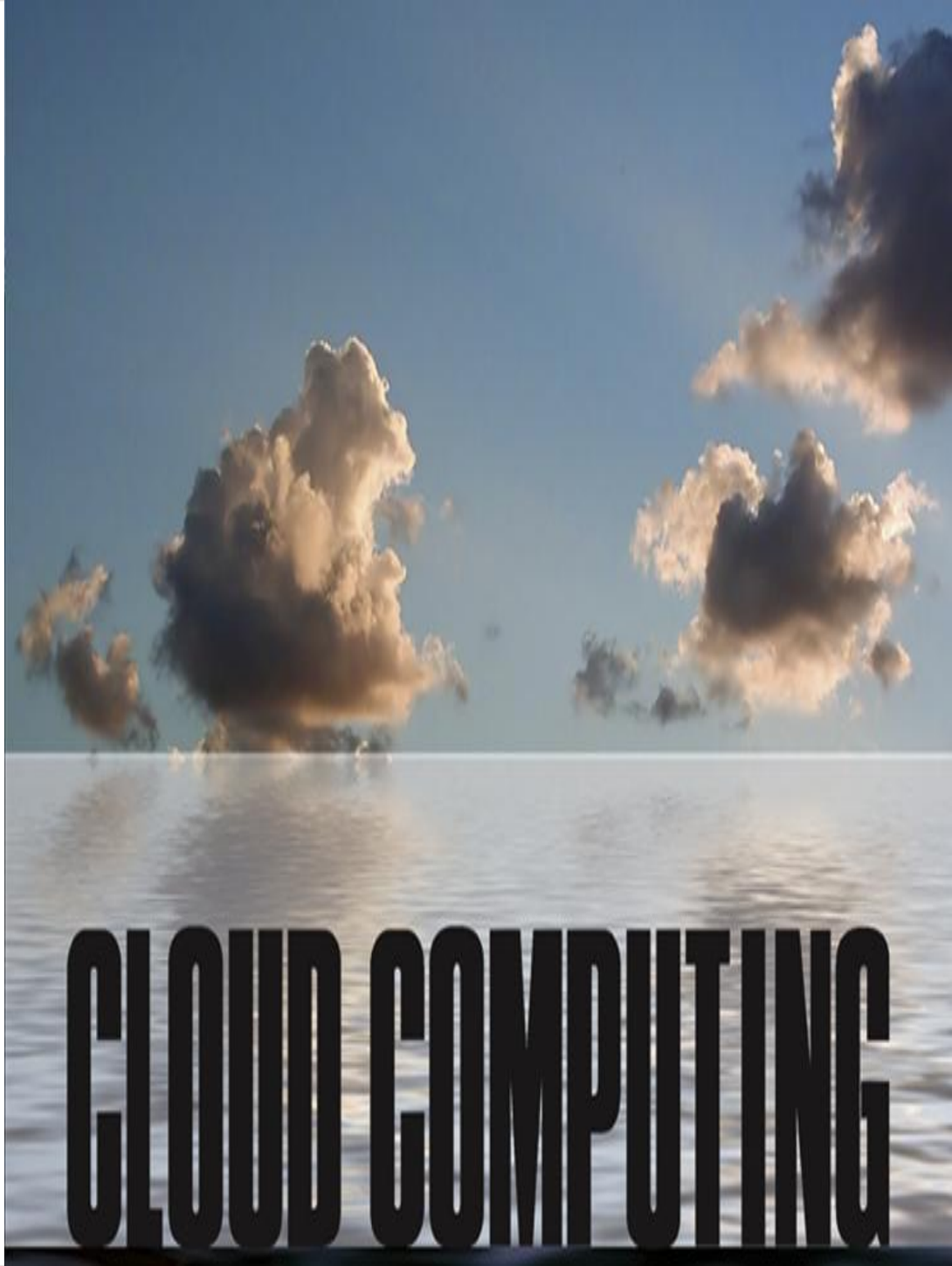
CLOUD COMPUTING AND SECURITY (BCS601)

Module-4



	CLOUD COMPUTING		Semester	6
	Course Code	BCS601	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:2:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	04	Exam Hou3rs	3
	Examination type (SEE)	Theory/Practical		

Course objectives:

- Introduce the rationale behind the cloud computing revolution and the business drivers
- Understand various models, types and challenges of cloud computing
- Understand the design of cloud native applications, the necessary tools and the design tradeoffs.
- Realize the importance of Cloud Virtualization, Abstraction`s, Enabling Technologies and cloud security

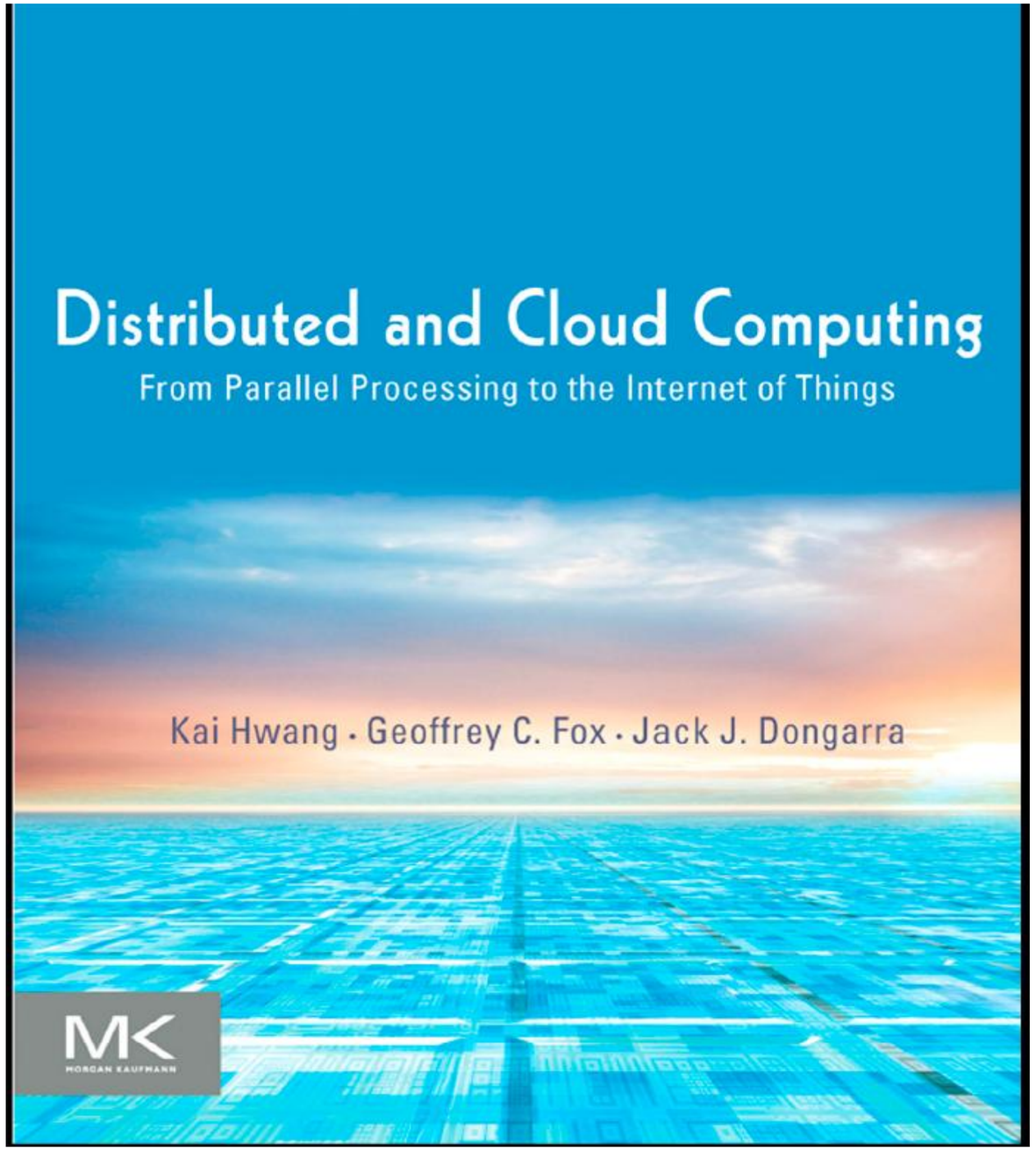
Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

