iNURTURE Education Solutions
TOMORROW'S HERE

Subject : Cloud Security

Module Number : 05

Module Name : Security of Cloud Services

Version Code: CS1

Released Date : 5-Apr-2019

Security of Cloud Services

Aim

- To familiarise students about the Cloud Security Architecture and its components.

Security of Cloud Services

Objectives

The objectives of this module are to:

- Understand the shared responsibility model between Cloud provider and Customer.
- List the cloud Security Architecture.
- Know protect the data at rest and in transit.
- List the security for the applications hosted in the cloud.
- Define the Multifactor authentication and SSO.
- Understand the Legal challenges involved in Cloud.
- Know about compliance standards followed by Cloud providers to secure the data.

Security of Cloud Services

Outcomes

The outcomes of this module are to:

- Explain the shared responsibility model between Cloud provider and Customer.
- Describe the cloud Security Architecture.
- Outline the steps to protect the data at rest and in transit.
- Discuss the methods to provide the security for the applications hosted in the cloud.
- Design the Multifactor authentication and SSO.
- Illustrate the Legal challenges involved in Cloud.
- Summarise the compliance standards followed by Cloud providers to secure the data.

Security of Cloud Services

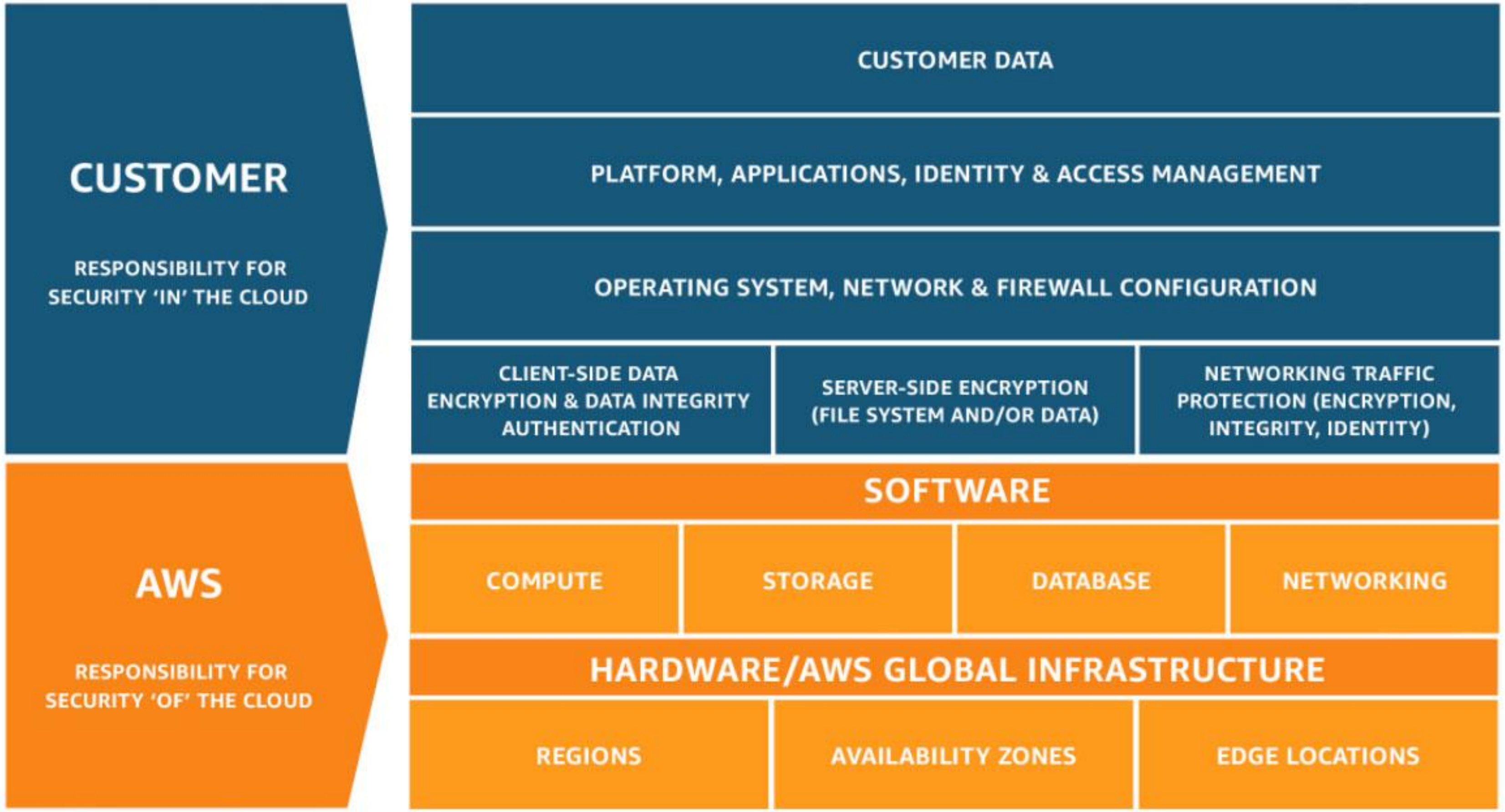
Content

1. Cloud Platform and Infrastructure security-physical environment
2. Security for Cloud networking
3. AWS Security for Computing
4. Security for Cloud Storage
5. Cloud Application Security
6. Cloud Application Architecture
7. Multi-factor authentication and SSO
8. Legal challenges involved in Cloud

Cloud Platform and Infrastructure security-physical environment

Security of Cloud Services

- Shared Responsibility Model
- Security and Compliance is a shared responsibility between AWS and the customer.



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Security of Cloud Services

AWS responsibility “Security of the Cloud”

- AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.
- This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

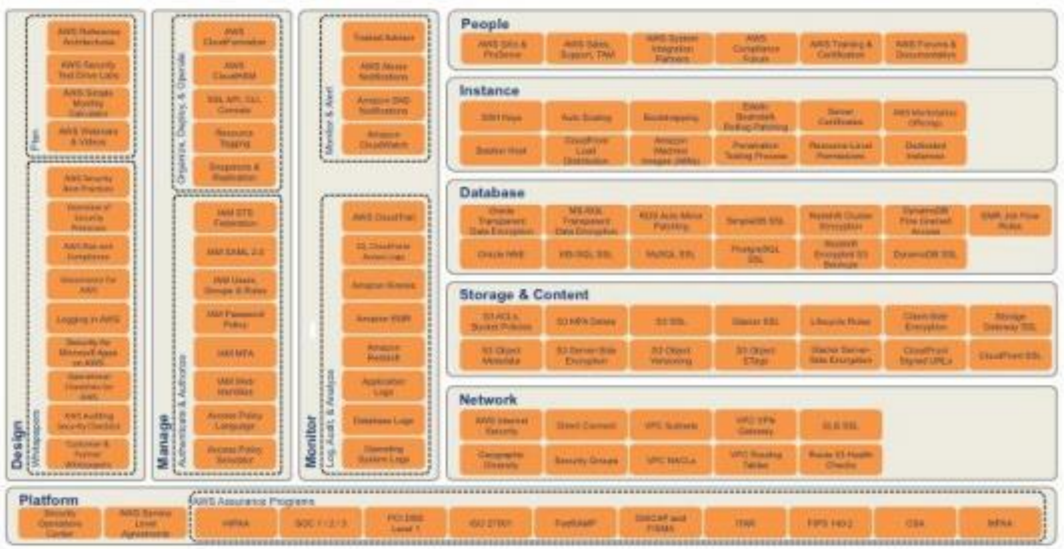
Customer responsibility “Security in the Cloud”

- Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.
- For example, services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 are categorised as Infrastructure as a Service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks.

