CS6006 - CLOUD COMPUTING

Module 6 - CLOUD SECURITY

Presented By
Dr. S. Muthurajkumar,
Assistant Professor,
Dept. of CT, MIT Campus,
Anna University, Chennai

CLOUD SECURITY

- Cloud Security Defense Strategies
- Securing the Cloud & Data
- Distributed Intrusion and Anomaly Detection
- Data and Software Protection Techniques
- Data Security in the Cloud
- The Current State of Data Security in the Cloud
- Cloud Computing and Data Security Risk
- The Cloud, Digital Identity, and Data Security
- Establishing Identity in Cloud

CLOUD SECURITY

- The Internet was designed primarily to be resilient; it was not designed to be secure.
- Any distributed application has a much greater attack surface than an application that is closely held on a Local Area Network.
- Cloud computing has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from pooled, virtualized, and outsourced resources.
- The following areas of cloud computing that they felt were uniquely troublesome:
- Auditing
- Data integrity
- e-Discovery for legal compliance
- Privacy
- Recovery
- Regulatory compliance

CLOUD SECURITY DEFENSE STRATEGIES

- Lacking trust between service providers and cloud users has hindered the universal acceptance of cloud computing as a service on demand.
- The trust models have been developed to protect mainly e-commerce and online shopping provided by eBay and Amazon.
- Common sense dictates that technology can enhance trust, justice, reputation, credit, and assurance in Internet applications.
- As a virtual environment, the cloud poses new security threats that are more difficult to contain than traditional client and server configurations.
- A healthy cloud ecosystem is desired to free users from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations.