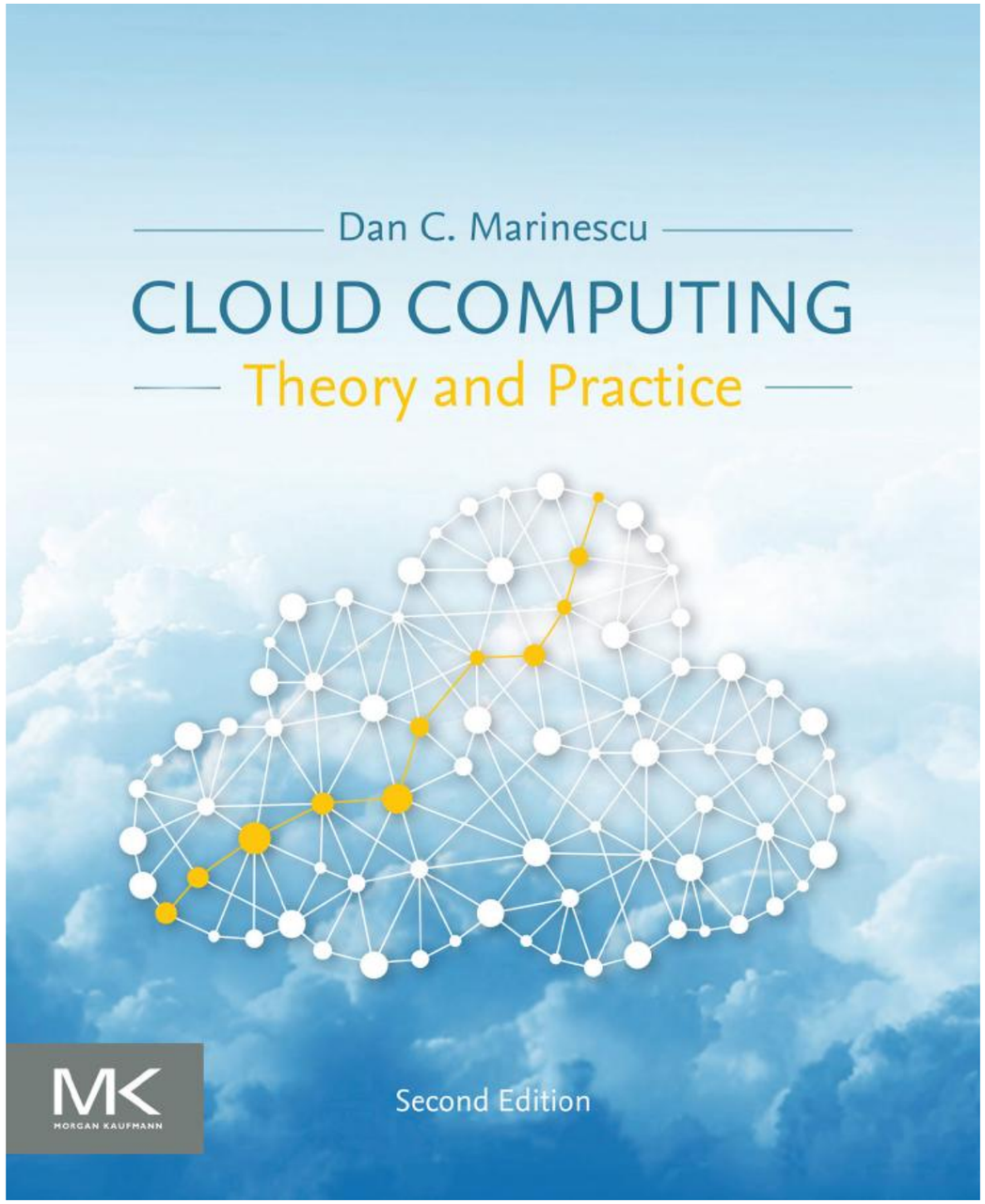
1. Describe various cloud computing platforms and service providers.
2. Illustrate the significance of various types of virtualization.
3. Identify the architecture, delivery models and industrial platforms for cloud computing based applications.
4. Analyze the role of security aspects in cloud computing.
5. Demonstrate cloud applications in various fields using suitable cloud platforms.

TEXT BOOKS

MODULE 1 to MODULE 5



MODULE 4



Module-4

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.

Textbook 2: Chapter 11: 11.1 to 11.3, 11.5 to 11.8, 11.10 to 11.14

Textbook 1: Chapter 4: 4.6

MODULE-4 :CLOUD SECURITY

- Security has been a concern since the early days of computing when a computer was isolated, and threats could only be posed by someone with access to the computer room.
- Security of computer and communication systems takes on a new urgency as the society becomes increasingly more dependent on the information infrastructure.
- A computer cloud is a target-rich environment for malicious individuals and criminal organizations. It is, thus, no surprise that security is a major concern for existing users and for potential new users of cloud computing services.

SECURITY, THE TOP CONCERN FOR CLOUD USERS

- The Service Level Agreements do not provide adequate legal protection for cloud computer users who are often left to deal with events beyond their control.
- Major user concerns are about the unauthorized access to confidential information and the data theft. Data is more vulnerable in storage, than while it is being processed.
- The next concerns regard the user control over the lifecycle of data. It is virtually impossible for a user to determine if data that should have been deleted was actually deleted. Even if deleted, there is no guarantee that the media was wiped out and the next user is not able to recover confidential data

The contract between a user and a CSP(Cloud Service Provider) should [400] state clearly:

1. CSPs obligations to handle sensitive information and its obligation to comply with privacy laws.
2. CSP liabilities for mishandling sensitive information, e.g., data loss.
3. The rules governing ownership of the data.
4. Specify the geographical regions where information and backups can be stored.

CLOUD SECURITY RISKS

A cloud could be used to launch large-scale attacks against other components of the cyber infrastructure.

- Traditional threats are those experienced for some time by any system connected to the Internet, but with some cloud-specific twists. The impact of traditional threats is amplified due to the vast amount of cloud resources and the large user population that can be affected.
- The traditional threats begin at the user site. The user must protect the infrastructure used to connect to the cloud and to interact with the application running on the cloud.
- The next threat is related to authentication and authorization

CLOUD SECURITY RISKS(continue)

- The favorite means of attack are: distributed denial of service (DDDS) attacks which prevent legitimate users to access cloud services, phishing, SQL injection, or cross-site scripting.

- SQL injection is typically used against a web site. An SQL command entered in a web form causes the contents of a database used by the web site to be either dumped to the attacker or altered.

- Availability of cloud services is another major concern. System failures, power outages, and other catastrophic events could shutdown cloud services for extended periods of time.

- Third-party control generates a spectrum of concerns caused by lack of transparency and limited user control.

- Auditing guidelines elaborated by the National Institute of Standards (NIST) such as the Federal Information Processing Standard (FIPS) and the Federal Information Security Management Act (FISMA) are mandatory for US Government agencies.

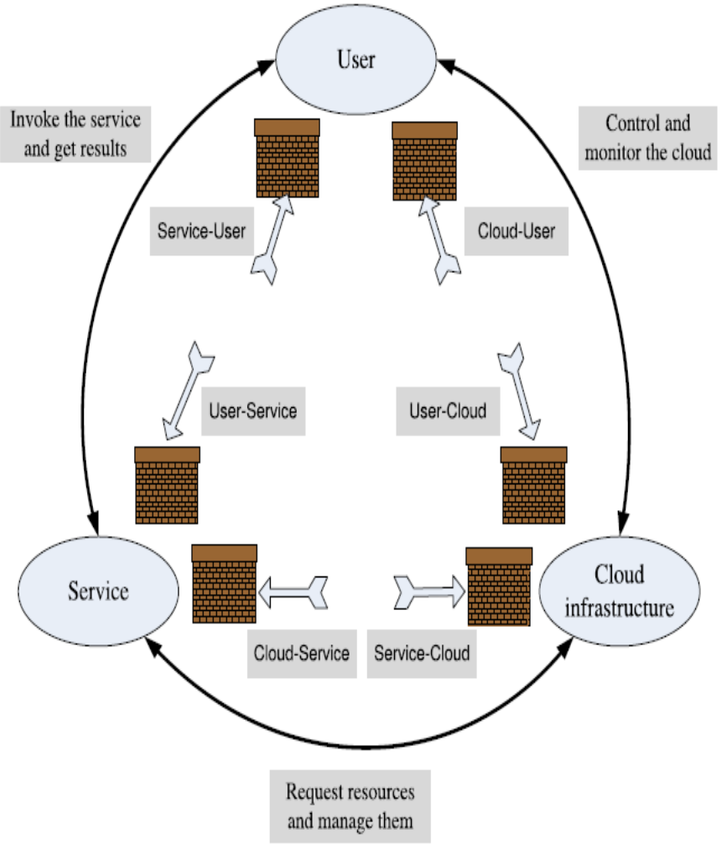
The 2010 Cloud Security Alliance (CSA) report.