Security of Cloud Services

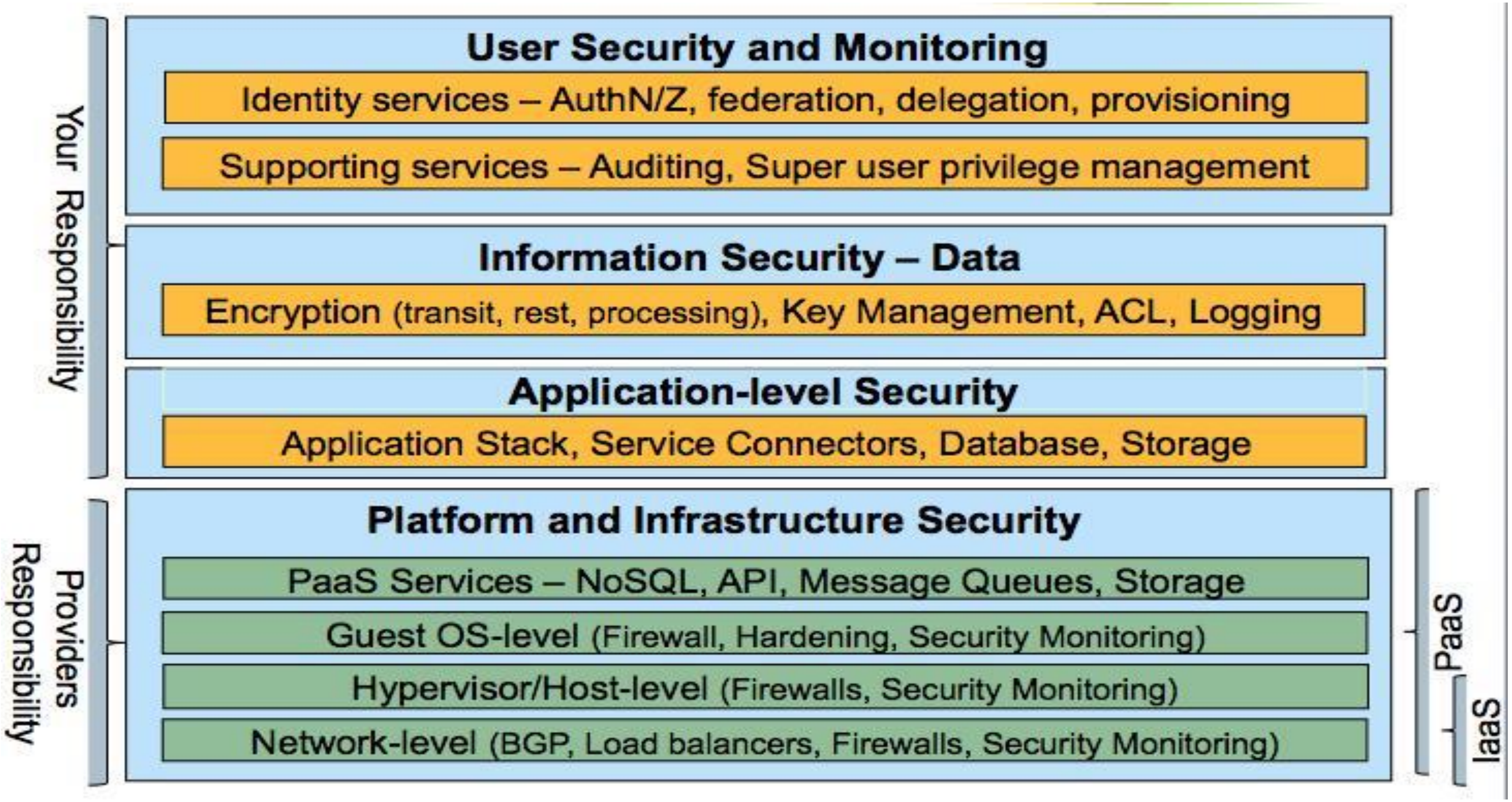
AWS Security Architecture

- Amazon’s shared security model clearly delineates the security responsibility that falls under the customer’s purview, but does not provide detailed guidance on building secure systems in accordance with FedRAMP guidelines.
- It is designed to provide an additional layer of guidance that can help organisations “right-size” the security approach so they can migrate faster while reducing compliance related security gaps in their system.



Security of Cloud Services

Cloud Security Architecture



User Security and Monitoring

Identity services – AuthN/Z, federation, delegation, provisioning

Supporting services – Auditing, Super user privilege management

Information Security – Data

Encryption (transit, rest, processing), Key Management, ACL, Logging

Application-level Security

Application Stack, Service Connectors, Database, Storage

Platform and Infrastructure Security

PaaS Services – NoSQL, API, Message Queues, Storage

Guest OS-level (Firewall, Hardening, Security Monitoring)

Hypervisor/Host-level (Firewalls, Security Monitoring)

Network-level (BGP, Load balancers, Firewalls, Security Monitoring)

Security for Cloud networking

Accessing Resources in Amazon VPC

Amazon VPC provides not only isolation from other customers in the private cloud, it also provides layer 3 (Network Layer IP routing) isolation from the Internet as well. The below table lists options for protecting your applications in Amazon VPC:

Concern	Description	Recommended Protection Approach
Internet-only	The Amazon VPC is not connected to any of your infrastructure on premises or elsewhere. You might or might not have additional infrastructure residing on premises, or elsewhere.	Encrypt application and administrative traffic using SSL/TLS, or build custom user VPN solutions. Carefully plan routing and server placement in public and private subnets. Use security groups and NACLs.
IPSec over the Internet	AWS provides industry-standard and resilient IPSec termination infrastructure for VPC. Customers can establish IPSec tunnels from their on-premises or other VPN infrastructure to Amazon VPC.	Establish a private IPSec connection using IKEv1 and IPSec using standard AWS VPN facilities (Amazon VPC VPN gateways, customer gateways, and VPN connections).
AWS Direct Connect without IPSec	With AWS Direct Connect, you can establish a connection to your Amazon VPC using private peering with AWS over dedicated links, without using the Internet.	Depending on your data protection requirements, you might not need additional protection over private peering.

