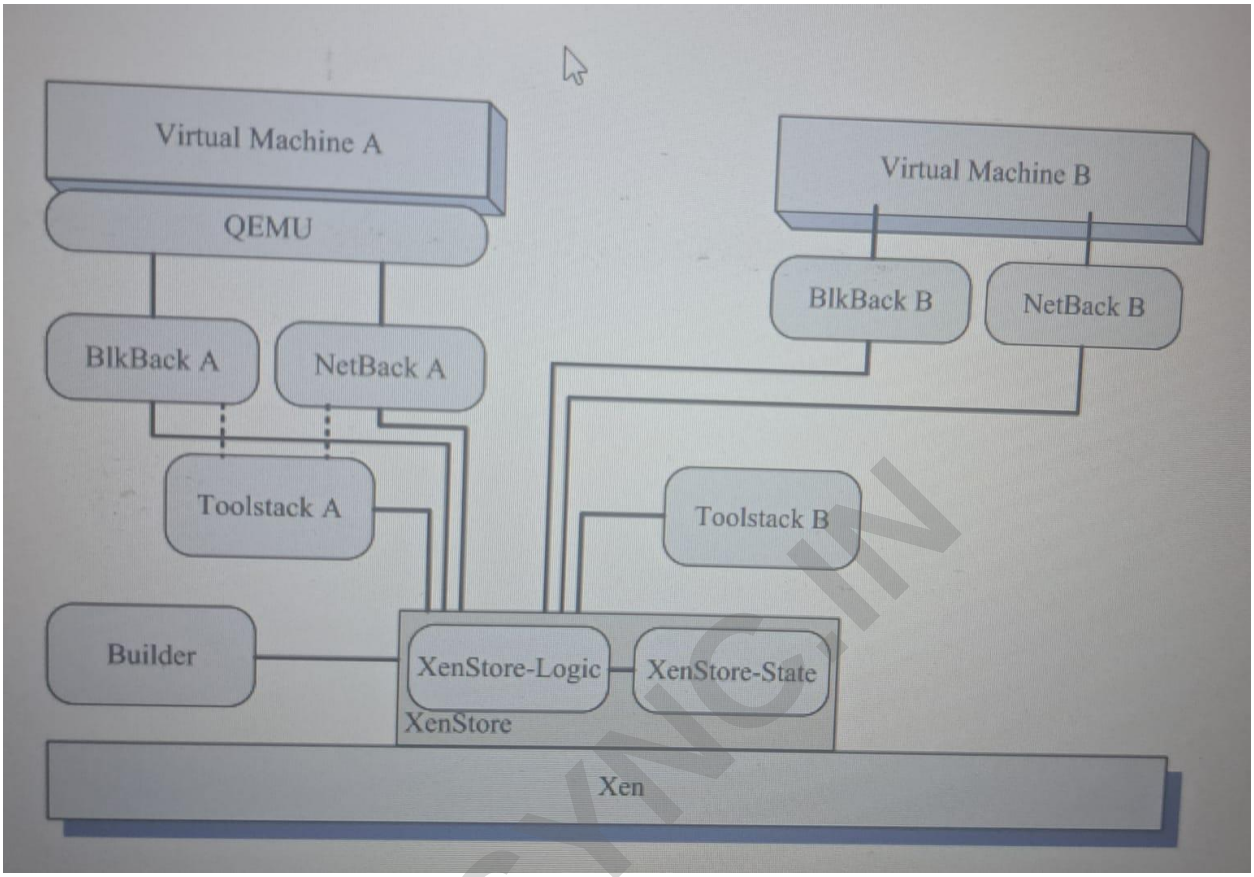


Fig 11.6 Component sharing between guest VM in Xoar. Two VM share only the XenStore components. Each one has a private version of the BlkBack, NetBack and Toolstack.

11.13 A TRUSTED HYPERVISOR

Terra is a trusted hypervisor designed to enhance security. Its key features include:

- **Support for both open-box and closed-box platforms**
    - Open-box: Traditional OS abstraction.
    - Closed-box: Prevents system content from being inspected or altered by the platform owner.
- **Customizable software stacks**
    - High-security applications (e.g., financial and voting systems) use a **thin OS** with only essential functions.
    - Low-security applications run on a **full-featured OS**.