- The abusive use of the cloud, APIs that are not fully secure, malicious insiders, shared technology, account hijacking, data loss or leakage, and unknown risk profile.
- Shared technology considers threats due to multi-tenant access supported by virtualization. Hypervisors can have flaws allowing a guest OS to affect the security of the platform shared with other VMs.
- Insecure APIs may not protect the users during a range of activities starting with authentication and access control to monitoring and control of the application during runtime.
- The potential harm due to this particular form of attacks is high.Data loss and data leakage are two risks with devastating consequences for an individual or an organization using cloud services.
- Account or service hijacking is a significant threat and cloud users must be aware of and guard against all methods to steal credentials. Lastly, unknown risk profile refers to exposure to the ignorance or underestimation of the risks of cloud computing
- Account or service hijacking is a significant threat and cloud users must be aware of and guard against all methods to steal credentials. Lastly, unknown risk profile refers to exposure to the ignorance or underestimation of the risks of cloud computing

The 2011 CSA report. The report “Security Guidance for Critical Area of Focus in Cloud Computing V3.0

The three actors involved in the model considered are: the user, the service, and the cloud infrastructure, and there are six types of attacks possible

- The user can be attacked from two directions, the service and the cloud. Secure Sockets Layer (SSL) certificate spoofing, attacks on browser caches, or phishing attacks are example of attacks that originate at the service.
- The user can also be a victim of attacks that either truly originate or that spoof originating from the cloud infrastructure.
- Buffer overflow, SQL injection, and privilege escalation are the common types of attacks from the service.
- The service can also be subject of attacks by the cloud infrastructure and this is probably the most serious line of attack. Limiting access to resources, privilege-related attacks, data distortion, injecting additional operations are only a few of the many possible lines of attacks originated at the cloud.
- The cloud infrastructure can be attacked by a user which targets the cloud control system.



Top twelve cloud security threats. The 2016 CSA report lists the top security threats

1. Data breaches. The most damaging breaches are for sensitive data including financial and health information, trade secrets, and intellectual property.

2. Compromised credentials and broken authentication. Such attacks are due to lax authentication, weak passwords, and poor key and/or certificate management.

3. Hacked interfaces and APIs. Cloud security and service availability can be compromised by a weak API. When third parties rely on APIs more services and credentials are exposed.

4. Exploited system vulnerabilities. Resource sharing and multi-tenancy create new attack surfaces but the cost to discover and repair vulnerabilities is small compared to the potential damage.

5. Account hijacking. All accounts should be monitored so that every transaction can be traced to the individual requesting it.

6. Malicious insiders. This threat can be difficult to detect and system administrator errors could sometimes be falsely diagnosed as threats. A good policy is to segregate duties and enforce activities such as logging, monitoring, and auditing administrator activities.

The other six threats are: advanced persistent threats (APTs), permanent data loss, inadequate diligence, cloud service abuse, DoS attacks, and shared technology

PRIVACY AND PRIVACY IMPACT ASSESSMENT: The term privacy refers to the right of an individual, a group of individuals, or an organization to keep information of personal nature or proprietary information from being disclosed

1. Digital age has confronted legislators with significant challenges related to privacy as new threats have emerged. For example, personal information voluntarily shared, but stolen from sites granted access to it or misused can lead to identity theft.

2. Privacy concerns are different for the three cloud delivery models and also depend on the actual context. For example, consider the widely used Gmail; Gmail privacy policy reads (see http://www.google.com/policies/privacy/ accessed on October 6, 2012):

3. The main aspects of cloud privacy are: the lack of user control, potential unauthorized secondary use, data proliferation, and dynamic provisioning [400]. The lack of user control refers to the fact that user-centric data control is incompatible with cloud usage. Once data is stored on the servers of the CSP the user losses control on the exact location, and in some instances it could lose access to the data. For example, in case of the Gmail service the account owner has no control on where the data is stored or how long old Emails are stored on some backups of the servers.

4. "Consumer oriented commercial web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices:

PRIVACY AND PRIVACY IMPACT ASSESSMENT: (continued)

1. Notice – web sites should be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
2. Choice – web sites should be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided, e.g., to consummate a transaction. Such choices would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses, such as disclosing data to other entities.
3. Access – web sites would be required to offer consumers reasonable access to the information a web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

4. Security – web sites would be required to take reasonable steps to protect the security of the information they collect from consumers. The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations."

CLOUD DATA ENCRYPTION

Encryption is the obvious solution to protect outsourced data and cloud service providers have been compelled to offer encryption services. For example, Amazon offers AWS Key Management Service (KMS) to create and control the encryption keys used by clients to encrypt their data.

Homomorphic encryption. The homomorphic encryption, a long time dream of security experts, reflects the concept of homomorphism, a structure-preserving map f (·) between two algebraic structures of the same type.

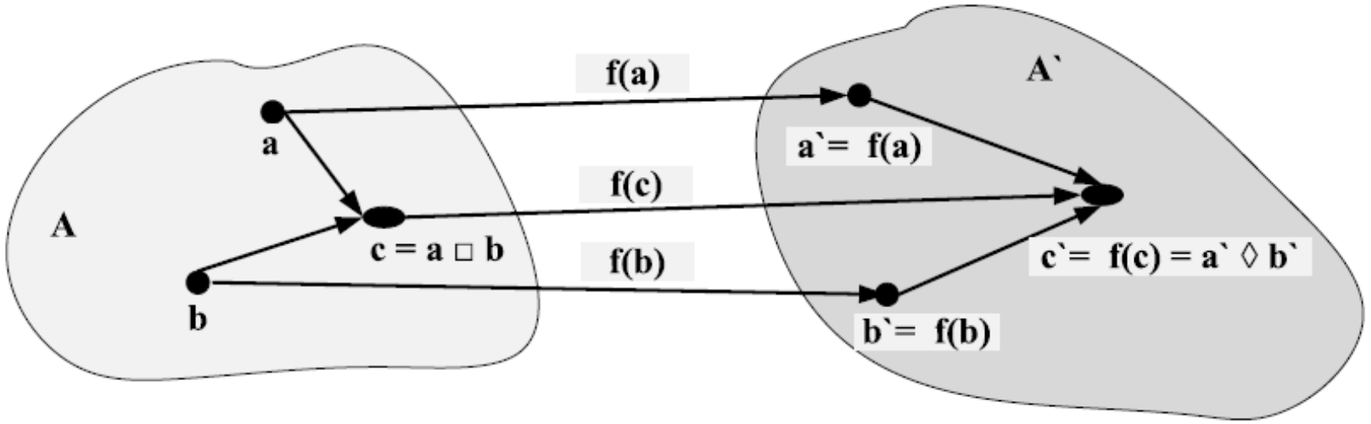


FIGURE 11.2

A homomorphism $f : A \rightarrow A'$ is a structure-preserving map between sets A and A' with the composition operations $\square$ and $\diamond$, respectively. Let $a, b, c \in A$ with $c = a \square b$ and $a', b', c' \in A'$ with $c' = a' \diamond b'$. Let $a' = f(a), b' = f(b), c' = f(c)$ be the results of the mapping $f(\cdot)$. If f is a homomorphism, then the composition operation $\diamond$ in the target domain A' produces the same result as mapping the result of the operation $\square$ applied to the two elements in the original domain A: $f(a) \diamond f(b) = f(a \square b)$.

Order Preserving Encryption. OPE can be used for encryption of numeric data, it maps a range of numerical values into a much larger and sparse range of values [70]. Let a order-preserving function $f : \{1, ..., M\} \rightarrow \{1, ..., N\}$ with $N >> M$ be uniquely represented by a combination of M out of N ordered items. Given N balls in a bin, M black and $N - M$ white, we draw a ball at random without replacement at each step. The random variable X describing the total number of balls in our sample after we collect the k-th black ball follows the negative hypergeometric distribution (NHG). One can

To encrypt plaintext x the OPE encryption algorithm performs a binary search down to x. Given the secret key K the algorithm first assigns $Encrypt(K, M/2)$, then $Encrypt(K, M/4)$ if the index $m < M/2$ and $Encrypt(K, 3M/4)$ otherwise, and so on, until $Encrypt(K, x)$ is assigned. Each ciphertext assignment is made according to the output of the negative hypergeometric sampling algorithm. One can prove by strong induction on the size of the plaintext space that the resulting scheme induces a random order-preserving function from the plaintext to ciphertext space.

To allow efficient range queries on encrypted data, it is sufficient to have an order-preserving hash function family H (not necessarily invertible). The OPE algorithm would use a secret key $(K_{Encrypt}, K_H)$ where $K_{Encrypt}$ is a key for a normal (randomized) encryption scheme and K_H is a key for H. Then $Encrypt(K_{Encrypt}, x) \,||\, H(K_H, x)$ will be the encryption of x [70].

SECURITY OF DATABASE SERVICES

1. Cloud users often delegate control of their data to the database services supported by virtually all CSP and are concerned with security aspects of DBaaS. The model used to evaluate DBaaS security includes several groups of entities: data owners, users of data, CSPs, and third party agents or Third Party Auditors (TPAs).