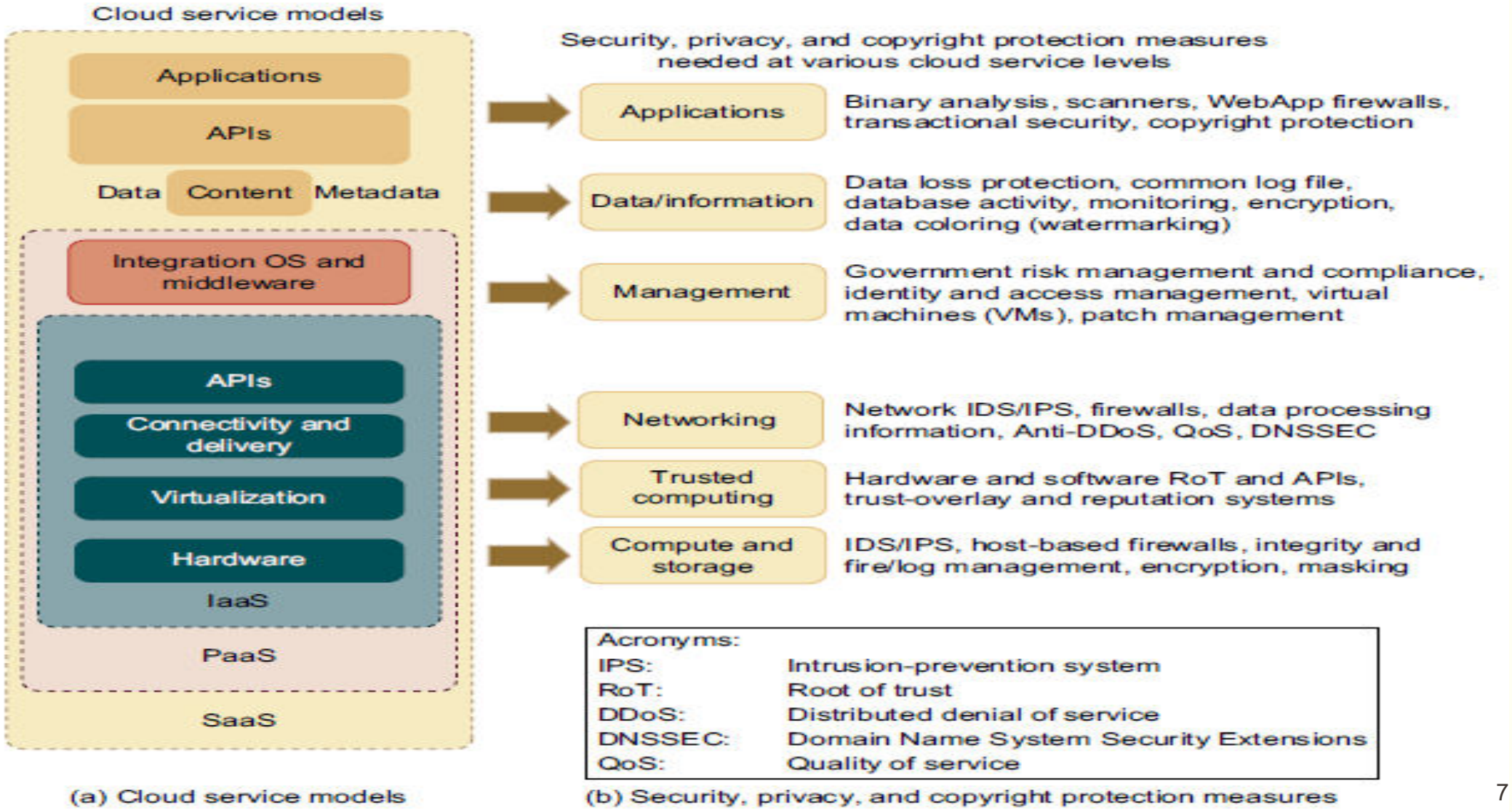
CLOUD SECURITY DEFENSE STRATEGIES

- The security demands of three cloud service models, IaaS, PaaS, and SaaS, are described in this section.
- These security models are based on various SLAs between providers and users.
- Basic Cloud Security
- Security Challenges in VMs
- Cloud Defense Methods
- Defense with Virtualization
- Privacy and Copyright Protection

CLOUD SECURITY DEFENSE STRATEGIES

- **Basic Cloud Security**
- Three basic cloud security enforcements are expected.
- First, facility security in data centers demands on-site security year round. Biometric readers, CCTV (close-circuit TV), motion detection, and man traps are often deployed.
- Also, network security demands fault-tolerant external firewalls, intrusion detection systems (IDSes), and third-party vulnerability assessment.
- Finally, platform security demands SSL and data decryption, strict password policies, and system trust certification.

CLOUD SECURITY DEFENSE STRATEGIES



CLOUD SECURITY DEFENSE STRATEGIES

- **Basic Cloud Security**
- 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

CLOUD SECURITY DEFENSE STRATEGIES

- **Security Challenges in VMs**
- Traditional network attacks include buffer overflows, DoS attacks, spyware, malware, rootkits, Trojan horses, and worms.
- In a cloud environment, newer attacks may result from hypervisor malware, guest hopping and hijacking, or VM rootkits.
- Another type of attack is the man-in-the-middle attack for VM migrations.
- In general, passive attacks steal sensitive data or passwords.
- Active attacks may manipulate kernel data structures which will cause major damage to cloud servers.

CLOUD SECURITY DEFENSE STRATEGIES

- **Cloud Defense Methods**
- Virtualization enhances cloud security.
- But VMs add an additional layer of software that could become a single point of failure. With virtualization, a single physical machine can be divided or partitioned into multiple VMs (e.g., server consolidation).
- This provides each VM with better security isolation and each partition is protected from DoS attacks by other partitions.
- Security attacks in one VM are isolated and contained from affecting the other VMs.

CLOUD SECURITY DEFENSE STRATEGIES

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 DEFENSE STRATEGIES

- **Defense with Virtualization**
- The VM is decoupled from the physical hardware.
- The entire VM can be represented as a software component and can be regarded as binary or digital data.
- The VM can be saved, cloned, encrypted, moved, or restored with ease.
- VMs enable High Availability and faster disaster recovery.

