TechLift

KICKSTART YOUR CAREER

Cloud Computing Basics
What, why, & how

P@SHA

Pakistan Software Houses Association for IT & ITES

PAKISTAN PSEB SOFTWARE EXPORT BOARD

S. No.	Topics
1	What’s in it for you? Before Cloud Computing About Hypervisors and virtualization
2	What is cloud computing? Types of Cloud Computing Public Cloud Private Cloud Hybrid Cloud IP Addressing with Types
3	Cloud Architecture Benefits IaaS, PaaS, SaaS
4	Benefits Of Cloud Computing
5	Cloud Management
6	Microservices Architecture How MicroServices Works? Benefits Microservices Challenges of MicroServices Characteristics of MicroServices MicroServices in Cloud Benefits of using Microservices in cloud

S. No.	**Topics**
7	Cloud VS on-prem Security Introduction On-prem Security Benefits Cost of On-prem Security Benefits of Cloud Security Cons of Cloud Security
8	**Cloud Computing Security Deep Dive** **What is Cloud Security** **Principal of Cloud Computing Security** **Cloud Computing Security Best practice**
9	Module Review AWS Certification Road Map Azure Certification Road Map

TechLift

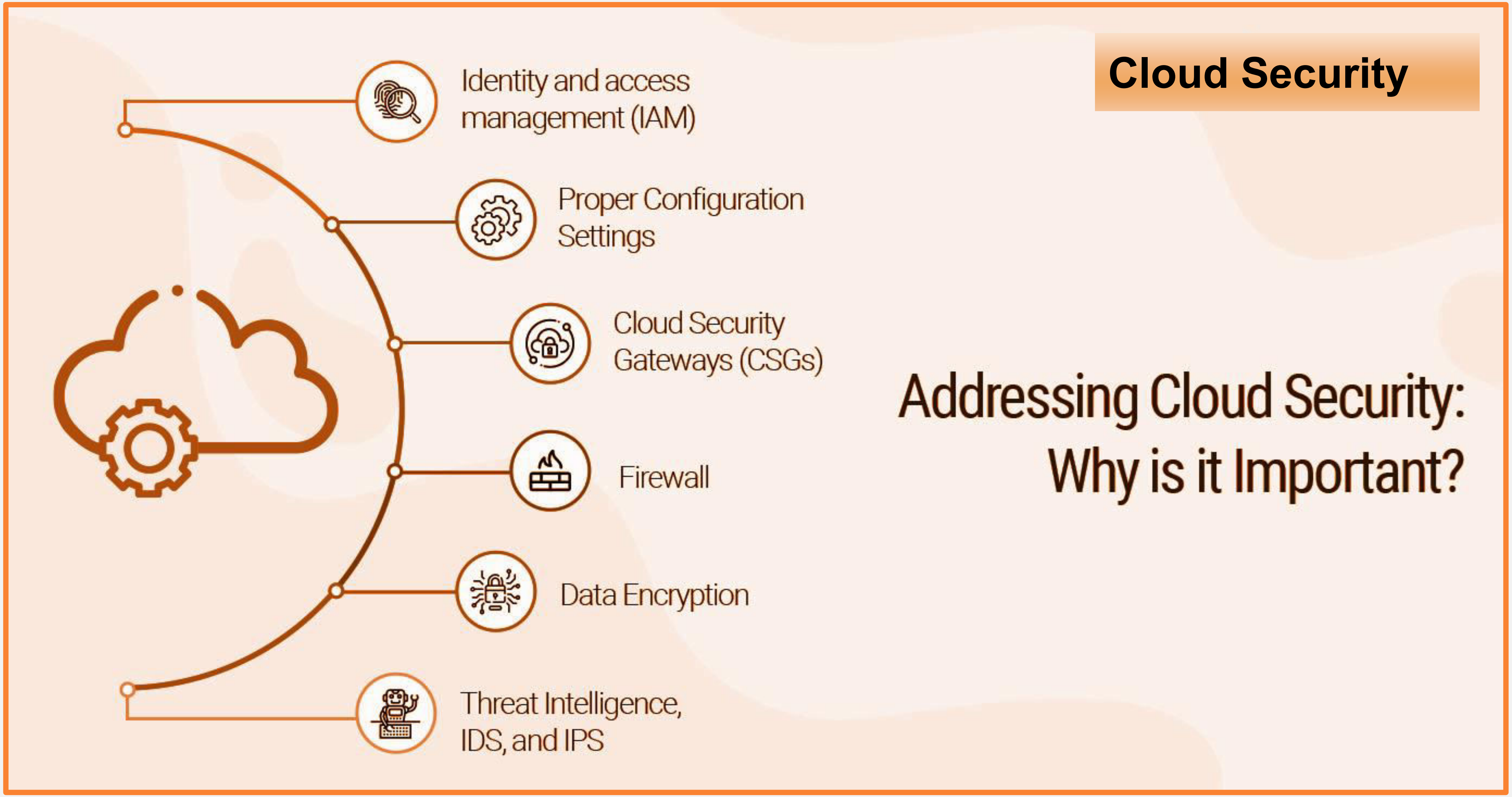
KICKSTART YOUR CAREER

Cloud Computing Security

P@SHA
Pakistan Software Houses Association for IT & ITES

PAKISTAN
PSEB
SOFTWARE EXPORT BOARD

Cloud Security



Addressing Cloud Security: Why is it Important?