2. Data owners and DBaaS users fear compromised integrity and confidentiality, as well as data unavailability. Insufficient authorization, authentication and accounting mechanisms, inconsistent use of encryption keys and techniques, alteration or deletion of records without maintaining backup, and operational failures are the major causes of data loss in DBaaS.

3. Some data integrity and privacy issues are due to the absence of authentication, authorization and accounting controls, or poor key management for encryption and decryption. Confidentiality means that only authorized users should have access to the data. Unencrypted data is vulnerable to bugs, errors, and attacks from external entities affecting data confidentiality.

4. Malicious external attackers use spoofing, sniffing, man-in-the-middle attacks, side channeling and illegal transactions to launch DoS attacks.

5. Data provenance, the process of establishing the origin of data and its movement between databases, uses metadata to determine the data accuracy, but the security assessments are time-sensitive. Moreover, analyzing large provenance metadata graphs is computationally expensive.

6. Auditing and monitoring are important functions of a DBaaS but generate their own security risks when delegated to TPAs.

In summary, DBaaS data availability is affected by several threats including

- Resource exhaustion caused by imprecise specification of user needs or incorrect evaluation of user specifications.

- Failures of the consistency management; multiple hardware and/or software failures lead to inconsistent views of user data.

- Failure of the monitoring and auditing system.

- DBaaS data confidentiality is affected by insider and outsider attacks, access control issues, illegal data recovery from storage, network breaches, third-party access, inability to establish the provenance of the data.

OPERATING SYSTEM SECURITY

1. A critical function of an OS is to protect applications against a wide range of malicious attacks such as unauthorized access to privileged information, tampering with executable code, and spoofing.

2. The mandatory security of an OS is considered to be [295]: "any security policy where the definition of the policy logic and the assignment of security attributes is tightly controlled by a system security policy administrator." Access control, authentication usage, and cryptographic usage policies are all elements of the mandatory OS security.

3. Applications with special privileges performing security-related functions are called trusted applications. Such applications should only be allowed the lowest level of privileges required to perform their functions.

4. Enforcing mandatory security through mechanisms left at user's discretion can lead to a breach of security, sometimes due to malicious intent, in other cases due to carelessness, or to lack of understanding.

5. A trusted path mechanism is required to prevent malicious software invoked by an authorized application to tamper with the attributes of the object and/or with the policy rules.

6. Another question is how an OS can protect itself and applications running under it from malicious mobile code attempting to gain access to data and other resources and compromise system confidentiality and/or integrity.

7. Specialized *closed-box platforms* such as the ones on some cellular phones, game consoles, and Automatic Teller Machines (ATMs) could have embedded cryptographic keys that allow themselves to reveal their true identity to remote systems and authenticate the software running on them

8. A highly secure operating system is necessary but not sufficient. Application-specific security is also necessary.

9. We conclude that commodity operating systems offer low assurance. Indeed, an OS is a complex software system consisting of millions of lines of code and it is vulnerable to a wide range of malicious attacks.

10.Operating systems provide only weak mechanisms for applications to authenticate one another and do not have a trusted path between users and applications.

VIRTUAL MACHINE SECURITY

Virtual security services are typically provided by the hypervisor as shown in Figure 11.3A; another alternative is to have a dedicated VM providing security service as in Figure 11.3B

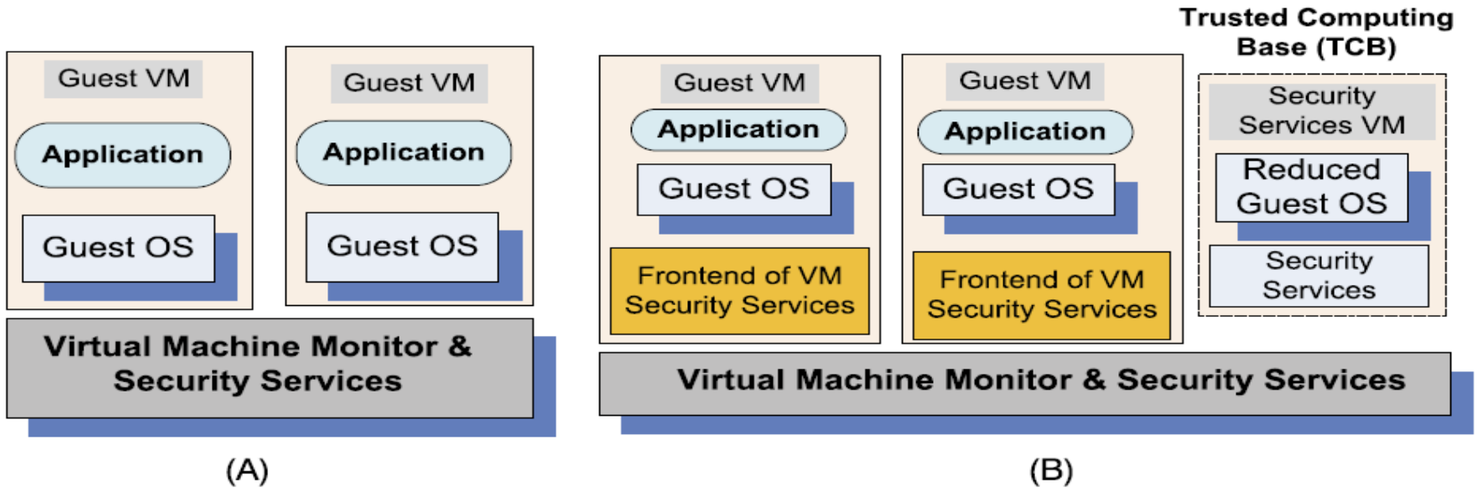


FIGURE 11.3

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

Hypervisors are considerably less complex and better structured than traditional operating systems thus, in a better position to respond to security attacks.

Sophisticated attackers are able to fingerprint VMs and avoid VM honey pots designed to study the methods of attack. They can also attempt to access VM-logging files and thus, recover sensitive data.

This price includes:
(i) higher hardware costs because a virtual system requires more resources such as CPU cycles, memory, disk, and network bandwidth;
(ii) the cost of developing hypervisors and modifying the host operating systems in case of paravirtualization; and
(iii) the overhead of virtualization as the hypervisor is involved in privileged operations.

NIST security group distinguishes two groups of threats, hypervisor-based and VM-based. There are several types of hypervisor-based threats:

1. Starvation of resources and denial of service for some VMs. Probable causes:
(a) badly configured resource limits for some VMs;
(b) a rogue VM with the capability to bypass resource limits set in hypervisor.

2. VM side-channel attacks: malicious attack on one or more VMs by a rogue VM under the same hypervisor. Probable causes:
(a) lack of proper isolation of inter-VM traffic due to misconfiguration of the virtual network residing in the hypervisor;
(b) limitation of packet inspection devices to handle high speed traffic, e.g., video traffic;
(c) presence of VM instances built from insecure VM images, e.g., a VM image having a guest OS without the latest patches.

3. Buffer overflow attacks.

There are also several types of VM-based threats:

1. Deployment of rogue or insecure VM; unauthorized users may create insecure instances from images or may perform unauthorized administrative actions on existing VMs. Probable cause: improper configuration of access controls on VM administrative tasks such as instance creation, launching, suspension, re-activation and so on.

2. Presence of insecure and tampered VM images in the VM image repository. Probable causes: (a) lack of access control to the VM image repository; (b) lack of mechanisms to verify the integrity of the images, e.g., digitally signed image.

SECURITY RISKS POSED BY SHARED IMAGES

AWS user has the option to choose between Amazon Machine Images (AMIs) accessible through the Quick Start or the Community AMI menus of the EC2 service.

First, we review the process to create an AMI. We can start from a running system, from another AMI, or from the image of a VM and copy the contents of the file system to the S3, a process called bundling.

Two procedures, ec2-bundle-image and ec2-bundle-volume, are used for creation of an AMI. The first is used for images prepared as loopback files3 when data is transferred to the image in blocks. To bundle a running system the creator of the image can use the second procedure when bundling works at the level of the file system and files are copied recursively to the image.

Three types of security risks are analyzed:
(1) backdoors and leftover credentials,
(2) unsolicited connections, and
(3) malware. An astounding finding is that about 22% of the scanned Linux AMIs contained credentials allowing an intruder to remotely login to the system.

To rent a Linux AMI a user must provide the public part of the her ssh key and this key is stored in the authorized_keys in the home directory.

This opens a backdoor for a malicious creator of an AMI who does not remove her own public key from the image and can remotely login to any instance of this AMI. Another backdoor is opened when the ssh server allows password-based authentication and the malicious creator of an AMI does not remove her own password.

Another threat is posed by the omission of the cloud-init script that should be invoked when the image is booted.