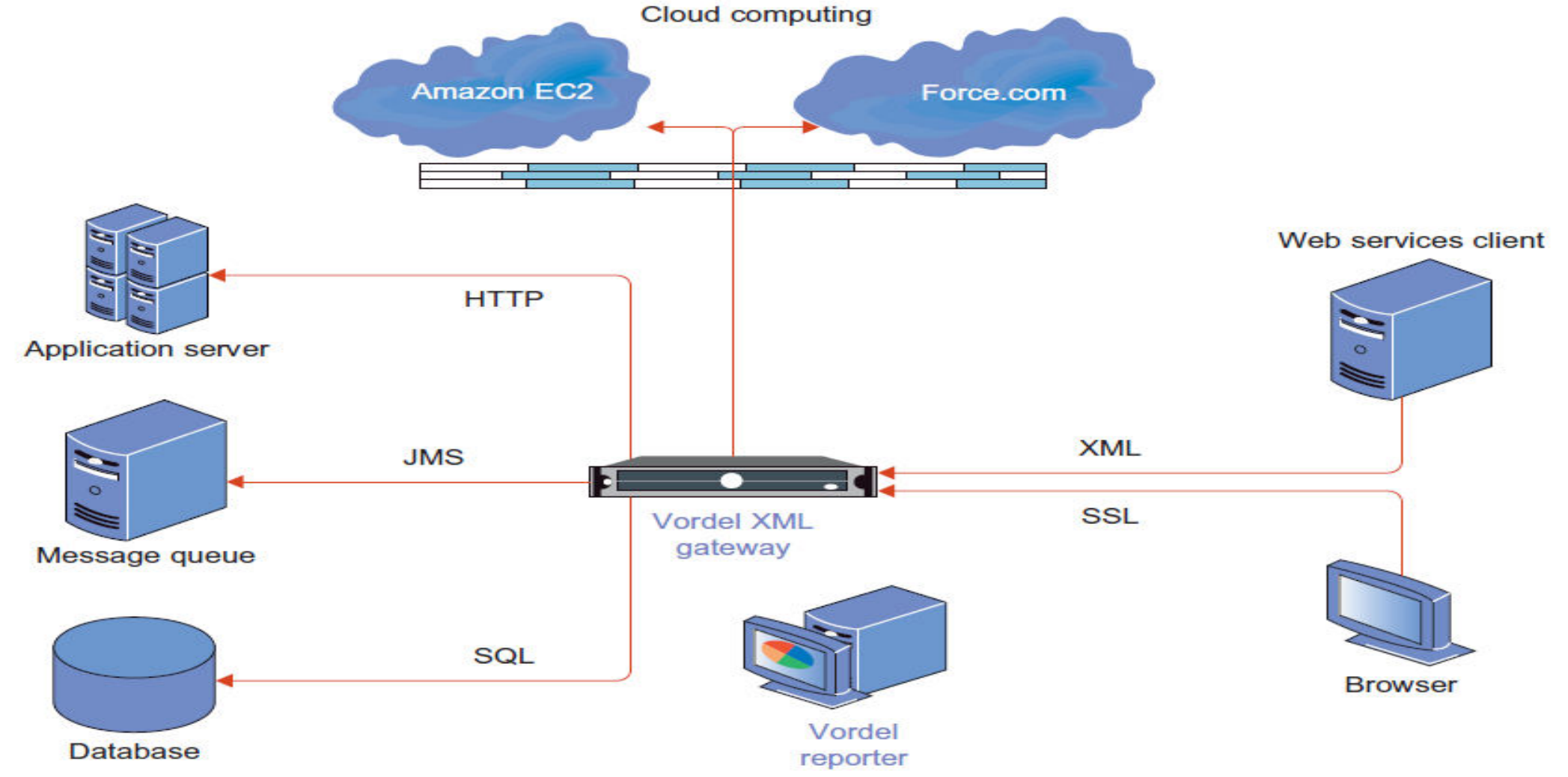
CLOUD SECURITY DEFENSE STRATEGIES

- **Privacy and Copyright Protection**
- The user gets a predictable configuration before actual system integration.
- Yahoo!’s Pipes is a good example of a lightweight cloud platform.
- 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.

CLOUD SECURITY DEFENSE STRATEGIES

- **Privacy and Copyright Protection**
- Here are 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

CLOUD SECURITY DEFENSE STRATEGIES



SECURING THE CLOUD AND DATA

- Organizations in all sectors recognize the benefits of cloud computing.
- Some are only beginning their migration journey as part of digital transformation efforts, while others are adopting advanced multi-cloud, hybrid strategies.
- One of the biggest challenges at any stage of implementation is data security in cloud computing, stemming from the unique risks that the technology brings.
- The cloud erodes the traditional network perimeter that drove cybersecurity strategies in the past.
- Data security in cloud computing requires a different approach one that considers not only the threats but also the complexity of data governance and security models in the cloud.

