Cloud Security: Top concern for cloud users, Risks, Privacy Impact Assessment, Cloud Data Encryption, Security of Database Services, OS security, VM Security, Security Risks Posed by Shared Images and Management OS, XOAR, A Trusted Hypervisor, Mobile Devices and Cloud Security

Cloud Security and Trust Management: Cloud Security Defense Strategies, Distributed Intrusion/Anomaly Detection, Data and Software Protection Techniques, Reputation-Guided Protection of Data Centers.

SECURITY, THE TOP CONCERN FOR CLOUD USERS

Cloud computing offers convenience and cost savings, but security and privacy concerns remain significant. Users must trust cloud service providers (CSPs) with their sensitive data, yet security threats like unauthorized access, insider attacks, and data theft persist.

Key concerns include:

1. **Data Security Risks** – Stored data is more vulnerable than data in transit or processing, requiring strong encryption and server security.
2. **Loss of User Control** – Users cannot always verify if deleted data is permanently erased, as CSPs perform backups without user consent.
3. **Standardization Issues** – Lack of industry-wide standards creates challenges in interoperability, auditing, and compliance.
4. **Legal Uncertainties** – Data stored across different countries raises questions about jurisdiction and legal protections.
5. **Emerging Technologies** – Future developments like autonomic computing may introduce new security challenges.
6. **Multi-Tenancy Risks** – Shared environments can expose private data if security measures fail.
7. **Contractual Protections** – Users should ensure clear agreements outlining data handling, security obligations, liabilities, and storage locations.
8. **Minimizing Risks** – Encrypting sensitive data and carefully evaluating CSP security policies can help mitigate threats.

While cloud computing is valuable, security remains a top priority, requiring vigilance and proactive measures.

CLOUD SECURITY RISKS

Cloud computing offers great benefits but also serious security challenges. The main risks and concerns include:

1. **Traditional Security Threats** – Cloud environments amplify familiar cyber risks like phishing, SQL injection, cross-site scripting, and distributed denial-of-service (DDoS) attacks.

VTUSYNC.IN

2. **Authentication & Authorization Issues** – Managing user access and privilege levels in an organization can be complex.
3. **Multi-Tenancy Vulnerabilities** – Sharing cloud resources with other users can expose sensitive data if security measures fail.
4. **System Availability Concerns** – Outages, power failures, or catastrophic events can disrupt access to cloud services.
5. **Third-Party Control & Transparency** – Outsourced cloud services can lead to data leaks, trust issues, or poor infrastructure security.
6. **Data Ownership & Liability** – Service providers may absolve themselves of responsibility, leaving users vulnerable in case of data breaches or loss.
7. **Audit & Compliance Challenges** – Ensuring proper security and legal compliance remains difficult due to a lack of transparency.

To minimize risks, users should enforce strong security policies, encrypt sensitive data, and ensure clear contractual agreements with cloud providers. Proactive security measures and due diligence are key to protecting cloud-based assets.

The Cloud Security Alliance (CSA) reports from 2010 and 2011 highlight key threats in cloud computing:

2010 CSA Report - Seven Major Threats

1. **Abusive Use of Cloud** – Using cloud resources for **malicious activities** like spam or cyberattacks.
2. **Insecure APIs** – Weak authentication and access controls **expose users** to security risks.
3. **Malicious Insiders** – CSP employees could **misuse access** to confidential data.
4. **Shared Technology Risks** – Multi-tenant architectures and **virtualization flaws** pose security threats.
5. **Account Hijacking** – **Stolen credentials** can lead to unauthorized access.
6. **Data Loss/Leakage** – Failures in **backup, replication, or encryption** may lead to permanent loss or theft.
7. **Unknown Risk Profile** – Users may **underestimate security risks**, leading to vulnerabilities.

2011 CSA Report - Attack Classification

- **Three key actors:** User, Service, Cloud Infrastructure.
- **Common attacks: SSL spoofing, phishing, SQL injection, privilege escalation.**
- **Cloud-specific threats: Data distortion, excessive resource usage, multi-tenancy vulnerabilities.**

VTUSYNC.IN

To mitigate these risks, organizations should enforce **strong authentication, encryption, auditing, and secure API practices** while selecting trusted cloud service providers. Security awareness and proactive measures are key to safer cloud usage.