An attacker impersonates the agents at both ends of a communication channel in the **man-in-the middle attack** and makes them believe that they communicate through a secure channel. For example, if B sends her public key to A, but C is able to intercept it, such an attack proceeds as follows: C sends a forged message to A claiming to be from B, but instead includes C's public key. Then A encrypts her message with C's key, believing that she is using B's key, and sends the encrypted message to B. The intruder, C, intercepts, deciphers the message using her private key, possibly alters the message, and re-encrypts with the public key B originally sent to A. When B receives the newly encrypted message, she believes it came from A.

SECURITY RISKS POSED BY A MANAGEMENT OS

A hypervisor supports a stronger isolation between the VMs running under it than the isolation between processes supported by a traditional operating system.

A small hypervisor can be carefully analyzed, thus one could conclude that the security risks in a virtual environment are diminished

see Figure 11.4. System vulnerabilities can be introduced by both software components, Xen and the management operating system.

Dom0 manages the building of all user domains (DomU), a process consisting of several steps:

1. Allocate memory in the Dom0 address space and load the kernel of the guest OS from secondary storage.

2. Allocate memory for the new VM and use foreign mapping to load the kernel to the new VM. The foreign mapping mechanism of Xen is used by Dom0 to map arbitrary memory frames of a VM into its page tables.

3. Set up the initial page tables for the new VM.

4. Release the foreign mapping on the new VM memory, set up the virtual CPU registers, and launch the new VM.

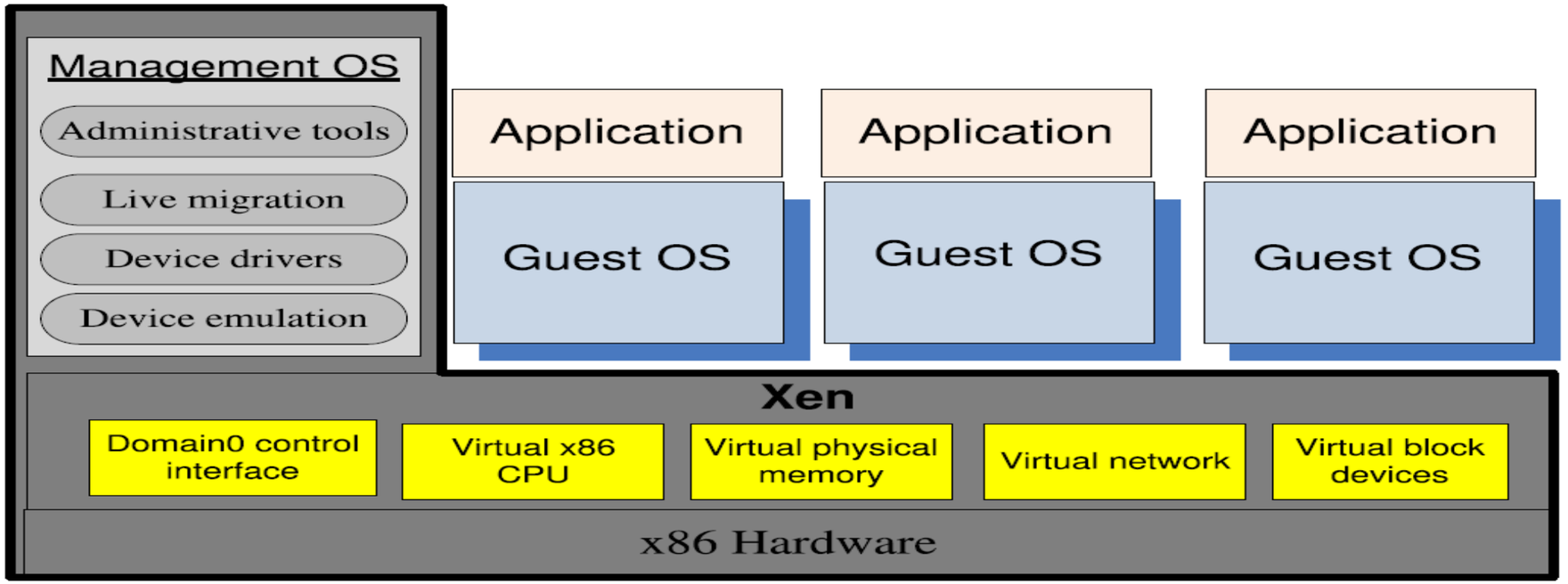


FIGURE 11.4

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.

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.

We should check the integrity of DomU after the execution of such security-critical hypercalls. New hypercalls are necessary to protect:

1. The privacy and integrity of the virtual CPU of a VM. When Dom0 wants to save the state of the VM the hypercall should be intercepted and the contents of the virtual CPU registers should be encrypted. The virtual CPU context should be decrypted and then an integrity check should be carried out when DomU is restored.

2. The privacy and integrity of the VM virtual memory. The page table update hypercall should be intercepted and the page should be encrypted so that Dome handles only encrypted pages of the VM. The hypervisor should calculate a hash of all the memory pages before they are saved by Dom0 to guarantee the integrity of the system. An address translation is necessary because a restored DomU may be allocated a different memory region [302].

3. The freshness of the virtual CPU and the memory of the VM. The solution is to add to the hash a version number.

XOAR (Xen-based On-demand Architecture)– BREAKING THE MONOLITHIC DESIGN OF THE TCB

The security model of Xoar assumes that the system is professionally managed and that a privileged access to the system is granted only to system administrators.

Xoar modularity makes exposure to risk explicit and allows the guests to configure the access to services based on their needs. Modularity allows the designers of Xoar to reduce the size of the permanent footprint of the system and increase the level of security of critical components.

Maintain the functionality provided by Xen

- Ensure transparency with existing management and VM interfaces.
- Tight control of privileges. Each component should only have the privileges required by its function.
- Minimize the interfaces of all components to reduce the possibility that a component can be used by an attacker.
- Eliminate sharing. Make sharing explicit, whenever it cannot be eliminated, to allow meaningful logging and auditing.
- Reduce the opportunity of an attack targeting a system component by limiting the time window when the component runs.

The Xoar system has four types of components: permanent, self-destructing, restarted upon request, and restarted on timer

1. Permanent components. XenStore-State maintains all information regarding the state of the system.

2. Components used to boot the system; they self-destruct before any user VM is started. The two components discover the hardware configuration of the server including the PCI drivers and then boot the system:

PCIBack – virtualizes access to PCI bus configuration.

Bootstrapper – coordinates booting of the system.

3. Components restarted on each request:

XenStore-Logic

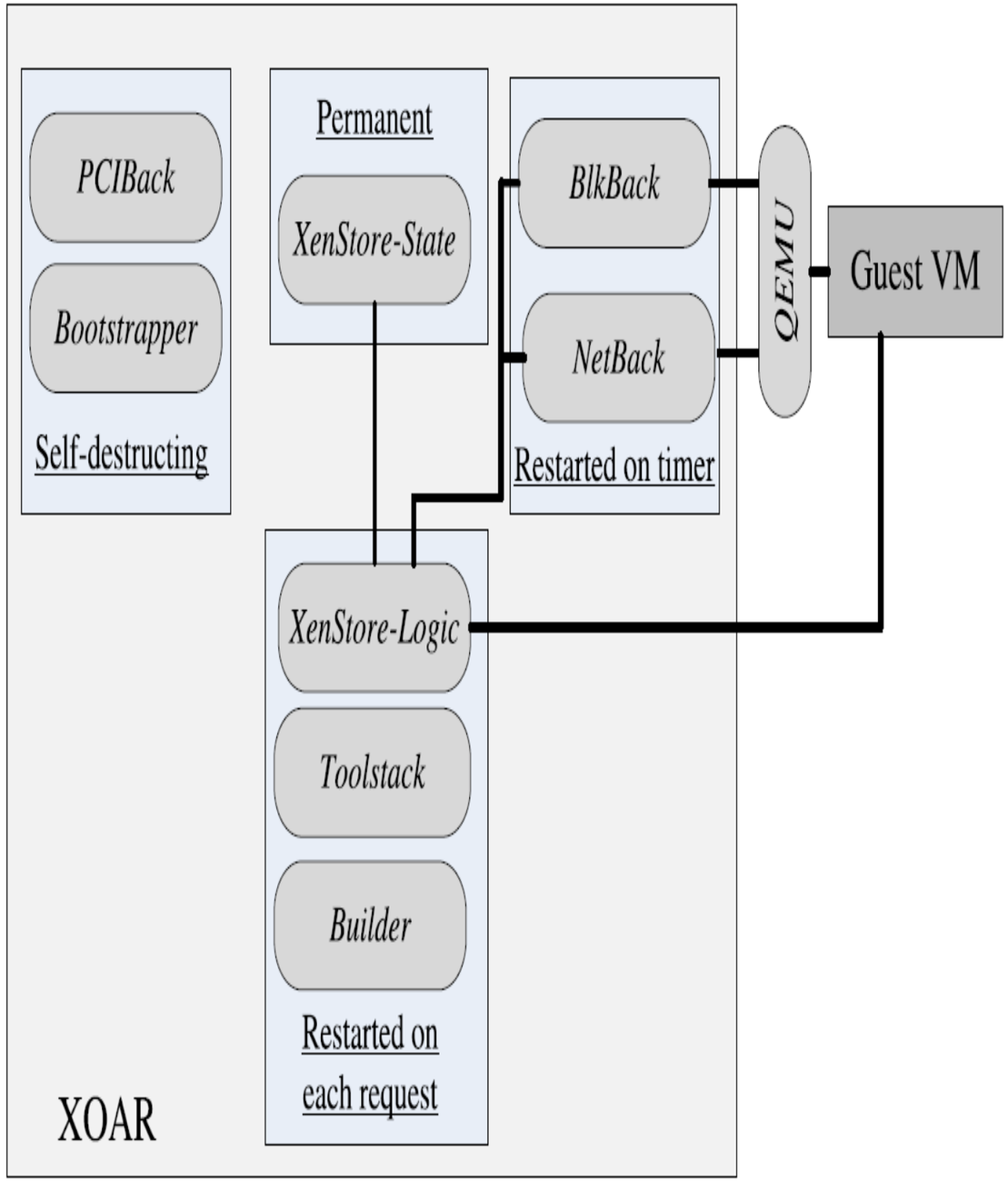
Toolstack – handles VM management requests, e.g., it requests the Builder to create a new guest VM in response to a user request.