SECURING THE CLOUD AND DATA

- Cloud data security is the combination of technology solutions, policies, and procedures that you implement to protect cloud-based applications and systems, along with the associated data and user access.
- The core principles of information security and data governance data confidentiality, integrity, and availability (known as the CIA triad) also apply to the cloud:
- **Confidentiality:** protecting the data from unauthorized access and disclosure
- **Integrity:** safeguard the data from unauthorized modification so it can be trusted
- **Availability:** ensuring the data is fully available and accessible when it's needed

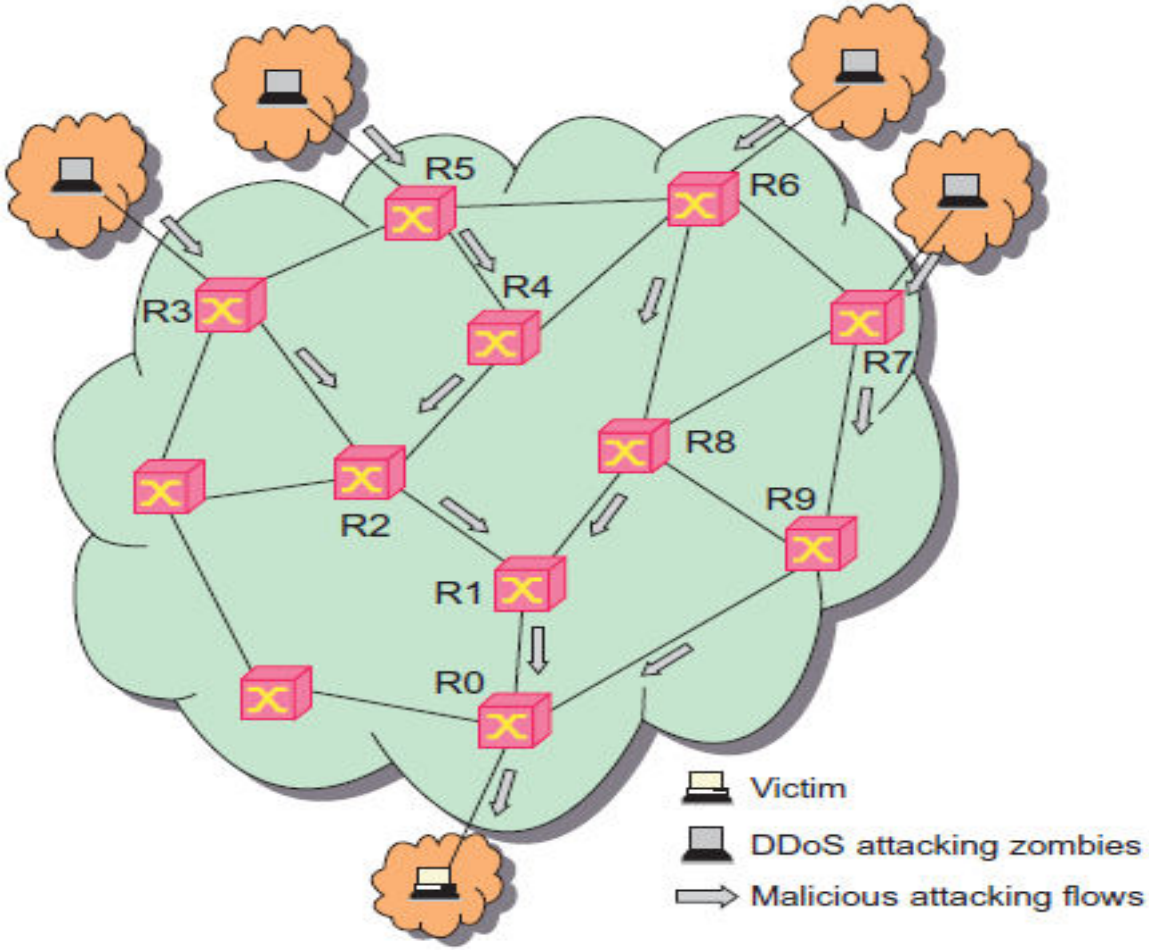
DISTRIBUTED INTRUSION AND ANOMALY DETECTION

- Data security is the weakest link in all cloud models.
- We need new cloud security standards to apply common API tools to cope with the data lock-in problem and network attacks or abuses.
- The IaaS model represented by Amazon is most sensitive to external attacks.
- Role-based interface tools alleviate the complexity of the provisioning system.
- For example, IBM's Blue Cloud provisions through a role-based web portal.
- A SaaS bureau may order secretarial services from a common cloud platform.
- Many IT companies are now offering cloud services with no guaranteed security.