    - **Information assurance (IA)** ensures **integrity, availability, authenticity, non-repudiation,** and **confidentiality** of application data.
- **Enhanced security capabilities**
    - **Trusted paths** ensure users interact with the correct VM.
    - **Attestation** allows applications in a closed-box to verify their identity cryptographically.
    - **Strict isolation** prevents the platform administrator from gaining root access.

Management VM and Guest VM Controls

- The **management VM** (chosen by the platform owner) controls:
    - Number of guest VMs.
    - Guest VM permissions (e.g., I/O access, CPU, memory, and disk usage).
- **Guest VMs** expose raw hardware interfaces, including virtual network and device interfaces.

Device Driver Security Risks

- **Device drivers** (especially for high-end wireless and video cards) are large, often poorly written, and pose security risks.
- To protect the **trusted hypervisor**, device drivers:
    - Should not access sensitive data.
    - Must be restricted by **hardware protection mechanisms**.
    - Should be prevented from using **DMA** to modify the kernel.

11.14 MOBILE DEVICES AND CLOUD SECURITY

Mobile devices are crucial to the cloud ecosystem, using cloud services for **data storage** and **computational tasks**. Security challenges for mobile devices, common to all systems, include:

1. **Confidentiality** – Prevent unauthorized access to stored and transmitted data.
2. **Integrity** – Detect modifications to data.
3. **Availability** – Ensure cloud resources are accessible.

4. **Non-repudiation** – Ensure a sender cannot deny sending a message.

Mobile Device Technology Stack

Includes **hardware, firmware, OS, and applications**. The **baseband processor**, responsible for cellular communication, operates independently from the **application processor** running the OS. Security hardware and firmware store **encryption keys, certificates, and credentials**.

Increased Security Risks

- **Frequent third-party app installations** from app stores.
- **Untrusted cellular and WiFi networks**.
- **Short authentication passcodes** and **weak storage encryption**.
- **Location services** exposing user movements, enabling **targeted attacks**.

Security Threats

1. **Mobile malware**.
2. **Data theft** due to loss or disposal.
3. **Unauthorized access**.
4. **Electronic eavesdropping**.
5. **Electronic tracking**.
6. **Third-party apps accessing sensitive data**.

Cloud Security Risks from Mobile Devices

- **Ransomware** affecting cloud backups.
- **Data leakage and compromise** due to:
    - **Device loss** and weak lock-screen protection (e.g., **smudge attacks** revealing password patterns).
    - **Insecure networks** lacking data encryption.
    - **Unpatched firmware or OS** (e.g., rooted/jailbroken devices).
    - **Malicious applications** bypassing security controls.

4.6 CLOUD SECURITY AND TRUST MANAGEMENT

Lack of trust between service providers and users hinders cloud computing adoption. Traditional trust models protected e-commerce platforms like eBay and Amazon. However, web and cloud services demand stronger security, as users resist fully relying on cloud providers. Concerns include privacy, security, and copyright protection. Trust is a social issue, but technology can enhance trust, reputation, and assurance. Cloud environments pose unique security threats, requiring new data-protection models. Some P2P and grid trust models can extend to cloud protection.

4.6.1 Cloud Security Defense Strategies

A healthy cloud ecosystem should prevent abuse, hacking, viruses, spam, and privacy violations. Security requirements differ for IaaS, PaaS, and SaaS, based on SLAs between providers and users.

4.6.1.1 Basic Cloud Security

Three key security enforcements exist. **Facility security** includes biometric readers, CCTV, motion detection, and man traps. **Network security** requires fault-tolerant firewalls, IDSes, and third-party vulnerability assessments. **Platform security** enforces SSL, data decryption, password policies, and system trust certification. Figure 4.31 maps security measures to cloud operating levels. Malware-based attacks like worms, viruses, and DDoS exploit system vulnerabilities, compromising functionality and unauthorized data access.