- **Builder – initiates user VMs.**

4. Components restarted on a timer: the two components export physical storage device drivers and the physical network driver to a guest VM.

BlkBack – exports physical storage device drivers using udev8 rules.

NetBack – exports the physical network driver.



XenStore is broken into two components, XenStore-Logic and XenStore-State. Access control checks are done by a small monitor module in XenStore-State. Guest VMs share only the Builder, XenStore-Logic, and XenStore-State.

Users of Xoar are able to only share service VMs with guest VMs that they control; to do so they specify a tag on all of the devices of their hosted VMs.

Rebooting provides the means to ensure that a VM is in a known good state. To reduce the overhead and the increased startup time demanded by a reboot, Xoar uses *snapshots* instead of rebooting

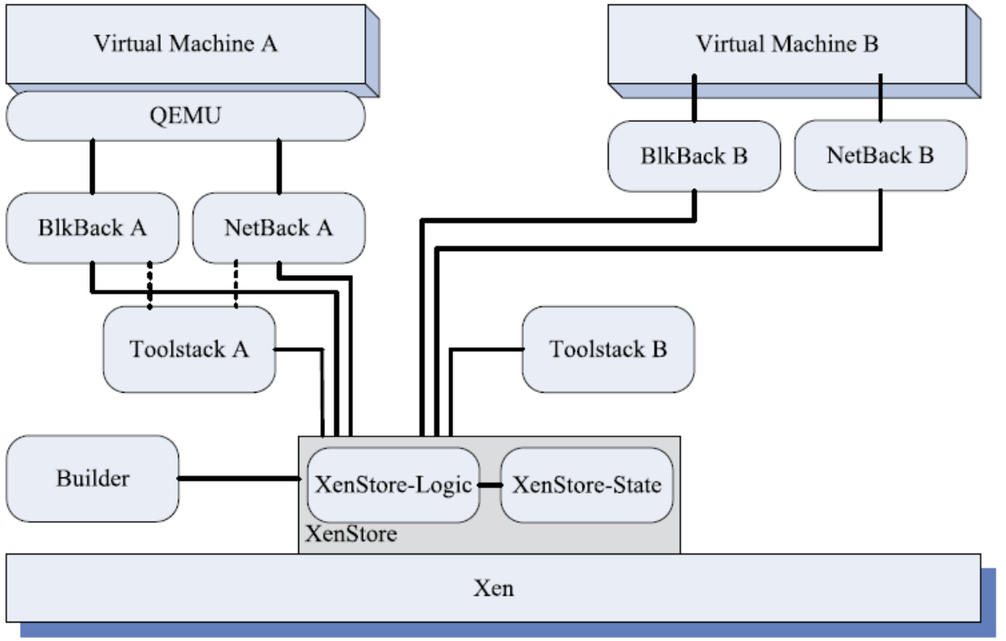


FIGURE 11.6

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.

A TRUSTED HYPERVISOR

After the discussion of Xoar we briefly analyze the design of a trusted hypervisor called Terra: The novel ideas of this design are:

- A trusted hypervisor should support not only traditional operating systems, by exporting the hardware abstraction for open-box platforms

- An application should be allowed to build its software stack based on its needs. Applications requiring a very high level of security, e.g., financial applications and electronic voting systems should run under a very thin OS supporting only the functionality required by the application and the ability to boot.

- **Support additional capabilities to enhance system assurance:**

1. – Provide trusted paths from a user to an application.We have seen in Section 11.7 that such a path allows a human user to determine with certainty the identity of the VM it is interacting with and, at the same time, allows the VM to verify the identity of the human user.

2. – Support attestation, the ability of an application running in a closed-box to gain trust from a remote party, by cryptographically identifying itself.

3. – Provide air-tight isolation guarantees for the hypervisor by denying the platform administrator the root access.

MOBILE DEVICES AND CLOUD SECURITY

Mobile devices are an integral part of the cloud ecosystem, mobile applications use cloud services to access and store data or to carry out a multitude of computational tasks. Security challenges for mobile devices common to all computer and communication systems include:

(i) Confidentiality – ensure that transmitted and stored data cannot be read by unauthorized parties;
(ii) Integrity – detect intentional or unintentional changes to transmitted and stored data;
(iii) Availability – ensure that users can access cloud resources whenever needed; and
(iv) Non-repudiation – the ability to ensure that a party to a contract cannot deny the sending of a message that they originated.

Special precautions must then be taken due to exposure to the unique security threats affecting mobile devices, including:

1. Mobile malware.
2. Stolen data due to loss, theft, or disposal.
3. Unauthorized access.
4. Electronic eavesdropping.
5. Electronic tracking.
6. Access to data by third party applications

The risks posed to the cloud infrastructure by mobile devices are centered around data leakage and compromise

- Loss of the mobile device, lock screen protection, enabling smudge attacks and other causes leading to mobile access control. A smudge attack is a method to discern the password pattern of a touchscreen device such as a cell phone or tablet computer.
- Lack of confidentiality protection for data in transit in unsafe or untrustedWiFi or cellular networks.
- Unmatched firmware or software including operating system and application software bypassing the security architecture, e.g., rooted/jailbroken devices.
- Malicious mobile applications bypassing access control mechanisms.
- Misuse or misconfiguration of location services, such as GPS.
- Acceptance of fake mobility management profiles.

Policies and mechanisms should also be applied to mobile devices connected to computer cloud

- 1.Use device encryption, application-level encryption, and remote wipe capabilities to protect storage.
- 2. Use Transport Layer Security (TLS) for all communication channels.
- 3. Isolate user-level applications from each other to prevent data leakage between applications using
- sandboxing.
- 4. Use device integrity checks for boot validation, verified application and OS updates.
- 5. Use auditing and logging.
- 6. Enforce authentication of the device owner.
- 7. Automatic, regular device integrity and compliance checks for threats and compliance.
- 8. Automated alerts for policy violations.