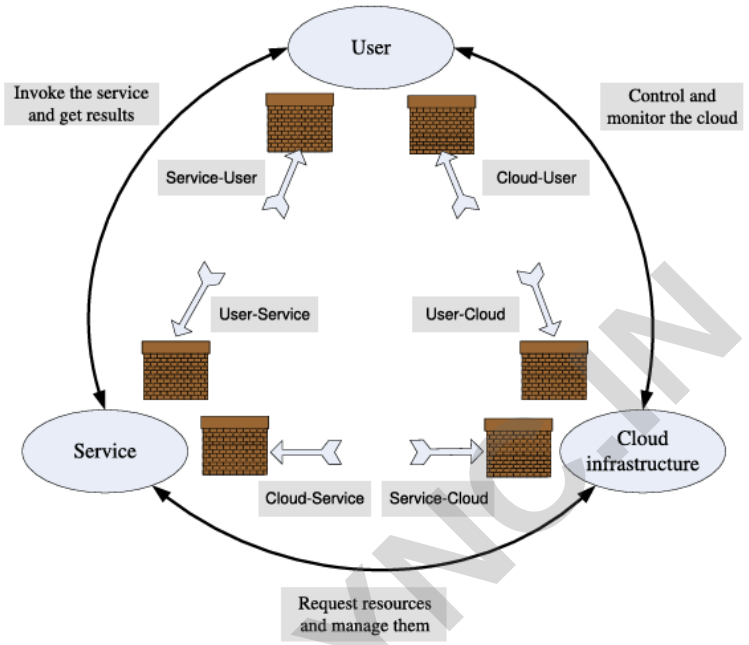

FIGURE 11.1
Surfaces of attacks in a cloud computing environment.

VTUSYNOIN

The 2016 Cloud Security Alliance (CSA) report outlines the **top 12 cloud security threats**:

1. **Data Breaches** – Sensitive data (financial, health, intellectual property) is at risk. **Multi-factor authentication and encryption** help mitigate this.
2. **Compromised Credentials & Weak Authentication** – **Poor passwords, insecure keys**, and certificate mismanagement increase risks.
3. **Insecure APIs** – Weak authentication and exposed credentials can lead to **security breaches**.
4. **System Vulnerabilities** – Multi-tenancy creates **attack surfaces**, making **patching and monitoring critical**.
5. **Account Hijacking** – Monitoring **every transaction** helps trace unauthorized access.
6. **Malicious Insiders** – Insider threats require **strict access control, auditing, and logging**.
7. **Advanced Persistent Threats (APTs)** – **Long-term cyber espionage** aimed at stealing confidential data.
8. **Permanent Data Loss** – Lack of proper **data backup strategies** can cause irreversible loss.

9. **Inadequate Diligence** – Failure to assess security policies before migrating to the cloud increases exposure.
10. **Cloud Service Abuse** – Misuse of **cloud computing power for cyberattacks**.
11. **Denial-of-Service (DoS) Attacks** – Overloading cloud services to **disrupt availability**.
12. **Shared Technology Threats** – Multi-tenancy risks include **hypervisor vulnerabilities** that expose users.

Additional risks include **natural disasters, hardware failures, malware, cyber-espionage, insider misuse, and web application attacks**. Organizations should **follow security best practices, encrypt data, and conduct regular audits** to mitigate these threats.

PRIVACY AND PRIVACY IMPACT ASSESSMENT

Privacy is the right to keep personal or proprietary information from unauthorized disclosure. Many countries recognize privacy as a fundamental right, but laws vary across regions.

Key Privacy Concerns in Cloud Computing:

1. Lack of User Control – Once data is stored on cloud servers, users may lose control over access and location.
2. Unauthorized Secondary Use – Cloud providers may use personal data for targeted advertising without user consent.
3. Data Proliferation & Outsourcing Risks – Subcontracting makes it unclear who manages and secures the data.
4. Legislation Challenges – Privacy laws differ globally, complicating enforcement and compliance.
5. Consumer Protection Measures – The U.S. Federal Trade Commission recommends notice, choice, access, and security for websites collecting personal data.
6. Privacy Impact Assessments (PIA) – Tools help organizations identify risks, ensure compliance, and embed privacy safeguards from the start.

A proactive approach to privacy protection—including encryption, secure policies, and robust legislation—is essential in the digital age.

VTUSYNC.IN

CLOUD DATA ENCRYPTION

Encryption is a key solution for securing sensitive data on public clouds. Cloud providers like **AWS Key Management Service (KMS)** offer encryption tools to protect user data across various services.