Thus, security defenses are needed to protect all cluster servers and data centers. Here are some cloud components that demand special security protection:

- Protection of servers from malicious software attacks such as worms, viruses, and malware
- Protection of hypervisors or VM monitors from software-based attacks and vulnerabilities
- Protection of VMs and monitors from service disruption and DoS attacks
- Protection of data and information from theft, corruption, and natural disasters
- Providing authenticated and authorized access to critical data and services

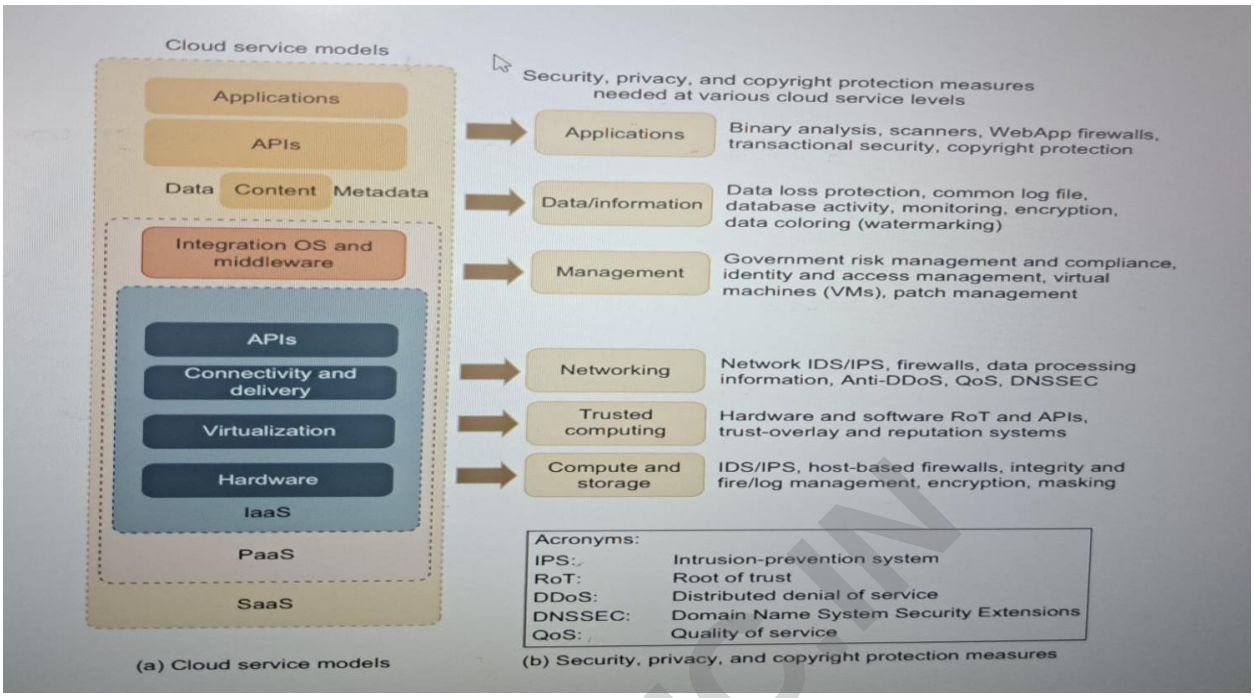


Fig 4.31 Cloud service models on the left (a) and corresponding security measures on the right (b); the IaaS is at the innermost level, PaaS is at the middle level, and SaaS is at the outermost level, including all hardware, software, datasets, and networking resources.

4.6.1.2 Security Challenges in VMs

Traditional network attacks include buffer overflows, DoS, spyware, malware, rootkits, Trojans, and worms. In cloud environments, new threats arise from hypervisor malware, guest hopping, VM hijacking, and rootkits. Man-in-the-middle attacks target VM migrations. Passive attacks steal sensitive data, while active attacks manipulate kernel structures, causing severe damage. IDS can be NIDS or HIDS, with program shepherding for code execution control. Defense tools include RIO dynamic optimization, VMware's vSafe and vShield, hypervisor compliance, Intel vPro, hardened OS environments, isolated execution, and sandboxing.

4.6.1.3 Cloud Defense Methods

Virtualization improves cloud security but introduces a failure risk. A physical machine can be partitioned into multiple VMs, ensuring isolation and protection from DoS attacks. Security threats in one VM do not spread to others. Hypervisors enhance guest OS visibility and enforce isolation. Fault containment strengthens security, while internet anomalies in routers and gateways can disrupt services. Trust negotiation is managed via SLAs, with PKI and reputation systems enhancing security. Worm and DDoS attacks require containment, as cloud security is challenging due to shared resources.