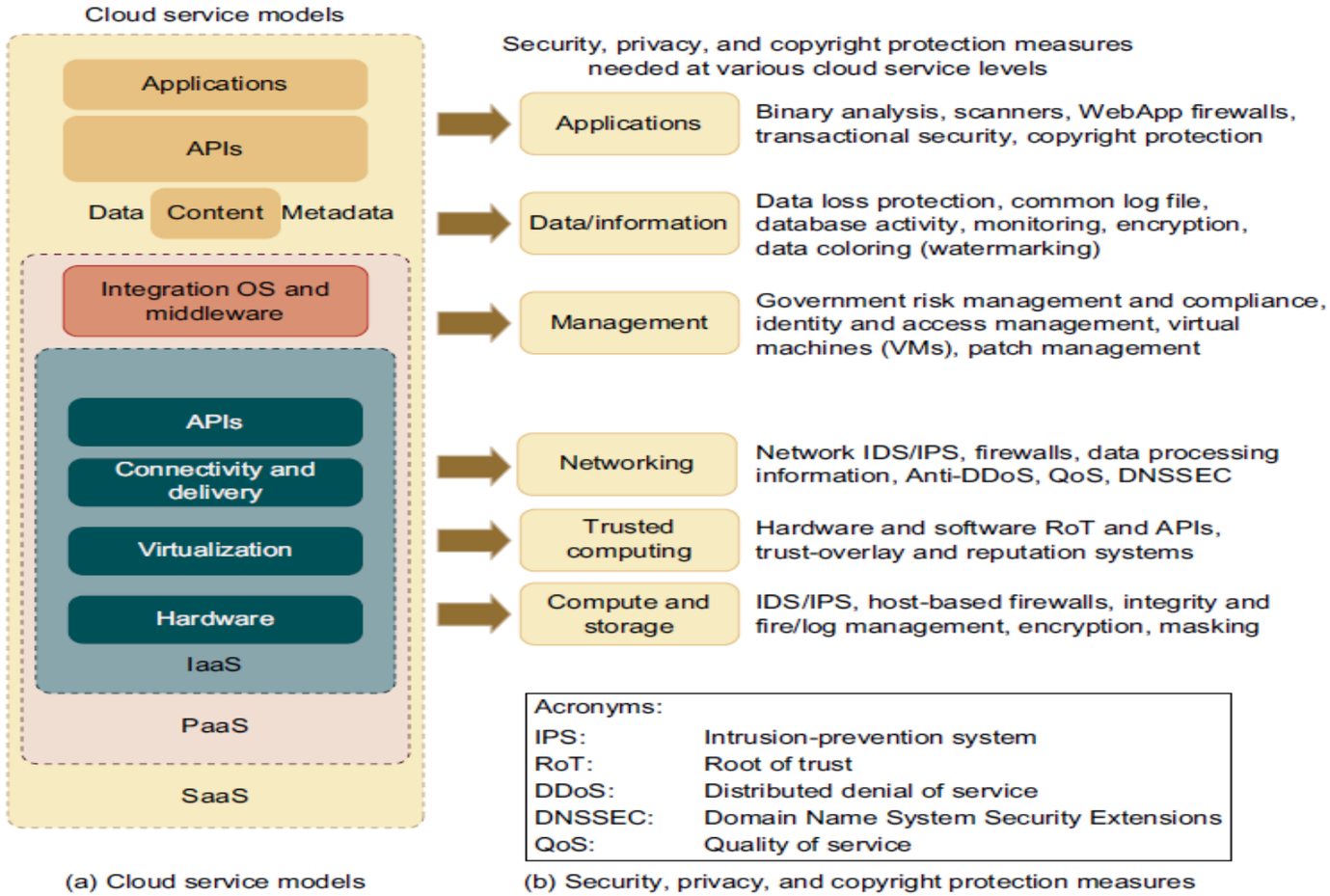
CLOUD SECURITY AND TRUST MANAGEMENT: Cloud Security Defense Strategies

•For web and cloud services, trust and security become even more demanding, because leaving user applications completely to the cloud providers has faced strong resistance by most PC and server users.

•Cloud platforms become worrisome to some users for lack of privacy protection, security assurance, and copyright protection.

•Trust is a social problem, not a pure technical issue and it can be solved with a technical approach.

•A healthy cloud ecosystem is desired to free users from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations.



(a) Cloud service models

(b) Security, privacy, and copyright protection measures

CLOUD SECURITY AND TRUST MANAGEMENT: Components that require high security

- 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

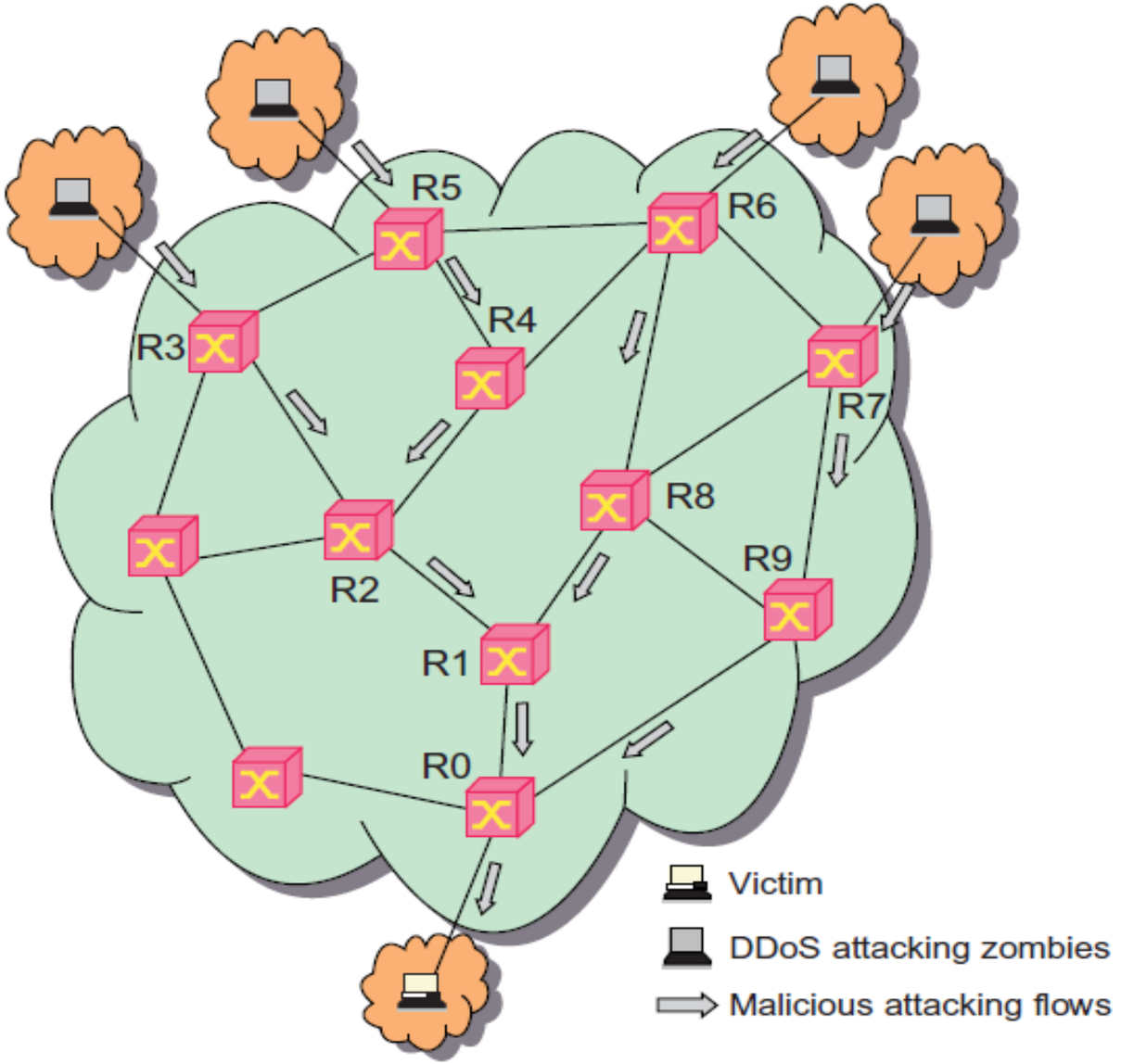
Table 4.9 Physical and Cyber Security Protection at Cloud/Data Centers

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.

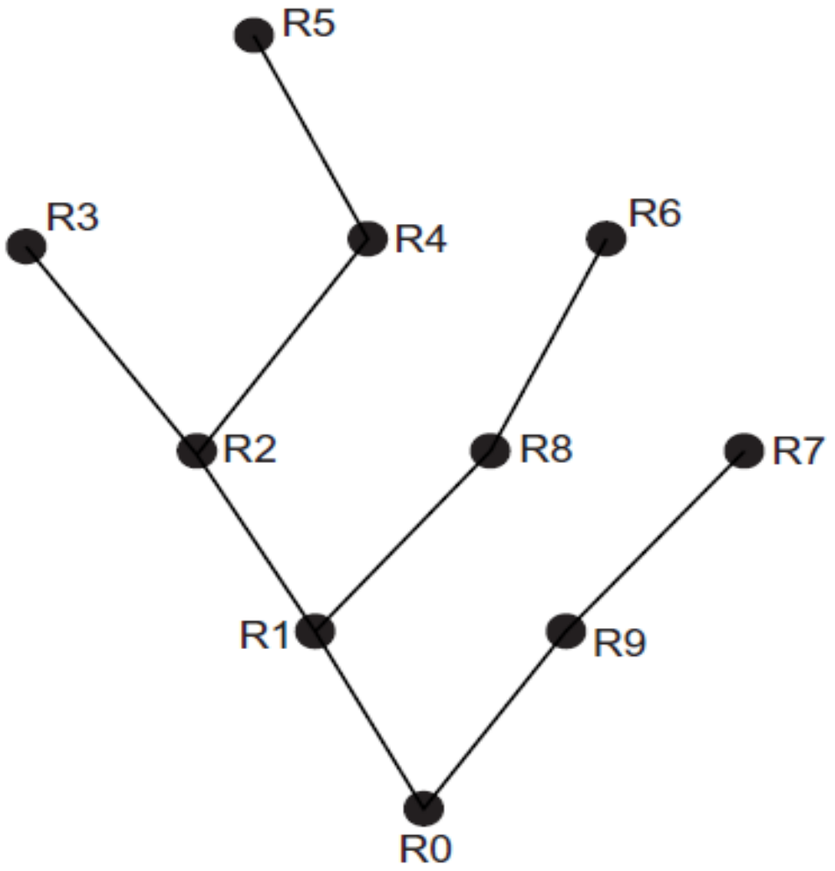
CLOUD SECURITY AND TRUST MANAGEMENT: Privacy and Copyright Protection