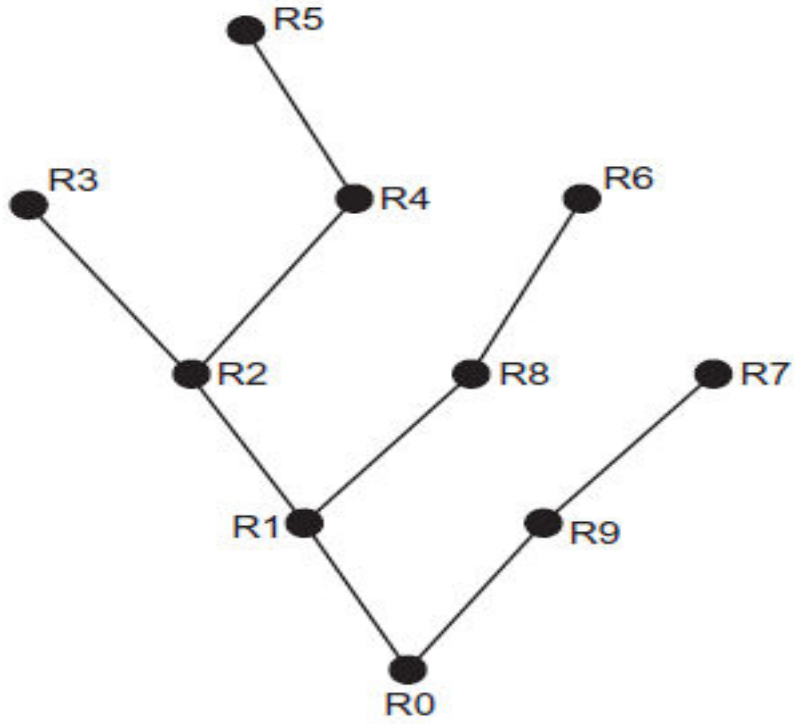
DISTRIBUTED INTRUSION AND ANOMALY DETECTION

- **Distributed Defense against DDoS Flooding Attacks**
- A DDoS defense system must be designed to cover multiple network domains spanned by a given cloud platform.
- These network domains cover the edge networks where cloud resources are connected.
- DDoS attacks come with widespread worms.
- The flooding traffic is large enough to crash the victim server by buffer overflow, disk exhaustion, or connection saturation.