Table 4.9 Physical and Cyber Security Protection at Cloud/Data Centers

Protection Schemes	Brief Description and Deployment Suggestions
Secure data centers and computer buildings	Choose hazard-free location, enforce building safety. Avoid windows, keep buffer zone around the site, bomb detection, camera surveillance, earthquake-proof, etc.
Use redundant utilities at multiple sites	Multiple power and supplies, alternate network connections, multiple databases at separate sites, data consistency, data watermarking, user authentication, etc.
Trust delegation and negotiation	Cross certificates to delegate trust across PKI domains for various data centers, trust negotiation among certificate authorities (CAs) to resolve policy conflicts
Worm containment and DDoS defense	Internet worm containment and distributed defense against DDoS attacks to secure all data centers and cloud platforms
Reputation system for data centers	Reputation system could be built with P2P technology; one can build a hierarchy of reputation systems from data centers to distributed file systems
Fine-grained file access control	Fine-grained access control at the file or object level; this adds to security protection beyond firewalls and IDSes
Copyright protection and piracy prevention	Piracy prevention achieved with peer collusion prevention, filtering of poisoned content, nondestructive read, alteration detection, etc.
Privacy protection	Uses double authentication, biometric identification, intrusion detection and disaster recovery, privacy enforcement by data watermarking, data classification, etc.

4.6.1.4 Defense with Virtualization

VMs are decoupled from physical hardware and can be saved, cloned, encrypted, moved, or restored. They enable high availability and fast disaster recovery. Live VM migration supports distributed intrusion detection (DIDS). Multiple IDS VMs can be deployed across data centers, requiring trust negotiation in PKI domains. Security policy conflicts must be resolved at design time and updated regularly.

4.6.1.5 Privacy and Copyright Protection

Users expect predictable configurations before system integration. Yahoo!'s Pipes is an example of a lightweight cloud platform. Shared data raises privacy, security, and copyright concerns. Users seek software environments with robust tools for cloud applications over large data sets. Google's platform secures resources with in-house software, while Amazon EC2 employs HMEC and X.509 certificates. Secure clouds require:

- Dynamic web services with secure web technologies
- Trust through SLAs and reputation systems
- User identity and data-access management

- Single sign-on/off for security efficiency
- Auditing and copyright compliance enforcement
- Control shift from clients to cloud providers
- Protection of sensitive data in shared environments