Notable Advances in Cloud Cryptography:

1. **RSA Encryption** – A foundational public-key cryptosystem for secure data transmission.
2. **Paillier Cryptosystem (1999)** – Uses **trapdoor mechanisms** based on factoring large numbers.
3. **Fully Homomorphic Encryption (FHE, 2009)** – Allows computations on **encrypted data** without decryption.
4. **Searchable Symmetric Encryption** – Enables secure searching within encrypted databases.

By leveraging encryption techniques like **homomorphic encryption, key management, and secure cryptographic protocols**, cloud users can significantly enhance data privacy and security.

Homomorphic encryption

Homomorphic encryption enables computations on **encrypted data** without needing decryption, eliminating a security vulnerability.

Key Aspects of Homomorphic Encryption:

1. **Encryption & Computation** – Allows arithmetic and logic operations to be performed directly on encrypted data.
2. **Eliminating Vulnerability** – Prevents exposure during processing, enhancing security.
3. **Challenges** – Fully Homomorphic Encryption (FHE) is **not yet practical** due to extreme computational overhead.
4. **Database Limitations** – Searching encrypted databases faces **performance issues**, as encryption prevents efficient indexing.

Despite its promise, **homomorphic encryption remains inefficient for large-scale cloud applications** due to processing delays and complexity. Advancements are needed before it becomes widely viable.

Order Preserving Encryption (OPE)

Order Preserving Encryption (OPE) allows encryption of numeric data while preserving the order of values, making **range queries** on encrypted data feasible.

Key Aspects of OPE:

1. **Order Preservation** – Maps numerical values into a **larger, sparse range** while maintaining their order.
2. **Encryption Process** – Uses **binary search** and the **negative hypergeometric distribution (NHG)** for ciphertext assignment.
3. **Efficient Queries** – Allows **order-preserving hash functions** for efficient searches on encrypted data.

VTUSYNC.IN

4. **Searchable Symmetric Encryption (SSE)** – Protects **database queries** from explicit data leakage while enabling **single-keyword, multi-keyword, ranked, and Boolean searches**.
5. **Private Cloud Risks** – While **firewalls** protect against outsiders, insider threats remain a concern. **Access restrictions and monitoring** help mitigate risks.

By utilizing **OPE and SSE**, encrypted databases can support efficient searches while enhancing data security. However, **insider threats and query pattern exposure** require additional safeguards.

SECURITY OF DATABASE SERVICES

DBaaS allows cloud users to store and manage their data, but security risks include data integrity, confidentiality, and availability concerns.

Major Security Threats:

1. Authorization & Authentication Issues – Weak access controls can lead to data leaks or unauthorized modifications.
2. Encryption & Key Management – Poor encryption handling exposes data to external attacks.
3. Insider Threats – Superusers with excessive privileges may misuse confidential data.
4. External Attacks – Methods like spoofing, sniffing, man-in-the-middle, and DoS attacks can compromise cloud databases.
5. Multi-Tenancy Risks – Shared environments increase data recovery vulnerabilities if proper sanitation isn't enforced.
6. Data Transit Risks – Without encryption, data transfer over public networks is vulnerable.
7. Data Provenance Challenges – Tracking data origin and movement requires complex metadata analysis.
8. Lack of Transparency – Users may not know where their data is stored, complicating security assessments.
9. Replication & Consistency Issues – Synchronizing data across multiple cloud locations is difficult.
10. Auditing & Compliance Risks – Third-party audits can violate privacy laws if data is stored in restricted locations.

Mitigation Strategies:

- Implement **strong authentication and authorization protocols**.
- Use **robust encryption** for stored and transmitted data.
- Restrict **superuser access** and enforce **logging and monitoring**.
- Conduct **regular audits** while ensuring legal compliance.

VTUSYNC.IN

- Optimize **data replication and consistency mechanisms** for reliability.

Cloud databases enhance efficiency, but **proper security measures** are essential to prevent unauthorized access, data breaches, and operational failures.

OPERATING SYSTEM SECURITY

An OS manages hardware resources while protecting applications from **malicious attacks** like unauthorized access, code tampering, and spoofing. Security policies include **access control, authentication, and cryptographic protection**.

