# Cloud Computing Security Reference Architecture Framework

*Skills and expertise to help you increase your knowledge in the field of secure cloud technologies*

TLC Education & Training Services

## About this workshop

Security in the cloud is just as vital as security in on-premises environments. Hardening a system is a way to protect it by reducing vulnerability. While hundreds of security recommendations may exist to harden any one technology, this course especially focuses on standard cloud security best practices, knowing key objectives prior embarking in the cloud, consensus-driven security configuration guidelines and recommendations subject to different cloud services and deployment models.

Moreover, before you invest in migrating your application to cloud, there is a need to study what measures to be taken prior selecting cloud security tools that not only support feature like DLP and Shadow IT but also understand how to provide end to end API security. We will be covering the role of Multi-Mode Next-Generation CASB Architecture details in this two-day online workshop.

It is important to perform a due diligence and thorough planning session prior selecting your CASB product/vendor. You should avoid taking a wrong decision in opting your solution based on API-only CASB architecture and Multi-Mode First Generation CASB Architecture. We will be covering Multi-Mode Next-Generation CASB Architecture as one of the unit in our course.

Cloud security architecture is a strategy designed to secure and view an enterprise's data and applications in the cloud through the lens of **shared responsibility** between you and your services provider

## Target Audience

- Customers who want to build their knowledge in the space of Cloud security technologies and want to understand how to smartly tackle the growing security challenges associated with businesses and how to address complex problems associated with data hosted in the cloud.
- CIO/CTO/CISO/CDO, IT Directors/GM IT, Business and Technology Leaders, IT Managers, Strategic Planners, Project Managers, Solution/IT/Systems Architects, Enterprise Architects, Business Analysts, Security Operations Center Teams, Risk professionals, Cloud Engineers, and Technical Writers, and technology vendors.

## Unit 1 – Cloud and Cloud Storage Fundamentals

- Cloud Computing and Cloud Storage Defined.
- Defining Service Oriented Architecture (SOA) and Web Services.
- Describe Representational State Transfer (REST) Architecture.
- Understand Cloud Service and Deployment Models' their details.
- Problems in moving workloads to cloud and Application Readiness.
- Cloud solution to common IT problems & challenges.
- Business benefits of using Cloud Storage and associated Risks.
- Cloud Storage Initiative by SNIA – Cloud Data Mgt. Interface.
- Scalable Cloud Services Architecture & Storage Access Protocols.
- Types of Cloud Storage Models and their types and applications.
- Understand API and Cloud storage API protocols.
- Obstacles to establish connectivity to Object Cloud Storage.
- Understanding the Role of Cloud Storage Gateways.
- Protocols supported by Cloud Storage Gateways.
- What are the negatives to cloud computing and Security Concerns.
- Data protection in the cloud and Cloud Seeding problems.
- Compliance in the context of Data Protection & Technologies.
- Understanding the Role of Data Sanitization and Best Practices.
- Cloud enabling infrastructure technology used by low cost CSP.
- Unit 1 Assessment

## Unit 2 - User and Entity Behavior Analytics Fundamental Principles

- UEBA – User and Entity Behavior Analytics Defined.
- Understanding UEBA Engines.
- Three pillars of UEBA – Use Cases, Data Sources, and Analytics.
- Exploring main components of UEBA.
- Convergence of UEBA and SIEM.
- UEBA and SIEM comparison and UEBA integration with SIEM.
- Similarities and Dissimilarities between SIEM and UEBA solution.
- Why do organizations need UEBA and How UEBA works and UEBA Threat Workflow.
- Enterprise Data Sources analyzed by UEBA.
- Facts for a successful implementation of UEBA solution.
- UEBA for Enterprise Security – A layered-wise approach.
- UEBA Risk Scoring and Threat Indicator Signs.
- UEBA for Enterprise Security for threat hunting and incident investigation.
- Critical Devices of UEBA Systems.
- Best Practices for building a baseline of User Behavior – Define Use case, Define Data Source, Define Behaviors, Establish the Baseline, Update Policies and Training Awareness Program, Conduct Testing, Rebuild Baseline.
- Unit 2 Assessment.

## Unit 3 – Ensure Secure and Reliable Network Connections

- Ensure secure, Fast, and Reliable Customer Connections.
- Overcome DNS challenges and strengthening client side security.
- Explore client-side attacks and client side protection.
- TLS challenges and effectively implementing TLS based solutions.
- Global CDN, Faster Routing and Mobile Optimization.
- How to select tools for optimal network path selection.
- Web Application Firewall and their challenges.
- Strengthen Security Posture for your WAF Infrastructure.
- Bot Mitigation and their challenges.
- DDoS Attack Mitigation and what to look for in a DDoS mitigation services provider.
- Understand Load Balancing and its challenges.
- Detect Anomalous behavior and Secure Web properties at the Edge.
- Data Loss Prevention challenges and an end-to-end DLP solution.
- Edge Programmability challenges.
- Unit 3 Assessment.

## Unit 4 – The Role of CASB and SASE in Cloud Computing

- Cloud Management Components and Cloud Architecture.
- Cloud Computing Reference Architecture – CCRA.
- NIST Cloud Computing Reference Architecture.
- Pillars of Robust Cloud Security and Top Cloud Application Security Threats.
- Understand Cloud Access Security Broker.
- Security features offered by Cloud Access Security Broker.
- How Cloud Access Security Broker work?
- Requirements of a CASB Solution and why do I need a CASB solution?
- Cloud Access Security Broker Solution Deployment Models.
- Three key considerations for choosing a CASB.
- Multi-Mode Next-Gen CASB Architecture.
- Use Cases and Best Practices for Cloud Access Security Broker implementation.
- Cloud Access Security Broker Vs. Secure Access Service Edge.
- Privileged Access Management Defined.
- Unprivileged to Privileged Access Management using Zero Trust Architecture.
- Understand Secure Access Service Edge (SASE).
- SASE Architecture – CASB within SASE.
- Pros and Cons of SASE & CASB– Advantages and challenges for enterprises.
- Comparative Analysis on SASE Vs. CASB.
- Unit 4 Assessment.

## Detailed Information

| | |
|---|---|
| Course Code | : TN221 |
| Course Duration | : 2 Day Workshop |
| Course Location | : TLC, Customer On-site & Online. |
| Terms & Conditions | : 100% payment in advance. |
| Course Deliverable | : Comprehensive Student Guide and Course Certificate |