Security of Cloud Services

Security Zoning and Network Segmentation

- Different security requirements mandate different security controls. It is a security best practice to segment infrastructure into zones that impose similar security controls.

On AWS, you can build network segments using the following access control methods:

- Using Amazon VPC to define an isolated network for each workload or organisational entity.
- Using security groups to manage access to instances that have similar functions and security requirements; security groups are stateful firewalls that enable firewall rules in both directions for every allowed and established TCP session or UDP communications channel.
- Using Network Access Control Lists (NACLs) that allow stateless management of IP traffic.
- Using host-based firewalls to control access to each instance.
- Creating a threat protection layer in traffic flow and enforcing all traffic to traverse the zone.
- Applying access control at other layers (e.g. applications and services).

Security of Cloud Services

Creating a security zone requires additional controls per network segment, and they often include:

- Shared Access Control–a central Identity and Access Management (IDAM) system.
- Shared Audit Logging–shared logging is required for event analysis and correlation, and tracking security events.
- Shared Data Classification
- Shared Management Infrastructure–various components, such as anti-virus/anti spam systems, patching systems, and performance monitoring systems.
- Shared Security (Confidentiality/Integrity) Requirements–often considered in conjunction with data classification.

Security of Cloud Services

AWS provides flexible security zoning options. Security engineers and architects can leverage the following AWS features to build isolated security zones/segments on AWS per Amazon VPC access control:

- Per subnet access control
- Per security group access control
- Per instance access control (host-based)
- Per Amazon VPC routing block
- Per resource policies (S3/SNS/SMS)
- Per zone IAM policies
- Per zone log management
- Per zone IAM users, administrative users
- Per zone log feed
- Per zone administrative channels (roles, interfaces, management consoles)
- Per zone AMIs
- Per zone data storage resources (Amazon S3 buckets or Glacier archives)
- Per zone user directories
- Per zone applications/application controls

Security of Cloud Services

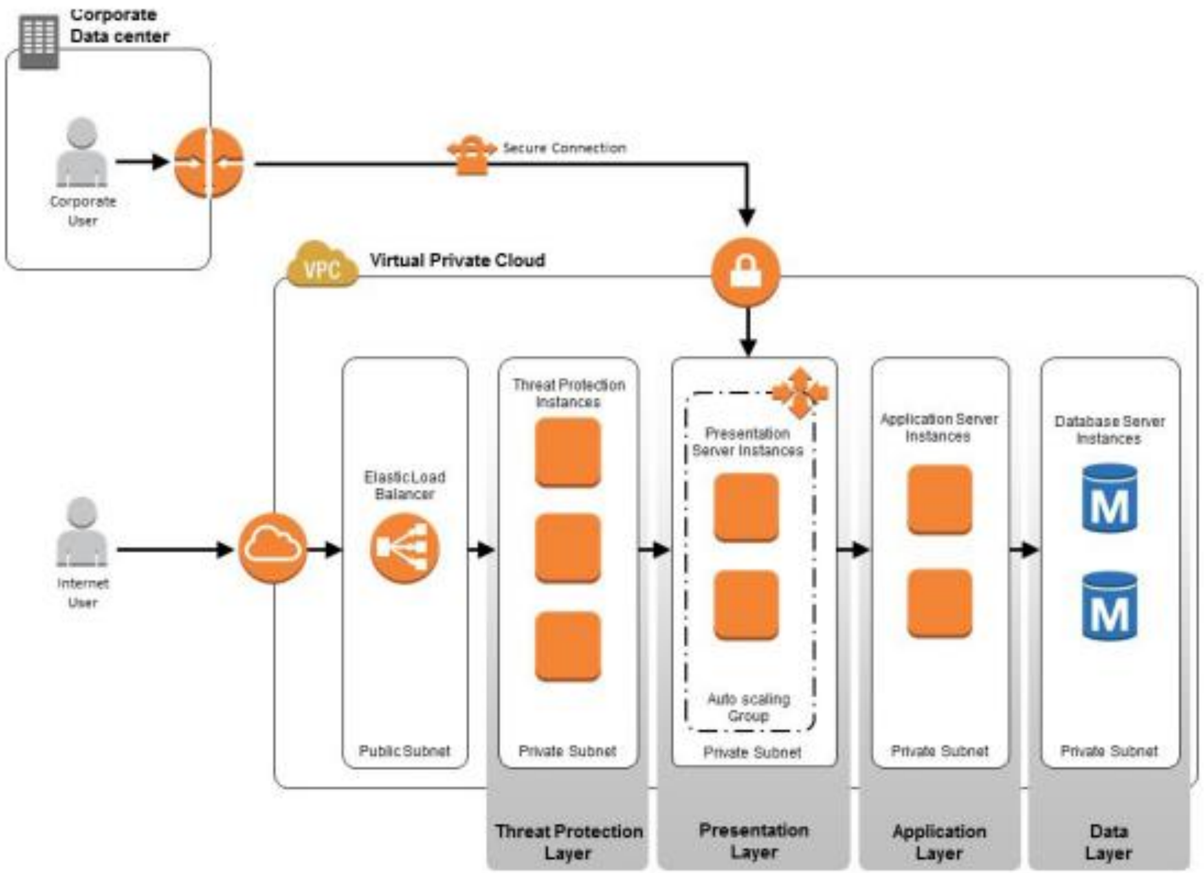
Controls for Periphery Systems

Common Control	Description
Separate administrative level access	Implement role separation and access controls to limit access to such services, often separate from access control required for application access, or access to other parts of the infrastructure.
Monitoring, alerting, audit trail	Log and monitor authorised and unauthorised activity.
Network layer access control	Restrict network access to only systems that require it. If possible, apply protocol enforcement for all network level access attempts (that is, enforce custom RFC standards for NTP and DNS).
Latest stable software with security patches	Ensure that the software is patched and not subject to any known vulnerabilities or other risks.
Continuous security testing (assessments)	Ensure that the infrastructure is tested regularly.
All other security controls processes in place	Make sure the periphery systems follow your information security management system (ISMS) best practices, in addition to service-specific custom security controls.

Security of Cloud Services

Layered Network Defence in the Cloud

- Many organisations consider layered security to be the best practice for protecting network infrastructure.
- In the cloud, you can use a combination of Amazon VPC, implicit firewall rules at the hypervisor-layer, alongside network access control lists, security groups, host-based firewalls, and IDS/IPS systems to create a layered solution for network security.