DISTRIBUTED INTRUSION AND ANOMALY DETECTION



(a) Traffic flow pattern of a DDoS attack



(b) The attack traffic flow tree over 10 routers

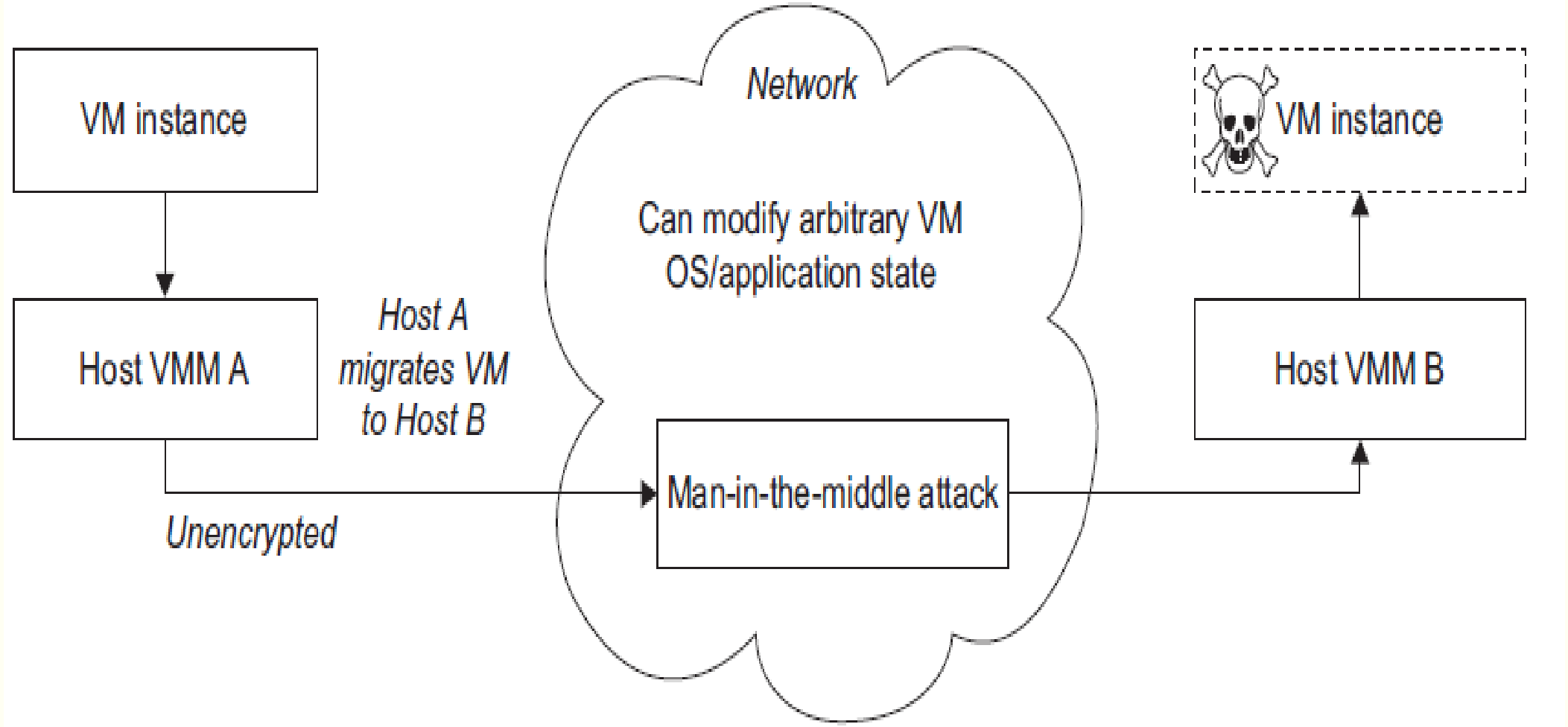
DATA AND SOFTWARE PROTECTION TECHNIQUES

- We will introduce a data coloring technique to preserve data integrity and user privacy.
- Then we will discuss a watermarking scheme to protect software files from being widely distributed in a cloud environment.
- **Data Integrity and Privacy Protection**
- **Data Coloring and Cloud Watermarking**
- **Data Lock-in Problem and Proactive Solutions**

DATA AND SOFTWARE PROTECTION TECHNIQUES

- **Data Integrity and Privacy Protection**
- Users desire a software environment that provides many useful tools to build cloud applications over large data sets.
- In addition to application software for MapReduce, BigTable, EC2, S3, Hadoop, AWS, GAE, and WebSphere2, users need some security and privacy protection software for using the cloud.