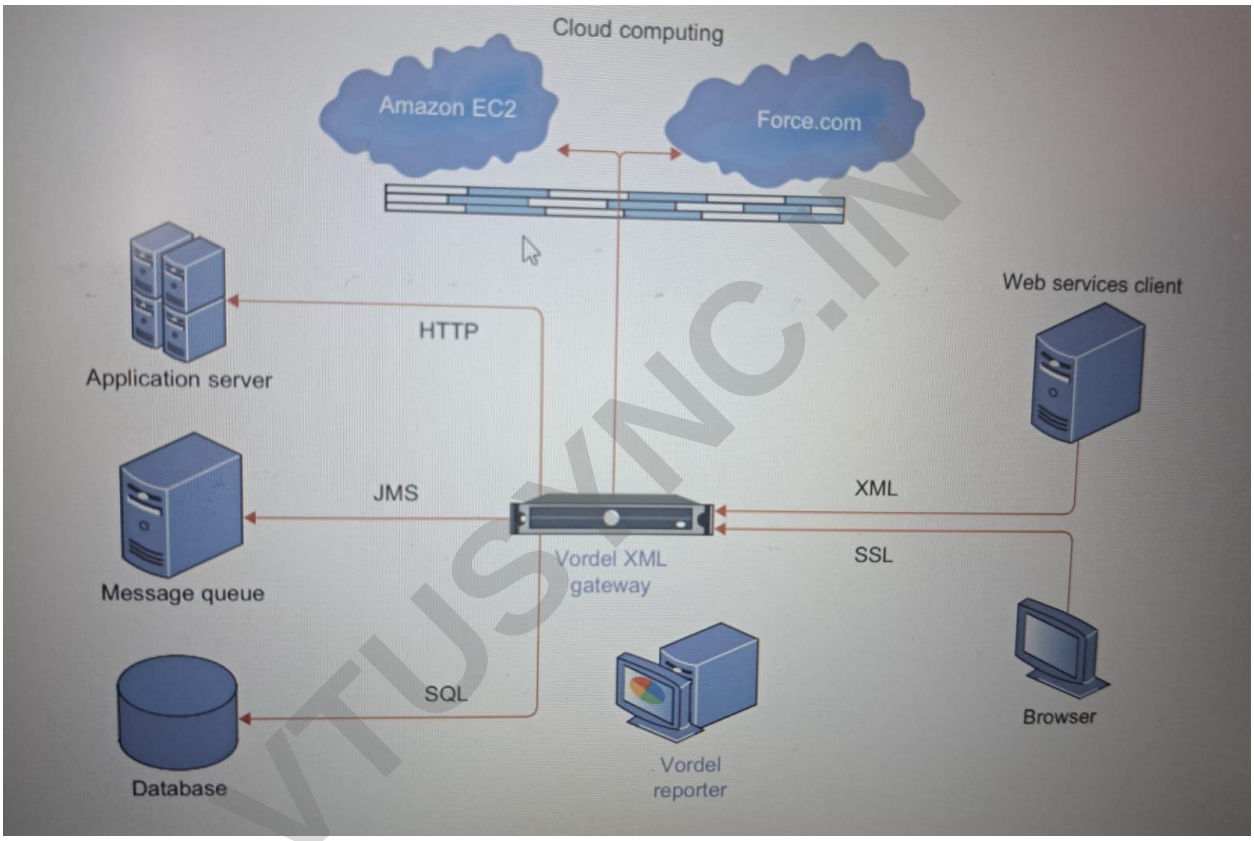


Fig 4.32 The typical security structure coordinated by a secured gateway plus external firewalls to safeguard the access of public or private clouds.

4.6.2 Distributed Intrusion/Anomaly Detection

Data security is the weakest link in cloud models. New cloud security standards must use common API tools to address data lock-in and network attacks. IaaS, like Amazon's model, is highly vulnerable. Role-based interface tools simplify provisioning, as seen in IBM's Blue Cloud. Many IT companies offer cloud services without security guarantees.

Threats target VMs, guest OSes, and software in the cloud. IDSes work to prevent these attacks. Signature-matching IDS is well-developed but requires frequent updates, while anomaly

detection identifies abnormal traffic patterns. Distributed IDSes are essential to counter both intrusion types.

4.6.2.1 Distributed Defense against DDoS Flooding Attacks

DDoS defense must cover multiple network domains in a cloud platform, including edge networks. DDoS attacks, often spread by worms, cause buffer overflow, disk exhaustion, or connection saturation.

The attack follows a tree pattern, with traffic surging through transit routers. A defense system based on change-point detection in routers identifies anomalies before overwhelming the victim. This scheme is effective for cloud core networks, reducing the need for edge network intervention.