Security of Cloud Services

Threat protection technologies

Examples of inline threat protection technologies include the following:

- Third-party firewall devices installed on Amazon EC2 instances (also known as soft blades).
- Unified threat management (UTM) gateways
- Intrusion prevention systems
- Data loss management gateways
- Anomaly detection gateways
- Advanced persistent threat detection gateways

Security of Cloud Services

The following key features in the Amazon VPC infrastructure support deploying threat protection layer technologies:

- Support for Multiple Layers of Load Balancers:
  - When you use threat protection gateways to secure clusters of web servers, application servers, or other critical servers, scalability is a key issue.
- Support for Multiple IP Addresses:
  - When threat protection gateways protect a presentation layer that consists of several instances (for example web servers, email servers, application servers), these multiple instances must use one security gateway in a many-to-one relationship.
- Support for Multiple Elastic Network Interfaces (ENIs):
  - Threat protection gateways must be dual-homed and, in many cases, depending on the complexity of the network, must have multiple interfaces. Using the concept of ENIs, AWS supports multiple network interfaces on several different instance types, which makes it possible to deploy multi-zone security features.

Security of Cloud Services

Latency, complexity, and other architectural constraints sometimes rule out implementing an inline threat management layer, in which case you can choose one of the following alternatives.

- A distributed threat protection solution:
    - This approach installs threat protection agents on individual instances in the cloud. A central threat management server communicates with all host-based threat management agents for log collection, analysis, correlation, and active threat response purposes.
- An overlay network threat protection solution:
    - Build an overlay network on top of your Amazon VPC using technologies such as GRE tunnels, vtun interfaces, or by forwarding traffic on another ENI to a centralised network traffic analysis and intrusion detection system, which can provide active or passive threat response.

Security of Cloud Services

Techniques for Mitigation and Protection from DoS/DDoS Attacks

Technique	Description	Protection from DoS/DDoS Attacks
Firewalls: Security groups, network access control lists, and host based firewalls	Traditional firewall techniques limit the attack surface for potential attackers and deny traffic to and from the source of destination of attack.	• Manage the list of allowed destination servers and services (IP addresses & TCP/UDP ports) • Manage the list of allowed sources of traffic protocols • Explicitly deny access temporarily or permanently from specific IP addresses • Manage the list of allowed
Web Application Firewalls (WAF)	Web application firewalls provide deep packet inspection for web traffic.	• Platform- and application-specific attacks • Protocol sanity attacks • Unauthorized user access
Host-based or inline IDS/IPS systems	IDS/IPS systems can use statistical/behavioural or signature-based algorithms to detect and contain network attacks and Trojans.	• All types of attacks
Traffic shaping/rate limiting	Often DoS/DDoS attacks deplete network and system resources	• ICMP flooding • Application request flooding
Embryonic session limits	TCP SYN flooding attacks can take place in both simple and distributed form.	• TCP SYN flooding

Security of Cloud Services

Log File Considerations

Area	Consideration
Log collection	Note how log files are collected. Often operating system, application, or third party/middleware agents collect log file information.
Log transport	When log files are centralised, transfer them to the central location in a secure, reliable, and timely fashion.
Log storage	Centralise log files from multiple instances to facilitate retention policies, as well as analysis and correlation.
Log taxonomy	Present different categories of log files in a format suitable for analysis.
Log analysis/ correlation	Log files provide security intelligence after you analyse them and correlate events in them. You can analyse logs in real time, or at scheduled intervals.
Log protection/ security	Log files are sensitive. Protect them through network control, identity and access management, encryption, data integrity authentication, and tamper-proof time stamping.

Security of Cloud Services

Proxy Systems

When you use a privilege escalation gateway, you centralise all access to the system via a single (clustered) gateway. Instead of making direct calls to the AWS infrastructure, your operating systems or applications, all requests are performed by proxy systems that act as trusted intermediaries to the infrastructure. Often such systems are required to provide or do the following:

- Automated password management for privileged access:
  - Privileged access control systems can rotate passwords and credentials based on given policies automatically using built-in connectors for MicrosoftActive Directory, UNIX, LDAP, MYSQL, etc.
- Regularly run least privilege checks using AWS IAM userAccess Advisor and AWS IAM user Last Used AccessKeys
- User authentication on the front end and delegated access to services from AWS on the back end:
  - Typically a website that provides single sign on for all users. Users are assigned access privileges based on their authorisation profiles. A common approach is using token-based authentication for the website and acquiring click-through access to other systems allowed in the user’s profile.
- Tamper-proof audit trail storage of all critical activities.

Security of Cloud Services

Proxy Systems

Different sign-on credentials for shared accounts:

- Sometimes multiple users need to share the same password. A privilege escalation gateway can allow remote access without disclosing the shared account.
- Restrict leapfrogging or remote desktop hopping by allowing access only to target systems.
- Manage commands that can be used during sessions. For interactive sessions like SSH or appliance management, or AWS CLI, such solutions can enforce policies by limiting the range of available commands and actions.
- Provide audit trail for terminals and GUI-based sessions for compliance and security-related purposes.
- Log everything and alert based on given threshold for the policies.

AWS Security for Computing

Security of Cloud Services

Managing OS-level Access to Amazon EC2 Instances

- When you launch a new Amazon EC2 instance from a standard AMI, you can access that instance using secure remote system access protocols, such as Secure Shell (SSH), or Windows Remote Desktop Protocol (RDP).
- You must successfully authenticate at the operating-system level before you can access and configure the Amazon EC2 instance to your requirements.
- After you have authenticated and have remote access into the Amazon EC2 instance, you can set up the operating system authentication mechanisms you want, which might include X.509 certificate authentication, Microsoft Active Directory, or local operating system accounts.
- To enable authentication to the EC2 instance, AWS provides asymmetric key pairs, known as Amazon EC2 key pairs.
  - These are industry-standard RSA key pairs.
  - Each user can have multiple Amazon EC2 key pairs, and can launch new instances using different key pairs.

Best Practices to Secure EC2

The process for securing EC2 instances involves principles that are applicable to any OS, whether running in a virtual machine or on premises:

- Least Access: Restrict server access from both the network and on the instance, install only the required OS components and applications, and leverage host-based protection software.
- Least Privilege: Define the minimum set of privileges each server needs in order to perform its function.
- Configuration Management: Create a baseline server configuration and track each server as a configuration item. Assess each server against the current recorded baseline to identify and flag any deviations. Ensure each server is configured to generate and securely store appropriate log and audit data.
- Change Management: Create processes to control changes to server configuration baselines.
- Audit Logs: Audit access and all changes to EC2 instances to verify server integrity to ensure only authorised changes are made.

Security of Cloud Services

Bootstrapping

- Common bootstrapping applications include Puppet, Chef, Capistrano, Cloud-Init and Cfn-Init. You can also run custom bootstrapping Bash or Microsoft Windows PowerShell scripts without using third-party tools.