DATA AND SOFTWARE PROTECTION TECHNIQUES



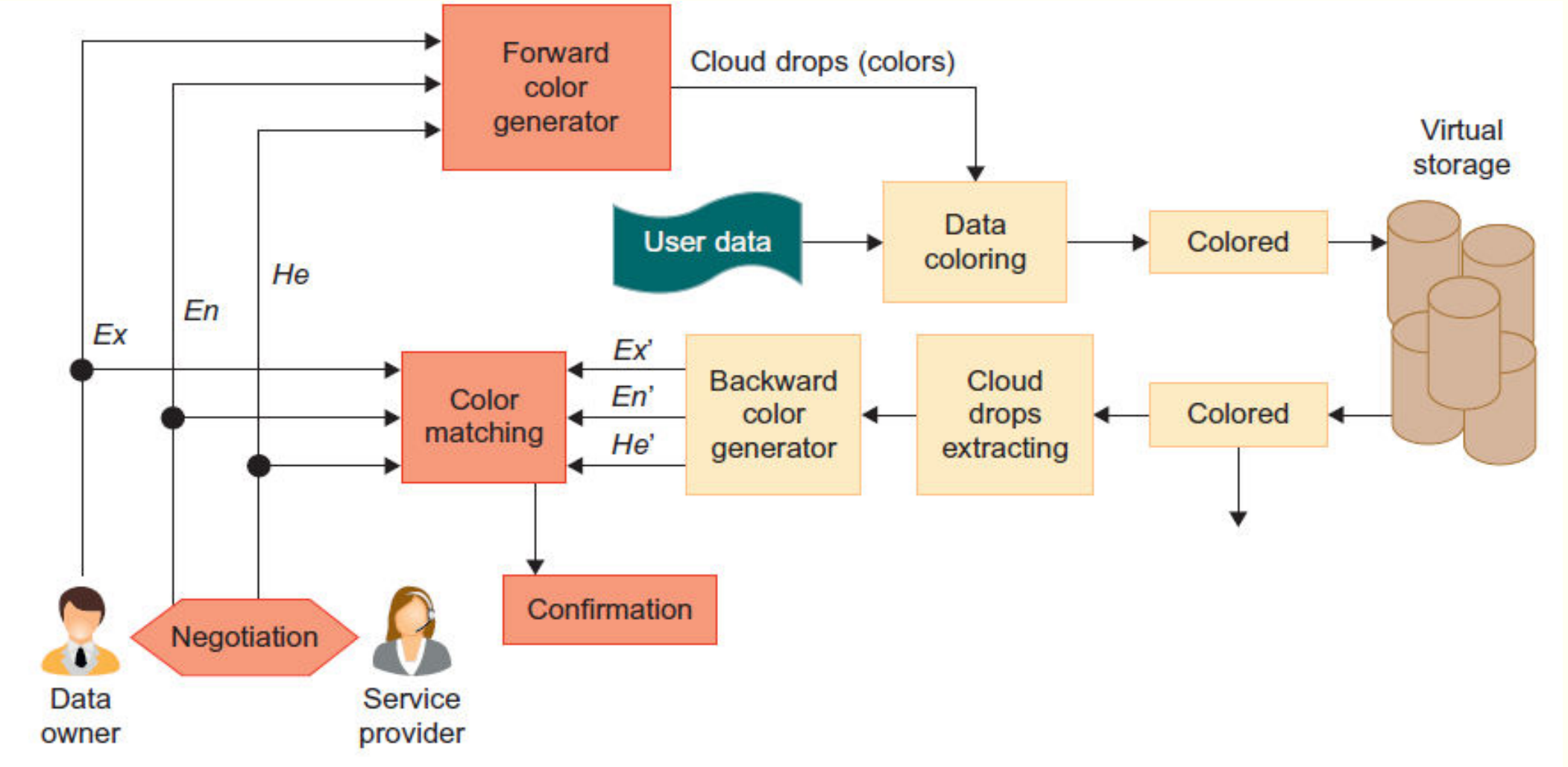
DATA AND SOFTWARE PROTECTION TECHNIQUES

- Such software should offer the following features:
  - 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 Coloring and Cloud Watermarking**
- 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.
- In the past, watermarking was mainly used for digital copyright management.
- 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.

DATA AND SOFTWARE PROTECTION TECHNIQUES



DATA AND SOFTWARE PROTECTION TECHNIQUES

- **Data Lock-in Problem and Proactive Solutions**
- Cloud computing moves both the computation and the data to the server clusters maintained by cloud service providers.
- Once the data is moved into the cloud, users cannot easily extract their data and programs from cloud servers to run on another platform.

DATA SECURITY IN THE CLOUD

- Organizations in all sectors recognize the benefits of cloud computing.
- Some are only beginning their migration journey as part of digital transformation efforts, while others are adopting advanced multi-cloud, hybrid strategies.
- One of the biggest challenges at any stage of implementation is data security in cloud computing, stemming from the unique risks that the technology brings.
- The cloud erodes the traditional network perimeter that drove cybersecurity strategies in the past.
- Data security in cloud computing requires a different approach one that considers not only the threats but also the complexity of data governance and security models in the cloud.