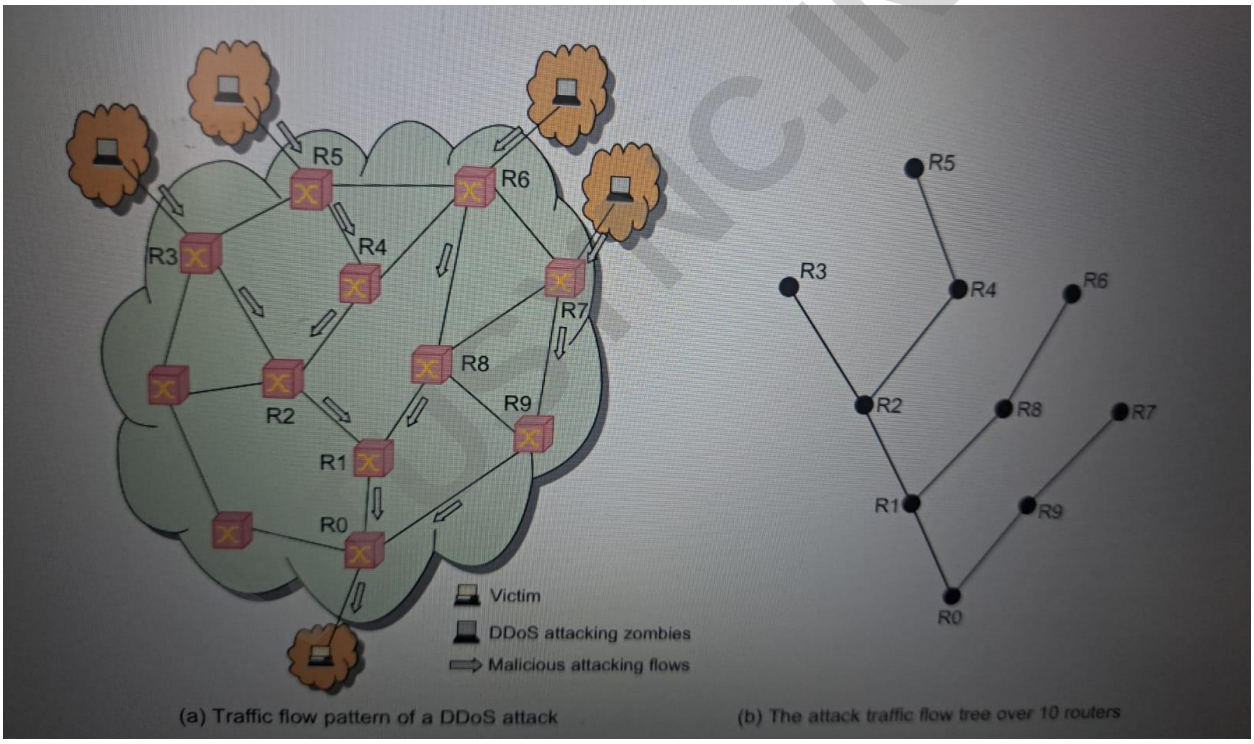


Fig 4.33 DDoS attacks and defense by change-point detection at all routers on the flooding tree

4.6.3 Data and Software Protection Techniques

This section introduces data coloring for integrity and privacy protection, followed by a watermarking scheme to prevent unauthorized software distribution.

4.6.3.1 Data Integrity and Privacy Protection

Users need secure software environments for cloud applications over large data sets. Security software should provide:

- Special APIs for authentication and email services
- Fine-grained access control to protect data integrity
- Protection for shared data against malicious alteration or deletion
- Security against ISP or cloud provider privacy invasion
- Personal firewalls to block Java, JavaScript, and ActiveX threats
- Privacy policies aligned with cloud providers to prevent identity theft
- VPN channels securing critical data transmissions

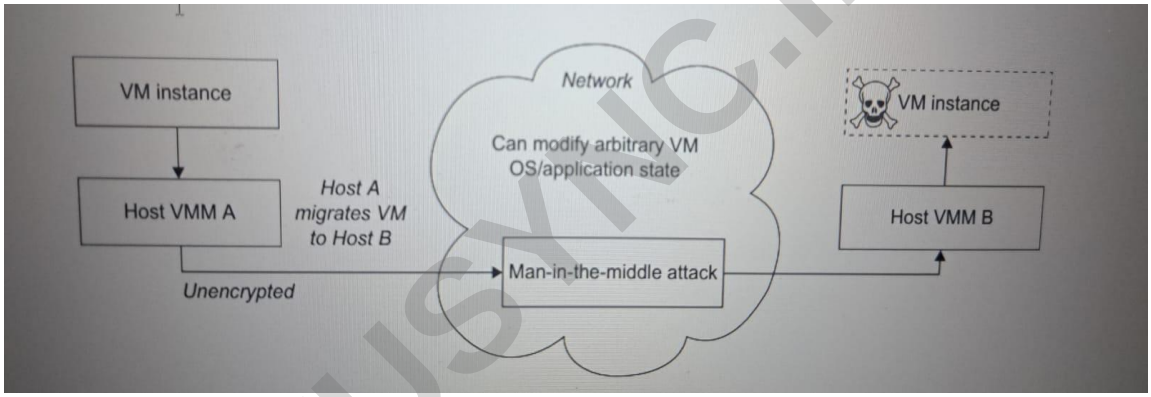


Fig 4.34 A VM migrating from host A to host B through a vulnerable network threatened by a man-in-the-middle attack to modify the VM template and OS state.