Here are a few bootstrap actions to consider:

- Security software updates install the latest patches, service packs, and critical updates beyond the patch level of the AMI.
- Initial application patches install application level updates, beyond the current application level build as captured in the AMI.
- Contextual data and configuration enables instances to apply configurations specific to the environment in which they are being launched–production, test, or DMZ/internal, for example.
- Register instances with remote security monitoring and management systems.

Security for Cloud Storage

Security of Cloud Services

Protecting Data at Rest

Concern	Recommended Protection Approach	Strategies
Accidental information disclosure	Designate data as confidential and limit the number of users who can access it.	Permissions File, partition, volume or application-level encryption
Data integrity compromise	To ensure that data integrity is not compromised through deliberate or accidental modification, use resource permissions to limit the scope of users who can modify the data.	Permissions, Data integrity checks (MAC/HMAC/Digital Signatures/Authenticated Encryption),Backup, Versioning (Amazon S3)
Accidental deletion	Using the correct permissions and the rule of the least privilege is the best protection against accidental or malicious deletion.	Permissions Backup, Versioning (Amazon S3), MFA Delete (Amazon S3)
System, infrastructure, hardware or software availability	In the case of a system failure or a natural disaster, restore your data from backup, or from replicas.	Backup Replication

Security of Cloud Services

Decommission Data and Media Securely

- When you ask AWS to delete data in the cloud, AWS does not decommission the underlying physical media; instead, the storage blocks are marked as unallocated.
- AWS uses secure mechanisms to reassign the blocks elsewhere.
- When you provision block storage, the hypervisor or Virtual Machine Manager (VMM) keeps track of which blocks your instance has written to.
- When an instance writes to a block of storage, the previous block is zeroed out, and then overwritten with your block of data.
- If your instance attempts to read from a block previously written to, your previously stored data is returned.
- If an instance attempts to read from a block it has not previously written to, the hypervisor zeros out the previous data on disk and returns a zero to the instance.
- When AWS determines that media has reached the end of its useful life, or it experiences a hardware fault, AWS follows the techniques detailed in Department of Defence (DoD) 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST SP 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.

Security of Cloud Services

Protect Data in Transit

Concern	Comments	Recommended Protection
Accidental information disclosure	Access to your confidential data should be limited. When data is traversing the public network, it should be protected from disclosure through encryption.	Encrypt data in transit using IPSec ESP and/or SSL/TLS.
Data integrity compromise	Whether or not data is confidential, you want to know that data integrity is not compromised through deliberate or accidental modification.	Authenticate data integrity using IPSec ESP/AH, and/or SSL/TLS.
Peer identity compromise/ identity spoofing/ man-in-the- middle	Encryption and data integrity authentication are important for protecting the communications channel.	Use IPSec with IKE with pre-shared keys or X.509 certificates to authenticate the remote end.

Cloud Application Security

Security of Cloud Services

Application Security Practices

General security - Best practices for your operating systems and applications:

- Always change vendor-supplied defaults before creating new AMIs or prior to deploying new applications, including but not limited to passwords, Simple Network Management Protocol (SNMP) community strings, and security configuration.
- Remove or disable unnecessary user accounts.
- Implement a single primary function per Amazon EC2 instance to keep functions that require different security levels from co-existing on the same server. For example, implement web servers, database servers and DNS on separate servers.
- Enable only necessary and secure services, protocols, daemons, etc., as required for the functioning of the system. Disable all non-essential services, because they increase the security risk exposure for the instance, as well as the entire system.
- Disable or remove all unnecessary functionality, such as scripts, drivers, features, subsystems, EBS volumes, and unnecessary web servers.

Cloud secure development lifecycle

Security of Cloud Services

Security Development Lifecycle (SDL)

What are the Microsoft SDL practices?

The Security Development Lifecycle (SDL) consists of a set of practices that support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in:

- Provide Training
- Define Security Requirements
- Define Metrics and Compliance Reporting
- Perform Threat Modelling
- Establish Design Requirements
- Define and Use Cryptography Standards
- Manage the Security Risk of using Third-Party Components
- Use Approved Tools
- Perform Static Analysis Security Testing (SAST)
- Perform Dynamic Analysis Security Testing (DAST)
- Perform Penetration Testing
- Establish a Standard Incident Response Process

Security of Cloud Services

Cloud Security

- Cloud security at AWS is the highest priority.
- As an AWS customer, you will benefit from a data centre and network architecture built to meet the requirements of the most security-sensitive organisations.
- An advantage of the AWS cloud is that it allows customers to scale and innovate, while maintaining a secure environment.
- Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment.

Security of Cloud Services

Benefits of AWS Security

- Keep Your Data Safe
  - The AWS infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure AWS data centres.
- Meet Compliance Requirements
  - AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
- Save Money
  - Cut costs by using AWS data centres. Maintain the highest standard of security without having to manage your own facility.
- Scale Quickly
  - Security scales with your AWS cloud usage. No matter the size of your business the AWS infrastructure is designed to keep data safe.

Security of Cloud Services

Cloud security capabilities

- Infrastructure Security
- DDoS Mitigation
- Data Encryption
- Inventory and Configuration
- Monitoring and Logging
- Identity and Access Control
- Penetration Testing

Cloud Application Architecture

Security of Cloud Services

Cloud Application Architecture

It will guide you through a selection of important considerations and resources to help determine the best approach for your cloud application:

- Choosing the right architecture style for your application based on the kind of solution you are building.
- Choosing the most appropriate compute and data store technologies.
- Incorporating the ten high-level design principles to ensure your application is scalable, resilient, and manageable.
- Utilising the five pillars of software quality to build a successful cloud application.
- Applying design patterns specific to the problem you are trying to solve.

Introduction

- The cloud is changing the way applications are designed. Instead of monoliths, applications are decomposed into smaller, decentralised services. These services communicate through APIs or by using asynchronous messaging or event.
- Applications scale horizontally, adding new instances as demand requires.

S No	Traditional on-premises	Modern cloud
1	Monolithic, centralized	Decomposed, de-centralized
2	Design for predictable scalability	Design for elastic scale
3	Relational database	Polyglot persistence (mix of storage technologies)
4	Strong consistency	Eventual consistency
5	Serial and synchronized processing	Parallel and asynchronous processing
6	Design to avoid failures (MTBF)	Design for failure (MTTR)
7	Occasional big updates	Frequent small updates
8	Manual management	Immutable infrastructure
9	Snowflake servers	

Security of Cloud Services

Architecture Styles

Architecture style	Dependency management	Domain type
N-tier	Horizontal tiers divided by subnet.	Traditional business domain. Frequency of updates is low.
Web-Queue-Worker	Front and backend jobs, decoupled by async messaging	Relatively simple domain with some resource intensive tasks.
Microservices	Vertically (functionally) decomposed services that call each other through APIs.	Complicated domain. Frequent updates.
CQRS	Read/write segregation. Schema and scale are optimized separately.	Collaborative domain where lots of users access the same data.
Event-driven architecture	Producer/consumer. Independent view per sub-system	IoT and real-time systems.
Big data	Divide a huge dataset into small chunks. Parallel processing on local datasets.	Batch and real-time data analysis. Predictive analysis using ML.
Big compute	Data allocation to thousands of cores	Compute intensive domains such as simulation

Multi-factor authentication and SSO

Security of Cloud Services

Multi Factor Authentication

- AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password.
- With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication response from their AWS MFA device (the second factor—what they have).
- Taken together, these multiple factors provide increased security for your AWS account settings and resources.
- You can enable MFA for your AWS account and for individual IAM users you have created under your account. MFA can be also be used to control access to AWS service APIs.
- After you've obtained a supported U2F security key, hardware device, or virtual MFA device, AWS does not charge any additional fees for using MFA.

