Certified Cloud Security Professional (CCSP)

Notes by Al Nafi

Domain 2

Cloud Data Security

Author:

Suaira Tariq Mahmood

Cloud Storage Architectures

Cloud storage architectures define how data is stored, accessed, and managed within cloud environments. This chapter builds upon the previous discussions on data classification, jurisdictional requirements, information rights management (IRM), and data control, ensuring that data is stored in the most efficient and secure manner. Understanding cloud storage architectures is critical for organizations implementing data retention, encryption, and access control policies, as different storage models influence how security measures are applied.

Cloud storage solutions are broadly categorized into Volume Storage (File-Based and Block Storage), Object-Based Storage, Databases, and Content Delivery Networks (CDNs). Each type serves specific use cases, offering different trade-offs in performance, scalability, and security. Selecting the appropriate storage model requires aligning business needs, compliance requirements, and operational workflows with the available cloud storage technologies.

Volume Storage: File-Based Storage and Block Storage

Volume storage is a foundational component of cloud infrastructure, designed to provide persistent and high-performance storage for applications, virtual machines, and containers. It is typically deployed in Infrastructure as a Service (IaaS) environments and is directly accessible by the operating system.

File-Based Storage

File-based storage follows a hierarchical model where data is stored in directories and subdirectories, similar to traditional file systems. It is commonly used for collaborative file-sharing, document storage, and network file systems (NFS or SMB) in enterprise environments. File-based storage is structured in a way that allows users to organize and retrieve data efficiently. It supports protocols such as Network File System (NFS), Server Message Block (SMB), and Common Internet File System (CIFS), enabling shared access across different users and systems.

Security considerations for file-based storage include authentication and authorization mechanisms that integrate with Active Directory, IAM policies, or role-based access control (RBAC). Encryption must be enforced at rest and in transit to prevent unauthorized access. File access logs and event monitoring help detect suspicious activities or potential data breaches.

Block Storage

Block storage divides data into fixed-size blocks and distributes them across storage nodes. Each block is treated as an individual unit, making it highly efficient for performance-intensive applications such as databases and virtual machines. Unlike file-based storage, block storage does not rely on a directory structure but instead presents raw storage volumes that operating systems can format and use as needed.

Block storage is preferred for high-performance workloads due to its low latency and high throughput. It is commonly used for virtual machine disks, container storage, high-performance databases, and transactional workloads. Security considerations include logical separation of storage volumes to prevent cross-tenant access in multi-tenant environments, regular backups and snapshots to ensure data recovery, and full disk encryption (FDE) or volume-level encryption to protect against physical theft or unauthorized access.

Object-Based Storage

Object storage is a scalable and flexible cloud storage model that stores data as objects rather than files or blocks. Each object consists of the data, metadata, and a unique identifier, enabling efficient retrieval and distribution across cloud regions. Unlike traditional storage methods, object storage does not use a hierarchical file system but instead organizes data in a flat namespace.

Object storage is designed for massive scalability and is commonly used for backup and archival, big data analytics, machine learning datasets, and media content. Security considerations include fine-grained IAM policies and bucket-level permissions to prevent unauthorized access, versioning and immutability features to protect against accidental deletion or ransomware attacks, and server-side or client-side encryption with integration into key management services (KMS).

Databases

Cloud databases provide managed, scalable, and resilient data storage solutions tailored for structured data. These can be relational (SQL-based) or non-relational (NoSQL-based), depending on the data model and application requirements.

Relational Databases (SQL-Based Storage)

SQL databases store data in a structured format using tables, rows, and columns with enforced relationships between entities. Examples include Amazon RDS, Google Cloud SQL, and Microsoft Azure SQL Database. Security considerations for relational databases include authentication and authorization mechanisms managed through IAM roles, database users, or federated authentication. Data encryption is enforced using Transparent Data Encryption (TDE) and column-level encryption for sensitive fields. Regular point-in-time recovery (PITR) backups are maintained to recover from accidental deletions or failures.

Non-Relational Databases (NoSQL-Based Storage)

NoSQL databases provide a flexible schema for handling semi-structured and unstructured data. Common types include document stores such as MongoDB and CouchDB, key-value stores like DynamoDB and Redis, and graph databases like Neo4j and Amazon Neptune. Security considerations include configuring least privilege access to prevent excessive permissions, implementing parameterized queries and input validation to prevent injection attacks, and real-time query auditing and anomaly detection for suspicious database activities.

Content Delivery Networks (CDNs)

A Content Delivery Network (CDN) is a distributed network of edge servers that cache and deliver content to users based on their geographic location. CDNs improve performance, reliability, and security for cloud-based applications by reducing latency, distributing traffic, and enhancing load balancing.

CDNs reduce latency by caching static assets closer to end-users, thereby improving responsiveness. They distribute traffic across multiple servers to prevent congestion and ensure availability. CDNs are primarily used for website acceleration, video streaming, API caching, and software distribution.

Security considerations for CDNs include DDoS mitigation using integrated Web Application Firewalls (WAFs) and other protection mechanisms. Ensuring all content is served over HTTPS protects against man-in-the-middle attacks. Restricting access to authorized users, specific IP ranges, or implementing geofencing policies prevents unauthorized access or data leaks.

Case Study: Secure Cloud Storage Implementation for a Financial Institution

A global financial institution required a secure cloud storage architecture to store, process, and deliver sensitive financial data while maintaining regulatory compliance with GDPR, PCI-DSS, and ISO 27001.

The institution faced challenges related to data classification, security, and scalability. Financial records, transactional data, and analytical workloads needed to be categorized based on sensitivity. Compliance required end-to-end encryption and access control policies tailored to different data types. A fast and secure content delivery mechanism was necessary to ensure optimal performance for client dashboards and reports.

To address these challenges, the institution deployed encrypted EBS volumes for core financial databases, ensuring data security at the storage level. AWS S3 with lifecycle policies was implemented for long-term retention of archived regulatory data, aligning with compliance requirements. Amazon RDS was used for structured financial records, while DynamoDB handled real-time fraud detection analytics. A CDN was integrated into the architecture using CloudFront, optimizing client access while enforcing strict geo-blocking and Web Application Firewall (WAF) rules.

The implemented solution improved data security by enforcing multi-layered encryption, IAM policies, and automated access monitoring. It ensured regulatory compliance, successfully passing independent security audits for PCI-DSS and GDPR. Performance improvements were observed, with CDN caching reducing page load times by 40%, thereby enhancing user experience.

Maintaining Continuity

Understanding cloud storage architectures is crucial for designing secure, scalable, and compliant cloud environments. These storage models directly impact data encryption, access control, backup policies, and data sovereignty—concepts that will be further explored in upcoming discussions on key management, tokenization, and secure data sharing strategies. By effectively leveraging cloud storage architectures, organizations can enhance data security, optimize performance, and meet stringent compliance requirements, ensuring a robust foundation for their cloud security strategy.