DATA SECURITY IN THE CLOUD

- Cloud data security refers to the technologies, policies, services and security controls that protect any type of data in the cloud from loss, leakage or misuse through breaches, exfiltration and unauthorized access. A robust cloud data security strategy should include:
- Ensuring the security and privacy of data across networks as well as within applications, containers, workloads and other cloud environments
- Controlling data access for all users, devices and software
- Providing complete visibility into all data on the network

DATA SECURITY IN THE CLOUD

- The cloud data protection and security strategy must also protect data of all types. This includes:
- **Data in use:** Securing data being used by an application or endpoint through user authentication and access control
- **Data in motion:** Ensuring the safe transmission of sensitive, confidential or proprietary data while it moves across the network through encryption and/or other email and messaging security measures
- **Data at rest:** Protecting data that is being stored on any network location, including the cloud, through access restrictions and user authentication

THE CURRENT STATE OF DATA SECURITY IN THE CLOUD

- A report looks at the perceptions and actions of IT professionals regarding cloud data security and cloud data protection measures.

1. Organizations are using centralized platforms to provide multi-cloud security
2. Organizations are taking steps to protect their data before it reaches the cloud
3. Identity and access control in the cloud has increased in importance for organizations
4. Organizational interest in SASE is growing
5. Cloud-based security continues to thrive

CLOUD COMPUTING AND DATA SECURITY RISK

- Cloud computing provides various advantages, such as improved collaboration, excellent accessibility, Mobility, Storage capacity, etc. But there are also security risks in cloud computing.
- Some most common Security Risks of Cloud Computing are given below-
  - Data Loss
  - Hacked Interfaces and Insecure APIs
  - Data Breach
  - Vendor lock-in
  - Increased complexity strains IT staff
  - Spectre & Meltdown
  - Denial of Service (DoS) attacks
  - Account hijacking

CLOUD COMPUTING AND DATA SECURITY RISK

- **Data Loss** - Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage.
- **Hacked Interfaces and Insecure APIs** - cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users.
- **Data Breach** - Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.
- **Vendor lock-in** - Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.

CLOUD COMPUTING AND DATA SECURITY RISK

- **Increased complexity strains IT staff** - Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.
- **Spectre & Meltdown** - Spectre & Meltdown allows programs to view and steal data which is currently processed on computer. It can run on personal computers, mobile devices, and in the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.
- **Denial of Service (DoS) attacks** - Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.
- **Account hijacking** - Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.

THE CLOUD, DIGITAL IDENTITY, AND DATA SECURITY

- In access management, digital identity is the recorded set of measurable characteristics by which a computer can identify an external entity.
- That entity may be a person, an organization, a software program, or another computer.
- Digital identity relies on computer-identifiable attributes.
- Almost every person who uses computers or accesses the Internet today has some form of digital identity.
- That may be an email address and password combination, their history of Internet browsing, their shopping history and credit card information saved by an online store, or identifying characteristics stored in an identity and access management (IAM) system.

ESTABLISHING IDENTITY IN CLOUD

- Cloud Identity is an Identity as a Service (IDaaS) solution that centrally manages users and groups.
- You can configure Cloud Identity to federate identities between Google and other identity providers, such as Active Directory and Azure Active Directory.
- Cloud Identity also gives you more control over the accounts that are used in your organization.
- For example, if developers in your organization use personal accounts, such as Gmail accounts, those accounts are outside of your control.
- When you adopt Cloud Identity, you can manage access and compliance across all users in your domain.
- When you adopt Cloud Identity, you create a Cloud Identity account for each of your users and groups. You can then use Identity and Access Management (IAM) to manage access to Google Cloud resources for each Cloud Identity account.

REFERENCES

1. Kai Hwang, Geoffrey C Fox and Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.
2. Barrie Sosinky,"Cloud Computing Bible", Wiley Publishing Inc,2011
3. Buyya R., Broberg J. and Goscinski A., "Cloud Computing: Principles and Paradigm", First Edition, John Wiley & Sons, 2011.
4. Rajkumar Buyya, Christian Vecchiola, S. ThamaraiSelvi,"Mastering the Cloud Computing", Morgan Kaufmann,2013
5. John W. Rittinghouse and James F. Ransome, "Cloud Computing: Implementation "Management, and Security", CRC Press, 2016.
6. David Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes", IEEE Cloud Computing, Volume: 1 , Issue: 3 , 2014.
7. VMware (white paper),"Understanding Full Virtualization, Paravirtualization, and Hardware Assist ":www.vmware.com/files/pdf/VMware_paravirtualization.pdf.

Thank You…