Security of Cloud Services

	Virtual MFA Device	Universal 2nd Factor (U2F) Security Key	Hardware Key Fob MFA Device	Hardware Display Card MFA Device	SMS MFA Device (Preview)	Hardware Key Fob MFA Device for AWS GovCloud (US)
Device	Android, iPhone, Windows with Athenticator	Need to Purchase a device	Need to Purchase a device	Need to Purchase a device	Mobile	Need to Purchase a device
Physical Form Factor	Use your existing smartphone or tablet running any application that supports the open TOTP standard.	Durable, waterproof, and crush resistant hardware YubiKey security key provided by Yubico, a third-party provider.	Tamper-evident hardware key fob device provided by Gemalto, a third-party provider.	Tamper-evident hardware display card device provided by Gemalto, a third-party provider.	Any mobile device that can receive Short Message Service (SMS) messages.	Tamper-evident hardware key fob device provided by SurePassID, a third-party provider.
Price	Free	$40.00	$12.99	$19.99	SMS or data charges may apply	$15.95
Features	Support for multiple tokens on a single device.	Support for multiple root and IAM users using a single security key.	The same type of device used by many financial services and enterprise IT organizations.	Similar to key fob devices, but in a convenient form factor that fits in your wallet like a credit card	Familiar option with low setup costs.	A key fob device exclusively for use with AWS GovCloud (US)accounts.

Security of Cloud Services

Single sign-on (SSO)

- AWS Single Sign-On is a cloud-based single sign-on (SSO) service that makes it easy to centrally manage SSO access to all of your AWS accounts and cloud applications.
- Specifically, it helps you manage SSO access and user permissions across all your AWS accounts in AWS Organisations.
- AWS SSO also helps you manage access and permissions to commonly used third-party software as a service (SaaS) applications as well as custom applications that support Security Assertion Markup Language (SAML) 2.0.
- AWS SSO includes a user portal where your end-users can find and access all their assigned AWS accounts, cloud applications, and custom applications in one place.

Security of Cloud Services

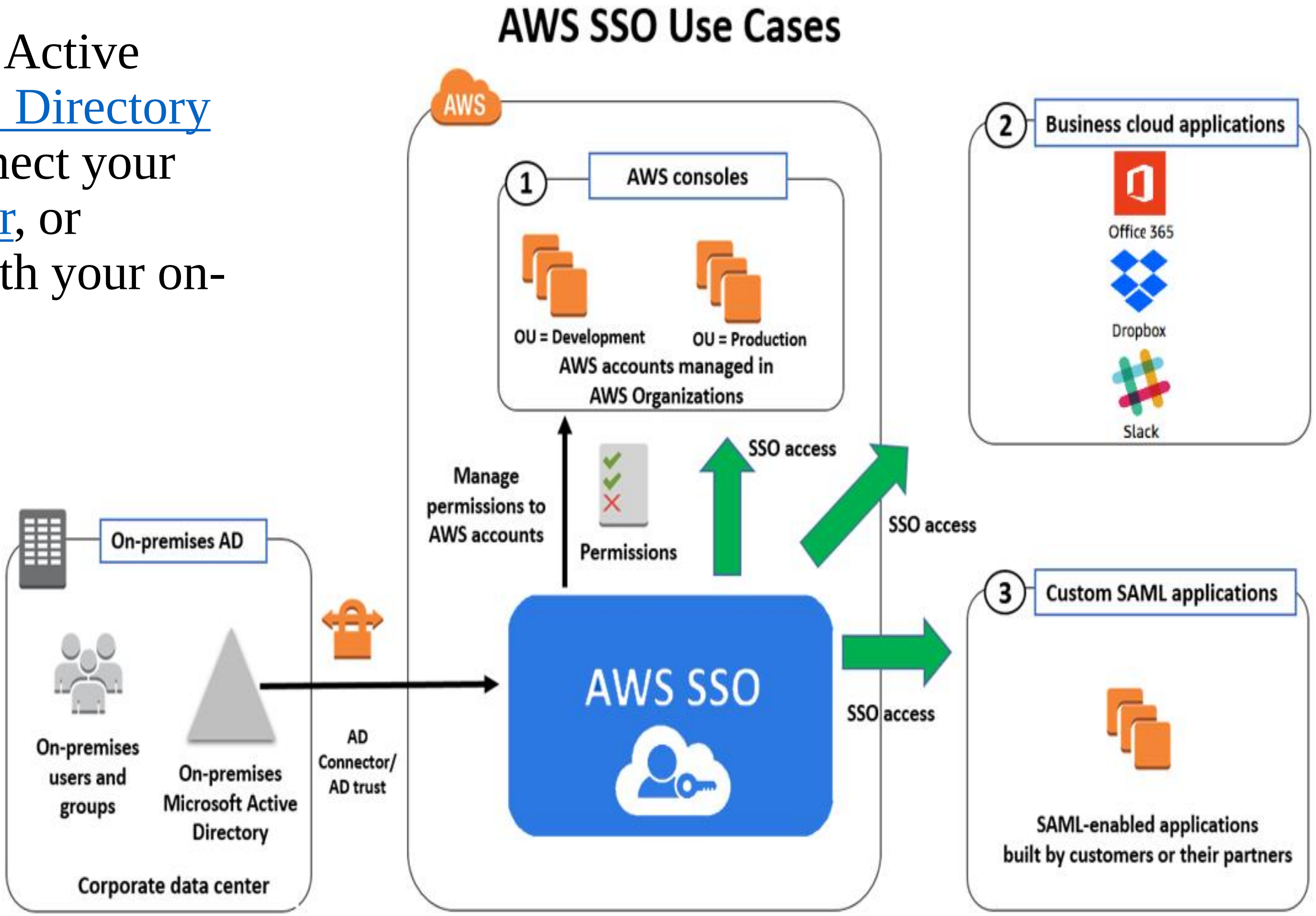
AWS SSO Features

AWS SSO provides the following features:

- **Integration with AWS Organisations.**
- **SSO access to your AWS accounts and cloud applications.**
- **Create and manage users and groups in AWS SSO.**
- **Leverage your existing corporate identities.**
- **Compatible with commonly used cloud applications.**
- **Easy to set up and monitor usage.**

AWS SSO Use Cases

- To get started, connect your corporate Active Directory to AWS SSO by using AWS Directory Service. You have two choices to connect your corporate directory: use AD Connector, or configure an Active Directory trust with your on-premises Active Directory.


