SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 7
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Topic 4 – Security Overview

Security Overview

- Cloud computing supports the development of elastically scalable systems
- This is done by leveraging large computing infrastructures that eventually host applications, services, and data.
- In this scenario, security arrangements constitute a fundamental requirement that cannot be overlooked.
- Cloud providers ensure that their customers' applications and data are secure if they hope to retain their customer base and competitiveness.
- Security management becomes even more complex in the case of a cloud federation, where confidential information is dynamically moved across several cloud computing vendors.

Security Overview

Three basic cloud security enforcements are expected.

- **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.
- **network secur**ity demands fault-tolerant external firewalls, intrusion detection systems (IDSes), and third-party vulnerability assessment.
- **platform security** demands SSL and data decryption, strict password policies, and system trust certification.

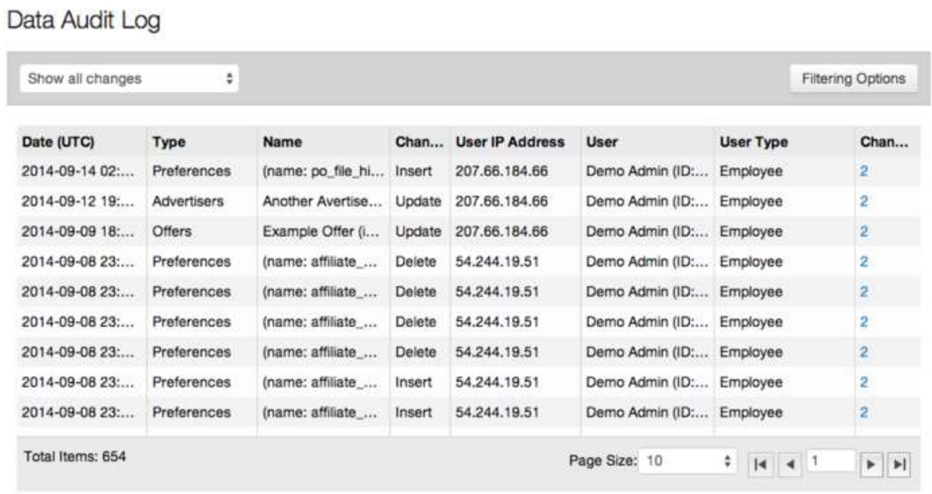
Security Overview

In-terms of services the following security measures are needed.

- IaaS vendors are required to provide basic security in terms of auditing and logging of access to virtual machine instances or cloud storage.

- PaaS vendors are expected to offer a secure development platform and a runtime environment for applications.

- SaaS vendors have the major responsibilities in terms of security, since they have to build a secure computing stack (infrastructure, platform, and applications) that users customize for their needs.



Data Audit Log

Date (UTC)	Type	Name	Chan...	User IP Address	User	User Type	Chan...
2014-09-14 02:...	Preferences	(name: po_file_hi...	Insert	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-12 19:...	Advertisers	Another Avertise...	Update	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-09 18:...	Offers	Example Offer (i...	Update	207.66.184.66	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Delete	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Insert	54.244.19.51	Demo Admin (ID:...	Employee	2
2014-09-08 23:...	Preferences	(name: affiliate_...	Insert	54.244.19.51	Demo Admin (ID:...	Employee	2

Total Items: 654

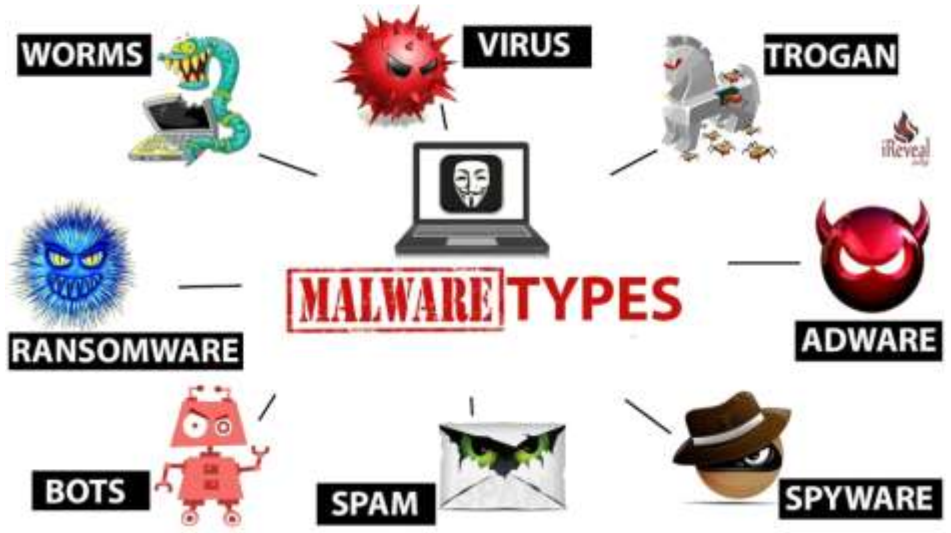
Page Size: 10

Security Overview

- 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



Data Protection and Privacy
HELP in the 28
EUROPEAN PROGRAMME FOR HUMAN RIGHTS EDUCATION FOR LEGAL PROFESSIONALS