Key Security Concerns:

1. **Mandatory vs. Discretionary Security** – Mandatory policies enforce strict security, while discretionary policies **leave security decisions to users**, increasing risks.
2. **Trusted Paths & Applications** – Trusted software needs **secure communication mechanisms** to prevent impersonation.
3. **OS Vulnerabilities** – Commodity OSs often **lack multi-layered security**, making them susceptible to privilege escalation.
4. **Malicious Software Threats** – **Java Security Manager** uses sandboxing but **cannot prevent all security bypasses**.
5. **Closed vs. Open Systems** – **ATMs, smartphones, and game consoles** have embedded cryptographic keys for **stronger authentication**.
6. **Weak Isolation Between Applications** – A compromised app **can expose the entire system**.
7. **Application-Specific Security** – Certain applications, like **e-commerce**, require **extra protection like digital signatures**.
8. **Challenges in Distributed Computing** – OS security gaps affect **application authentication and secure user interactions**.

A **secure OS is crucial**, but additional security measures like **encryption, auditing, and authentication** are necessary for comprehensive protection.

VIRTUAL MACHINE SECURITY

Virtual Machine (VM) security primarily relies on **hypervisors** for isolation and access control, reducing risks compared to traditional OS security.

VTUSYNC.IN

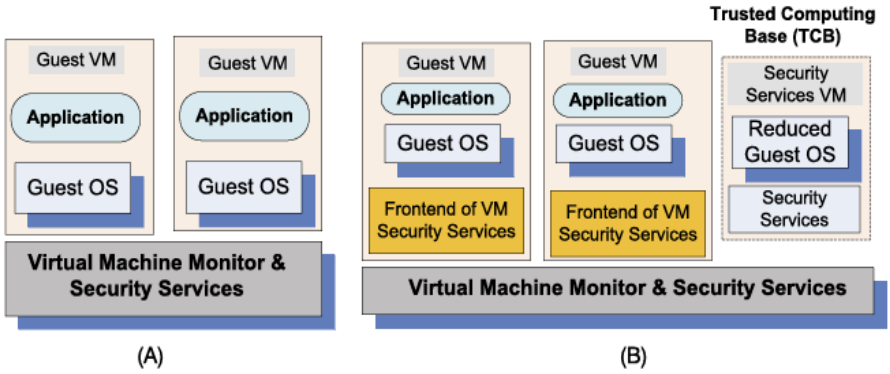

FIGURE 11.3

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

Key Aspects of VM Security:

1. **Hypervisor-Based Security** – Ensures **memory, disk, and network isolation** for VMs.
2. **Trusted Computing Base (TCB)** – A compromised TCB affects **entire system security**.
3. **VM State Management** – Hypervisors can **save, restore, clone, and encrypt VM states**.
4. **Attack Prevention** – Dedicated security VMs and **intrusion detection systems** enhance protection.
5. **Inter-VM Communication** – **Faster than physical machines**, enabling **secure file migration**.

Security Threats:

Hypervisor-Based Threats:

- **Resource starvation & DoS** due to misconfigured limits or rogue VMs.
- **VM side-channel attacks** exploiting weak inter-VM isolation.
- **Buffer overflow vulnerabilities** in hypervisor-managed processes.

VM-Based Threats:

- **Deployment of rogue or insecure VMs** due to weak administrative controls.
- **Tampered VM images** from insecure repositories lacking integrity checks.

Mitigation Strategies:

- Enforce **strong access controls** and **isolate inter-VM traffic**.
- Use **digitally signed VM images** to ensure integrity.
- Implement **intrusion detection & prevention systems** for proactive security.

Virtualization enhances security but requires **proper configurations, access control, and monitoring** to prevent exploits.

VTUSYNC.IN

SECURITY RISKS POSED BY SHARED IMAGES

Introduction to AMI Security Risks

-Shared AMIs may pose serious security threats.

- Public/Community AMIs are often chosen by inexperienced users.

- Risks include outdated software, embedded credentials, malware.

AMI Creation Process

- Created from running systems, other AMIs, or VM images.

- Tools: ec2-bundle-image, ec2-bundle-volume.

- Process: Image -> Compress/Encrypt -> Split -> Upload to S3.

Key Security Issues Identified

1. Use of Public AMIs

- Easy for new/inexperienced users to choose vulnerable Community or Quick Start AMIs.
- Many AMIs are outdated and poorly maintained.

2. Vulnerability Audit Findings

- **Windows AMIs**: 98% had critical vulnerabilities; average of 46 per image.
- **Linux AMIs**: 58% had critical vulnerabilities; average of 11 per image.
- Many AMIs were 2–4 years old.