AWS SSO Use Cases
AWS
1
AWS consoles
OU = Development
OU = Production
AWS accounts managed in AWS Organizations
Manage permissions to AWS accounts
Permissions
SSO access
SSO access
SSO access
2
Business cloud applications
Office 365
Dropbox
Slack
3
Custom SAML applications
SAML-enabled applications built by customers or their partners
On-premises AD
On-premises users and groups
On-premises Microsoft Active Directory
Corporate data center
AD Connector/ AD trust
AWS SSO

Legal challenges involved in Cloud

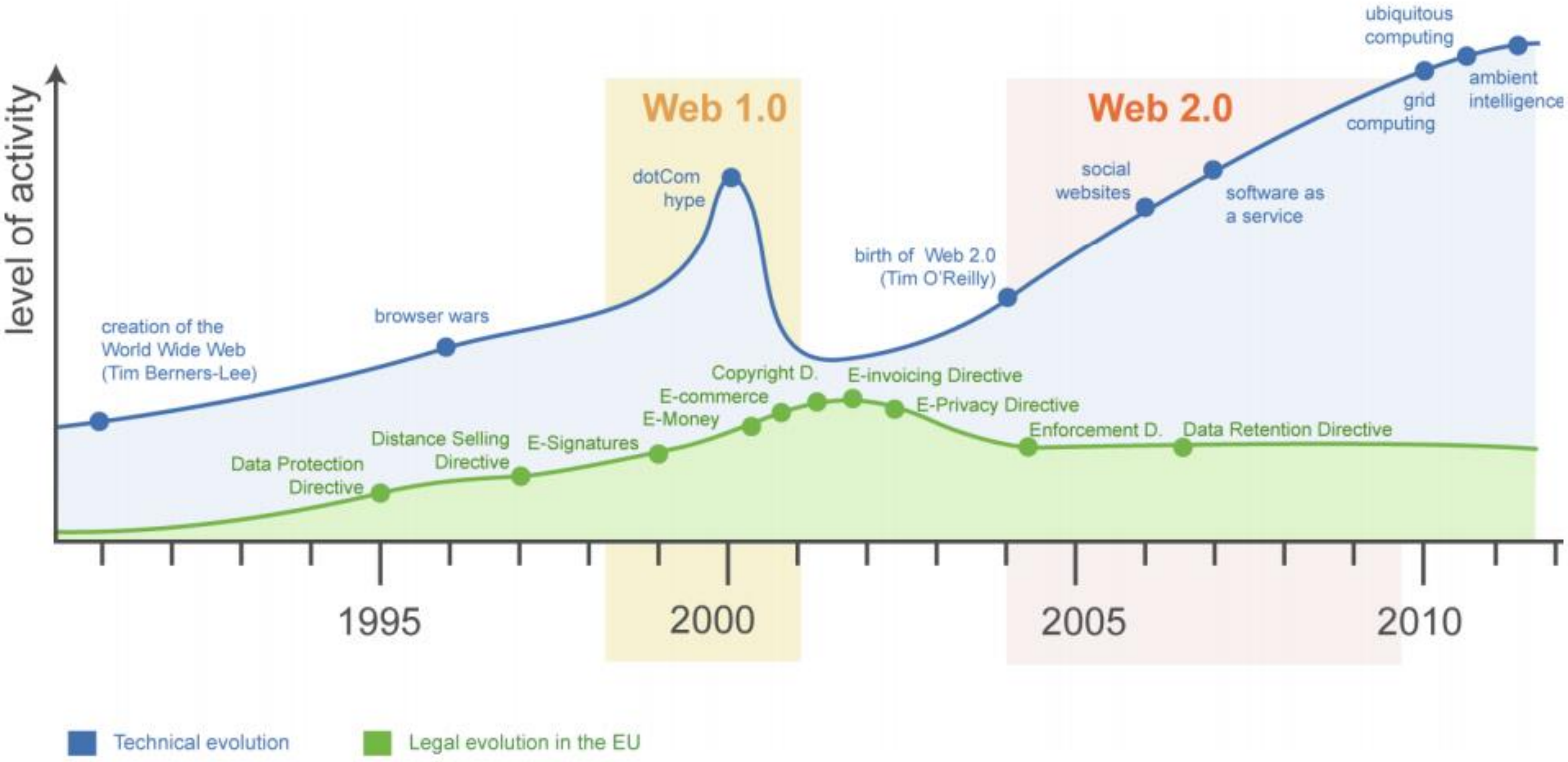
Security of Cloud Services

Cloud computing: legal challenges

- Liability.
- Applicable law.
- Data protection.
- Compliance.
- Copyright.
- Data portability.

Security of Cloud Services

EU legal framework



Security of Cloud Services

Personal data protection..

Privacy and data protection

Applicable laws

- EU Directive 95/46/EC
- National transpositions

  For Example, the Belgian Act of 8 December 1992 6
- Adopted in a pre-Internet area, when centralised and limited processing was the rule

EU rules are substantially more restrictive than rules from other countries (particularly the US)

- Cloud computing exposes the age, formality and complex application of the current laws
- Many legal issues are not yet resolved Reform of the current rules in the pipeline, but not for tomorrow

- Three examples of problems:
  - Who is a controller?
  - Which law is applicable?
  - Transfer outside of EU?

Security of Cloud Services

“Data controllers” and “data processors”

- The legislation makes a fundamental distinction between:
  - data controller: a party that defines the purpose and the means of the processing.
  - data processor: “dumb performer”.
- The distinction is crucial to know who is responsible.
- A data controller is liable towards the “data subjects”.
- The data controller must choose appropriate data processors and must seek adequate contractual protection from the “m”.

Security of Cloud Services

Data protection issues in the cloud

- Severe issues when applied in the cloud computing context:
  - Both customer and — particularly — the hosting provider define the “means” of the processing
  - The statutory assumption that the controller is entirely in control of the processing
  - Cloud computing is all about reducing the level of direct control, while EU legislation is all about keeping control of data
  - What about “sub-processors”?