4.6.3.2 Data Coloring and Cloud Watermarking

Cloud environments risk privacy, security, and copyright breaches. Users seek trusted environments with tools for cloud applications. Watermarking, initially for digital copyright, now includes data coloring, assigning unique colors to data objects for identification. User identity is also colored for trust management. Cloud storage enables watermark generation, embedding, and extraction. Unlike encryption, data coloring is computationally efficient and can be combined with cryptography for enhanced protection.

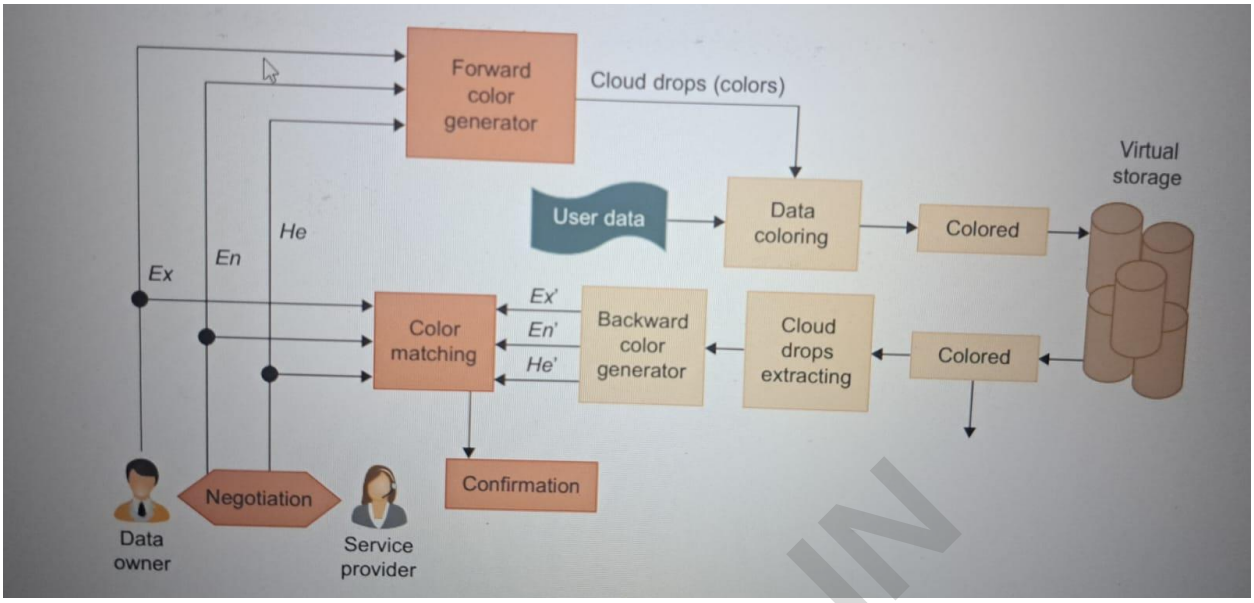


Fig 4.35 Data coloring with cloud watermarking for trust management at various security clearance levels in data centers.

4.6.3.3 Data Lock-in Problem and Solutions

Cloud computing centralizes computation and data in provider-managed servers. Users struggle to extract data for use on different platforms, leading to a **data lock-in problem** due to:

- **Lack of interoperability**—proprietary APIs restrict data extraction
- **Lack of compatibility**—clouds require users to rewrite applications from scratch

4.6.4 Reputation-Guided Protection of Data Centers

Trust is subjective and personal, while reputation is public and objective, relying on opinion aggregation. Reputation changes over time, with recent evaluations preferred. This section reviews reputation systems for securing data centers and cloud user communities.

4.6.4.1 Reputation System Design Options

Reputation reflects the collective evaluation of an entity's reliability. Many reputation systems were developed for P2P, multiagent, and e-commerce systems. These can be adapted for cloud security. Reputation systems are classified as **centralized** or **distributed**. Centralized systems are easier to implement but require strong server resources, while distributed systems are more scalable and failure-resistant.