3. Backdoors & Leftover Credentials

- 22% of Linux AMIs had accessible credentials:
  - 100 passwords, 995 SSH keys, 90 AMIs with both.
- SSH backdoors via:
  - Leftover SSH public keys.
  - Enabled password authentication.
- SSH passwords can be cracked using tools like **John the Ripper**.

4. Missing cloud-init Script

- Prevents regeneration of unique SSH host keys.
- Leads to **man-in-the-middle (MITM)** attack risks using tools like **NMap**.

5. Unsolicited External Connections

- Modified daemons forwarded logs (e.g., syslog) to external agents.
- Exfiltrates sensitive system activity and metadata.

VTUSYNC.IN

6. Malware Detection

- Two Windows AMIs found with Trojans:
    - Keylogging, data theft, and password recovery tools detected using **ClamAV**.

Privacy Risks for AMI Creators

- Recoverable sensitive data included:
    - **AWS API keys**, **SSH keys**, **passwords**, **browser history**, **command history**, etc.
- 98% of AMIs allowed deleted file recovery (up to 40,000 files).
- 612 AMIs contained shell history files (e.g., .bash_history).
- 187 AMIs had login databases (lastb) with >66,000 entries.

Security Recommendations

For AMI Users:

- Avoid community AMIs if possible.
- Use official or custom-built, regularly updated images.
- Run **security audits** before use.
- Regenerate SSH keys and credentials after launch.

For AMI Creators:

- Remove sensitive data and credentials.
- Disable password-based SSH logins.
- Include the cloud-init script.
- Use tools like shred, wipe, or scrub to securely delete data.

VTUSYNC.IN

SECURITY RISKS POSED BY A MANAGEMENT OS

- ✓ Virtualization enhances security by isolating VMs, and Xen's hypervisor is relatively small, making it easier to analyze.
- ✓ However, risks remain since Xen relies on a management OS (Dom0) for VM creation and data transfer. The Trusted Computing Base (TCB) includes both the hypervisor and Dom0, which introduces vulnerabilities.
- ✓ Most attacks target Dom0 services, exploiting buffer overflows and denial-of-service tactics. While a smaller hypervisor reduces complexity, securing Dom0 and its interactions with guest VMs is crucial to maintaining system integrity.
- ✓ Xen hypervisor enhances security with strong VM isolation and a smaller codebase, but vulnerabilities exist in its management OS (Dom0).

- ✓ Dom0 handles VM creation and resource management but can be exploited through denial-of-service attacks, kernel modifications, and unauthorized memory access.
- ✓ Encryption and strict hypercall controls are necessary to safeguard VM integrity.
- ✓ A secure architecture must restrict Dom0's access to VM memory, enforce encrypted communication, and perform integrity checks. While improved security increases overhead, these protections are essential for a trusted virtualization environment.

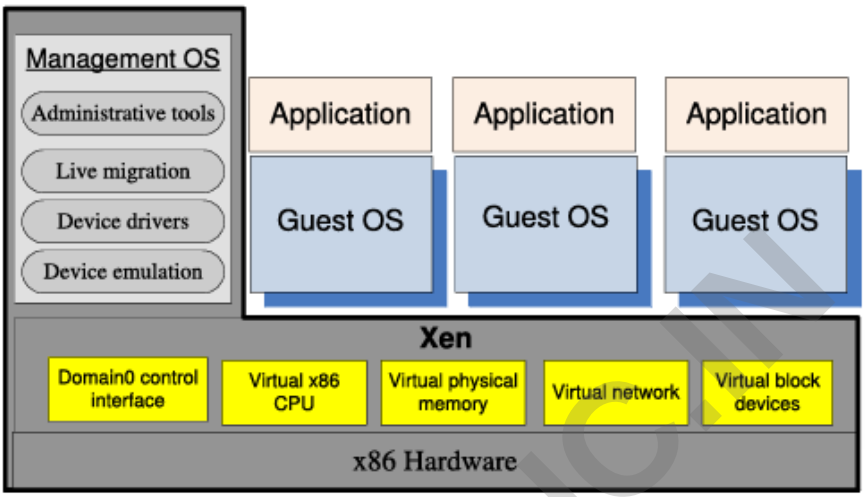

FIGURE 11.4

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.

VTUSYNC.IN

VTUSYNC.IN