Security Overview

- Key elements in management of security in a cloud scenario have been identified as the following,

✓ Availability management (ITIL)

✓ Access control (ISO/IEC 27002, ITIL)

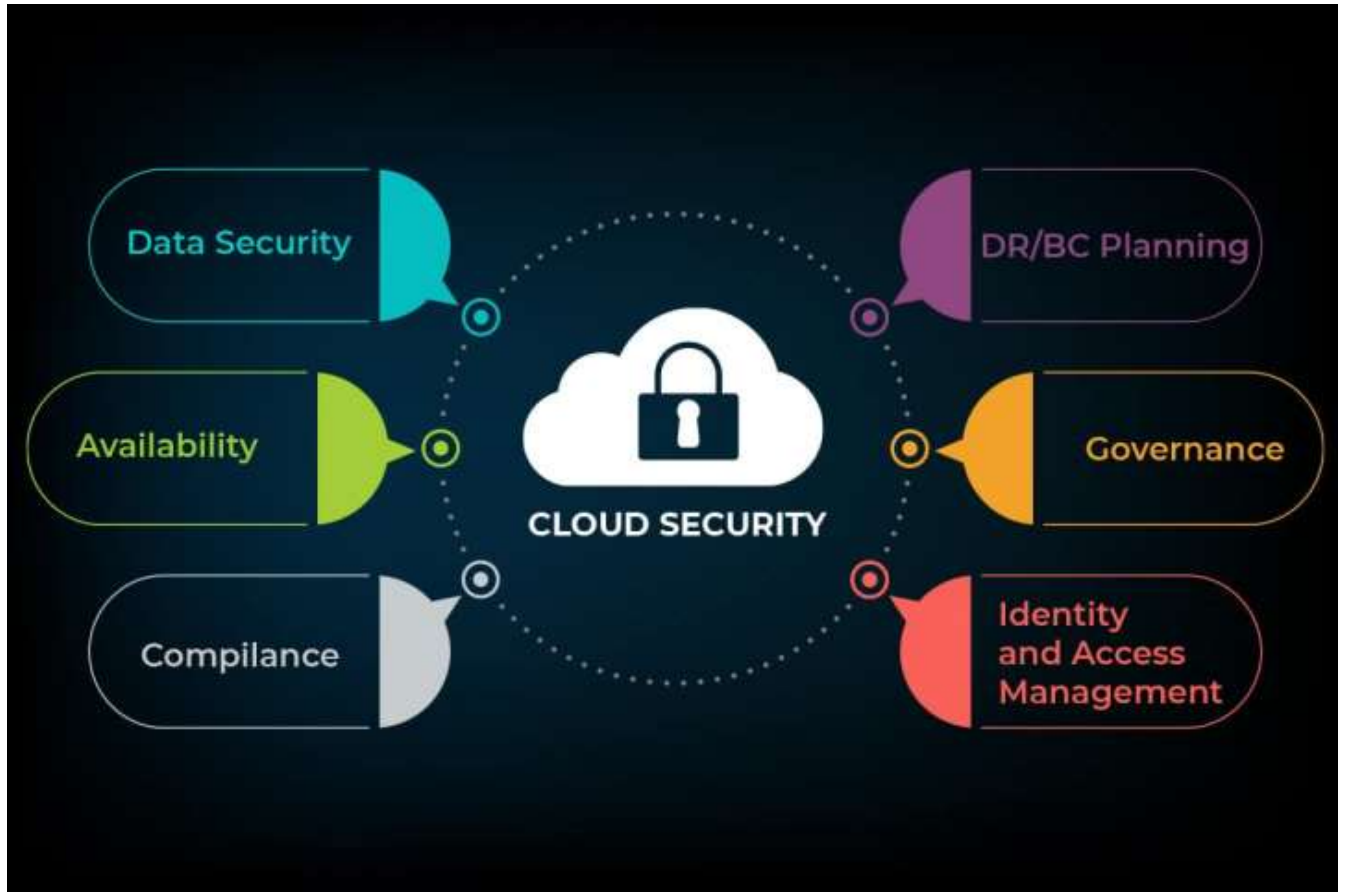
✓ Vulnerability management (ISO/IEC 27002)

✓ Patch management (ITIL)

✓ Configuration management (ITIL)

✓ Incident response (ISO/IEC 27002)

✓ System use and access monitoring



THANK YOU