- With shared files and data sets, privacy, security, and copyright data could be compromised in a cloud computing environment.
- Users desire to work in a software environment that provides many useful tools to build cloud applications over large data sets.
- Google's platform essentially applies in-house software to protect resources. The Amazon EC2 applies HMEC and X.509 certificates in securing resources.
- Several security features desired in a secure cloud:
    - Dynamic web services with full support from secure web technologies
    - Established trust between users and providers through SLAs and reputation systems
    - Effective user identity management and data-access management
    - Single sign-on and single sign-off to reduce security enforcement overhead
    - Auditing and copyright compliance through proactive enforcement
    - Shifting of control of data operations from the client environment to cloud providers
    - Protection of sensitive and regulated information in a shared environment

Distributed Intrusion/Anomaly Detection: Distributed Defense against DDoS Flooding Attacks



(a) Traffic flow pattern of a DDoS attack

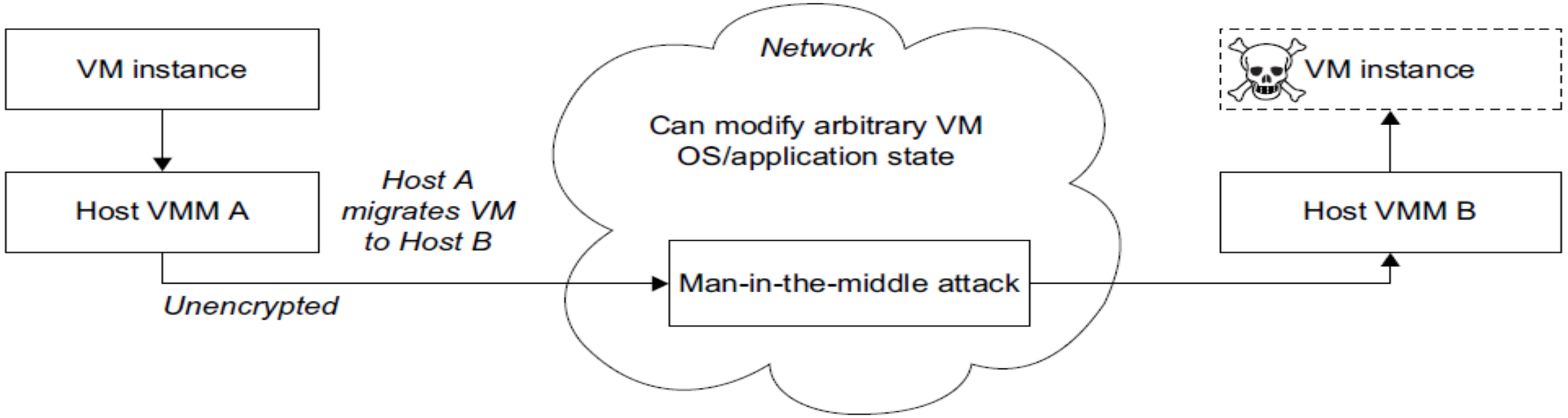


(b) The attack traffic flow tree over 10 routers

Data and Software Protection Techniques: Data Integrity and Privacy Protection

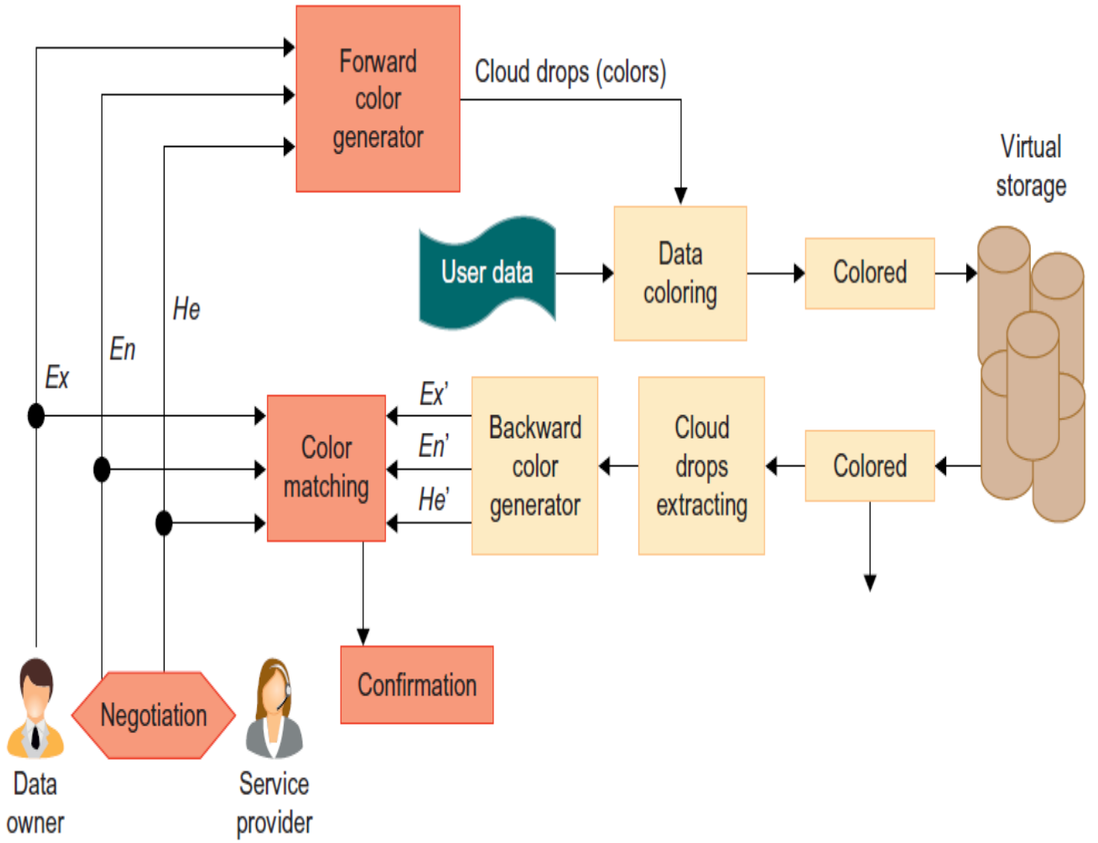
Features of security and privacy protection software

- Special APIs for authenticating users and sending e-mail using commercial accounts
- Fine-grained access control to protect data integrity and deter intruders or hackers
- Shared data sets protected from malicious alteration, deletion, or copyright violation
- Ability to secure the ISP or cloud service provider from invading users' privacy
- Personal firewalls at user ends to keep shared data sets from Java, JavaScript, and ActiveX applets
- A privacy policy consistent with the cloud service provider's policy, to protect against identity theft, spyware, and web bugs
- VPN channels between resource sites to secure transmission of critical data objects



Data and Software Protection Techniques: Data Integrity and Privacy Protection

- With shared files and data sets, privacy, security, and copyright information could be compromised in a cloud computing environment.
- Users desire to work in a trusted software environment that provides useful tools to build cloud applications over protected data sets.
- Watermarking was mainly used for digital copyright management.
- In modern days, the systems are used to generate special colors for each data object.
- Data coloring means labeling each data object by a unique color. Differently colored data objects are thus distinguishable.
- The user identification is also colored to be matched with the data colors.
- This color matching process can be applied to implement different trust management events.
- Cloud storage provides a process for the generation, embedding, and extraction of the watermarks in colored objects.



Reputation-Guided Protection of Data Centers : Reputation System Design Options

- Trust is a personal opinion, which is very subjective and often biased.
- Trust can be transitive but not necessarily symmetric between two parties.
- Reputation is a public opinion, which is more objective and often relies on a large opinion aggregation process to evaluate.
- Reputation may change or decay over time but Recent reputation should be given more preference than past reputation.
- To address reputation systems for cloud services, a systematic approach is based on the design criteria and administration of the reputation systems.
- Two-tier classification of existing reputation systems that have been proposed in recent years designed for P2P or social networks.
- These reputation systems can be converted for protecting cloud computing applications.
- In general, the reputation systems are classified as **Centralized** or **Distributed** depending on how they are implemented.
- In a centralized system, a single central authority is responsible for managing the reputation system, while the distributed model involves multiple control centers working collectively.
- Reputation-based trust management and techniques for securing P2P and social networks could be merged to defend data centers and cloud platforms against attacks from the open network.