- Identity and access management (IAM)
- Proper Configuration Settings
- Cloud Security Gateways (CSGs)
- Firewall
- Data Encryption
- Threat Intelligence, IDS, and IPS

What Is Cloud Securtiy:

- Cloud computing security refers to the discipline and practice of protection.
- Cloud security entails securing cloud environments
- While cloud security applies to security for cloud environments, the related term, cloud-based security, refers to the software as a service (SaaS) delivery model of security services, which are hosted in the cloud rather than deployed via on-premise hardware or software.

Principal Of Cloud Computing Securtiy:

Lack of Visibility & Shadow IT

- Cloud computing makes it easy for anyone to subscribe to a SaaS application or even to spin up new instances and environments.
- Users should adhere to strong acceptable use policies for obtaining authorization for, and for subscribing to, new cloud services or creating new instances.

Principal Of Cloud Computing Securtiy:

Lack of Control

- Leasing a public cloud service means an organization does not have ownership of the hardware, applications, or software on which the cloud services run.
- Ensure that you understand the cloud vendor’s approach to these assets.

Principal Of Cloud Computing Securtiy:

Transmitting & Receiving Data

- ➔ Cloud applications often integrate and interface with other services, databases, and applications.
- ➔ This is typically achieved through an application programming interface (API).
- ➔ It’s vital to understand the applications and people who have access to API data and to encrypt any sensitive information.

Principal Of Cloud Computing Securtiy:

Embedded/Default Credentials & Secrets

- Cloud applications may contain embedded and/or default credentials.
- Default credentials post an increased risk as they may be guessable by attackers.
- Organizations need to manage these credentials as they would other types of privileged credentials.

Principal Of Cloud Computing Securtiy:

Incompatibilities

IT tools architected for on-premise environments or one type of cloud are frequently incompatible with other cloud environments.

Incompatibilities can translate into visibility and control gaps that expose organizations to risk from misconfigurations, vulnerabilities, data leaks, excessive privileged access, and compliance issues.

Multitenancy

Multi Tenancy is the backbone for many of the cloud benefits of shared resources (e.g., lower cost, flexibility, etc.), but it also introduces concerns about data isolation and data privacy.

Principal Of Cloud Computing Securtiy:

Scalability Cuts Both Ways

Automation and rapid scalability are chief benefits of cloud computing, but the flip side of cloud computing security is listed below:

- Vulnerabilities
- Misconfigurations
- Sharing of secrets–APIs
- Privileged credentials
- SSH keys
- Can also proliferate at speed and scale.

Principal Of Cloud Computing Securtiy:

Malware & External Attackers

Attackers can make a living by exploiting cloud vulnerabilities.

Rapid detection, and a multi-layered security approach (firewalls, data encryption, vulnerability management, threat analytics, identity management, etc.) will help you to reduce risk, while leaving you better poised to respond to withstand an attack

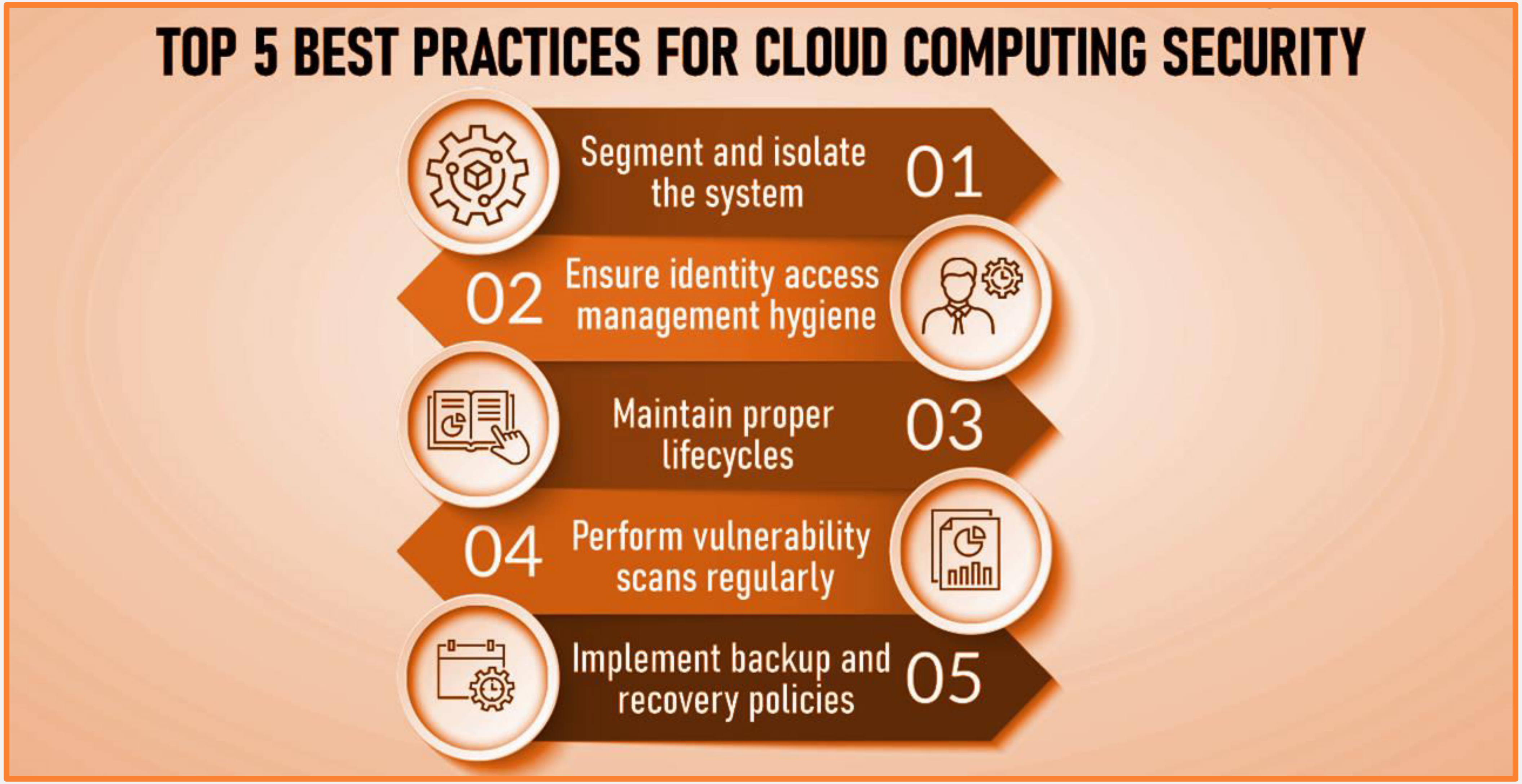
Principal Of Cloud Computing Securtiy:

Insider Threats – Privileges

Insider-related threats (either through negligence or malevolence), generally take the longest to detect and resolve, with the potential to be the most harmful.

A strong identity and access management framework along with effective privilege management tools are essential to eliminating these threats, and reducing the damage (such as by preventing lateral movement and privilege escalation) when they do occur.

Cloud Computing Security Best Practice



TOP 5 BEST PRACTICES FOR CLOUD COMPUTING SECURITY

01 Segment and isolate the system

02 Ensure identity access management hygiene

03 Maintain proper lifecycles

04 Perform vulnerability scans regularly

05 Implement backup and recovery policies

Best Practice Of Cloud Computing Securtiy:

Strategy & Policy

A holistic cloud security program should account for ownership and accountability (internal/external) of cloud security risks, gaps in protection/compliance, and identify controls needed to mature security and reach the desired end state.

Network Segmentation

In multi-tenant environments, assess what segmentation is in place between your resources and those of other customers, as well as between your own instances.

Leverage an isolation approach to isolate instances, containers, applications, and full systems from each other when possible.

Best Practice Of Cloud Computing Securtiy:

Identity and Access Management and Privileged Access Management

Leverage robust identity management and authentication processes to ensure only authorized users having access to the cloud environment, applications, and data.

Enforce least privilege to restrict privileged access and to harden cloud resources.

Ensure privileges are role-based, and that privileged access is audited and recorded via session monitoring.

Best Practice Of Cloud Computing Securtiy:

Discover and Onboard Cloud Instances and Assets

Once cloud instances, services, and assets are discovered and grouped, bring them under management (i.e. managing and cycling passwords, etc.).

Discovery and onboarding should be automated as much as possible to eliminate shadow Infrastructure.

Best Practice Of Cloud Computing Securtiy:

Password Control (Privileged and Non-Privileged Passwords)

Never allow the use of shared passwords. Combine passwords with other authentication systems for sensitive services. Ensure password management best practices.

Vulnerability Management

Regularly perform vulnerability scans and security audits, and patch known vulnerabilities.

Best Practice Of Cloud Computing Securtiy:

Encryption

Ensure your cloud data is encrypted, at rest, and in transit.

Disaster Recovery

Be aware of the data backup, retention, and recovery policies and processes for your cloud vendor(s).

Best Practice Of Cloud Computing Securtiy:

Monitoring, Alerting, and Reporting

Implement continual security and user activity monitoring across all environments and instances.

Integrate and centralize data from your cloud provider (if available) with data from in-house and other vendor solutions, so you have a holistic picture of what is happening in your environment.

Q&A Session

Q) What are the cloud security threats facing the public cloud?

A) Organizations rank the following threats as the largest obstacles for public clouds:

- Misconfigurations of the cloud platform/incorrect set up
- Unauthorized access
- Insecure interfaces/APIs

Q) Explain the Cloud Security controls?
A)

- Risk management
- Governance
- Data Protection
- Identity and Access Management
- Compliance

What we achieved?

Introducing the Cloud

Hypervisors

Types Of Cloud

Architecture of Cloud

Microservices

Cloud Security

AWS Certification RoadMap

Azure Certification RoadMap