At the second tier, reputation systems are further categorized:

- **User-oriented** (individual reputation, common in P2P networks)
- **Resource-oriented** (applies to cloud services and data centers)

Centralized reputation systems exist in commercial platforms like eBay, Google, and Amazon. Academic institutions developed distributed reputation models such as Eigentrust (Stanford), PeerTrust (Georgia Tech), and PowerTrust (USC). These models can be adapted to protect cloud resources.

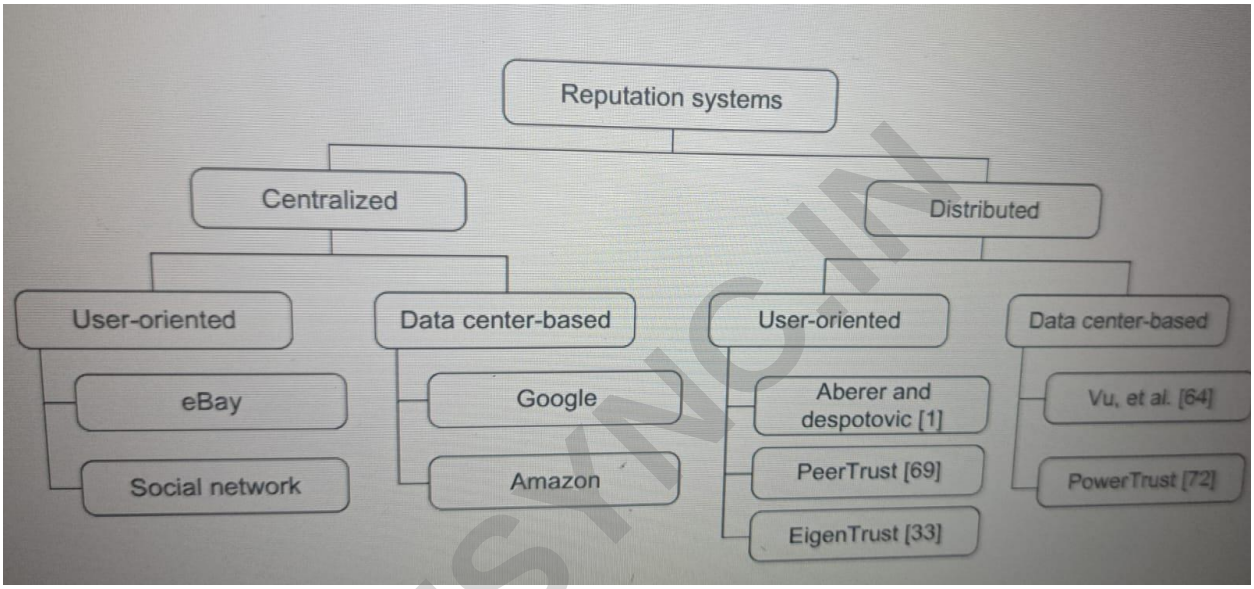


Fig4.36

4.6.4.2 Reputation Systems for Clouds

Reputation systems adapted for cloud data centers enhance security by ensuring data integrity, preventing unauthorized updates, and tracking breaches. Providers are responsible for data consistency, while users control access keys. A **trust overlay network** can protect resources at site and file levels, requiring coarse- and fine-grained access control.

Cloud reputation systems also support **safe VM cloning** and security mechanisms like:

- **Secured logging**
- **Migration over virtual LANs**
- **ECC-based encryption**
- **Sandboxed execution for security testing**

These measures enhance cloud protection and service quality.

4.6.4.3 Trust Overlay Networks

Reputation-based trust overlays support trusted cloud services. A **two-layer trust overlay network** was suggested:

- **Bottom layer**: Manages trust negotiation, authentication, access control, and data integrity.
- **Top layer**: Facilitates virus signature generation, worm containment, and copyright protection.

Content poisoning can prevent copyright violations. Matching **colored user identifications with data objects** strengthens privacy. Security enforcement in cloud data centers integrates reputation systems and watermarking for access control.

A new **Security as a Service (SaaS)** model is needed for trusted, global cloud computing. Standardized cloud interoperability is crucial for a secure, efficient cloud ecosystem.