Security of Cloud Services

Applicable data protection law

- An EU Member State’s national law will apply when:
  - establishment of EU-based controller located in its territory processes personal data.
  - controller outside the EU uses “equipment” within a territory.
- Applied to cloud computing:
  - using EU-based data centre = becoming subject to the very strict EU data protection rules?
  - most authorities interpret “equipment” in an extremely broad way (even browser cookies)

Security of Cloud Services

Transfer of data outside the EU

- Principle: no transfer of data to countries outside the EU that do not offer an “adequate level of protection”.
  - only Switzerland, Argentina and Canada
- Exceptions:
  - ask permission from every “data subject” involved.
  - if the transfer is necessary to execute a contract with the data subjects.
  - for the US: subscribing to “safe harbour list”.
  - “Binding Corporate Rules”.
  - European Commission’s model agreement.
- In practice:
- only use cloud provider with data centre within the EU.
  - **For Example,** Amazon EC2: choice of location (US East, US West or Ireland) or make sure that model agreement is concluded with the cloud provider.

Security of Cloud Services

Contracting issues

Small contract, big liability?

- Cloud computing services offer a low barrier to entry and easy scaling possibilities

  “click-wrap agreements” are legally enforceable!

- Many publicly available cloud computing contracts limit the liability of hosting provider to a level that is not in line 14 with the potential risk
- Cloud computing contracts resemble typical software licenses, although the potential risk is much higher
- Example,
  - We and our licensors shall not be responsible for any service interruptions, including, without limitation, power outages, system failures or other interruptions, including those that affect the receipt, processing, acceptance, completion or settlement of any payment services. (...)
  - Neither we nor any of our licensors shall be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages, including, but not limited to, damages for loss of profits, goodwill, use, data or other losses (...)

Security of Cloud Services

Other contractual issues

- Vendor lock-in
  - There is no general legal requirement for a vendor to provide you with data export facilities. Everything depends on your contractual agreement.
- Unilateral termination possibilities
  - Cloud provider often reserves the right to unilaterally terminate its service provision Involvement of multiple parties.
- no single point of contact.
- Auditing requirements:
  - Many contracts impose auditing possibilities that include physical inspection.
  - how can these auditing requirements be complied with when geographically decentralised cloud services are used?
- Applicable law and competent court
  - if outside own country, any litigation can become prohibitively expensive.
- What happens in case of bankruptcy of the provider?

Security of Cloud Services

Service Level Agreement

- Important in any service contract, crucial in a cloud computing context
- Points of attention:
  - How is the availability calculated by the provider?
    - Example, 10 outages of 6 minutes versus 1 outage of 1 hour.
  - Independent measurement of performance?
  - Are service credits the “sole remedy”?

Security of Cloud Services

Liability for illegal data

Liability of cloud provider for illegal content

- In many jurisdictions, cloud providers can be held liable for the illegal data they may be hosting.
- E-Commerce Directive (2000/31/EC) introduced special liability protection for hosting providers:
  - no liability for services that "consist of" the storage 20 of electronic information.
  - under the condition that the provider has no knowledge or awareness of illegal nature and removes or blocks illegal data when it does gain knowledge or become aware of illegal nature ("notice and takedown").
- Issues:
  - special protection is focused on storage and does not take into account processing activities.
  - significant amount of (particularly French) case law does not offer protection when services do not 21 consists exclusively of storage activities.
  - liability protection does not prevent so-called injunctions, which can be as costly and time-consuming.
  - no standard notice-and-takedown procedure.
  - Reform in the pipeline?

Security of Cloud Services

Compliance issues

- Compliance issues
- IaaS
  - Data retention obligations.
  - Tax related storage requirements.
  - Labour law related storage requirements etc.
- SaaS
  - electronic invoicing legislation.
  - ecommerce legislation.
  - electronic signature legislation etc.

Self Assessment Questions

Security of Cloud Services

Self Assessment Questions

1. In the shared responsibility model which component is the part of customers responsibility to secure the cloud.

   a. Operating System
   b. Compute
   c. Networking
   d. Edge Locations

Answer: C

Self Assessment Questions

2. Which term does not belongs to the AWS Ecosystem?

   a. Regions
   b. Availability Zones
   c. Networking
   d. Edge Locations

Answer: c

Self Assessment Questions

3. In the shared responsibility model which component is not the part of customers responsibility to secure the data.

   a. User Security and Monitoring

   b. Information Security-Data

   c. Application level Security

   d. Platform and Infrastructure Security

Answer: d

Security of Cloud Services

Self Assessment Questions

4. Security groups and NACL components are part of which AWS Service

   a. EC2

   b. VPC

   c. S3

   d. RDS

Answer: b

Self Assessment Questions

5. Which statement is not true for Security groups?

   a. We can apply on instance level

   b. We can block the ports and protocols

   c. We can only allow the port and protocols

   d. We can not apply on the subnet level

Answer: b

Self Assessment Questions

6. Which component is not part of Cloud Security Capability?

   a. Data Migration

   b. Inventory and Configuration

   c. Monitoring and Logging

   d. Identity and Access Control

Answer: a

Security of Cloud Services

Self Assessment Questions

7. Which Statement is not true for MFA?

   a. AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password.

   b. MFA can not be used to control access to AWS service APIs.

   c. You can enable MFA for your AWS account and for individual IAM users you have created under your account.

   d. After you have obtained a supported U2F security key, hardware device, or virtual MFA device, AWS does not charge any additional fees for using MFA.

Answer: b

Self Assessment Questions

8. Legal Challenges include__________.

   a. Data protection

   b. Compliance

   c. Copyright

   d. All of the above

Answer: D

Self Assessment Questions

9. What are the contractual issues in cloud ?

   a. Vendor lock-in

   b. Unilateral termination possibilities

   c. No single point of contact

   d. All of the above

Answer: d

Self Assessment Questions

10. Which of the below is not part of Compliance issue of IAAS?

a. Data retention obligations

b. Tax related storage requirements

c. Labour law related storage requirements

d. ecommerce legislation

Answer: d

Security of Cloud Services

Summary:

- The shared responsibility model between Cloud provider and Customer decides who has to take the responsibility to secure the services.
- Cloud Security Architecture gives the customer and providers responsibility for the different cloud services .
- Securing the data at rest and in transit which use different security layers to secure the data
- Security for the applications hosted in the cloud can be configured by deciding the level of access assigned for different users.
- Implementing Multifactor authentication and SSO provides the more than one authentication methods to access the resources.
- Legal challenges involved in Cloud are Liability, Applicable law, Data protection, Compliance, Copyright, Data portability.
- List of compliance standards followed by Cloud providers gives the detailed information about the Cloud providers how well they secure the data.

Security of Cloud Services

Assignment

1. Draw and explain Shared responsibility model for Cloud
2. List and explain the AWS networking Services
3. What is VPN? Explain the protocols used to secure the connection
4. What are the security features available for S3 service in AWS
5. Write a note on Cloud Application Security
6. Explain Cloud Application Architecture
7. Implement the Multi-factor authentication for your AWS Account
8. List and explain the compliance standards followed by AWS, Azure and Google Cloud Platform.

Security of Cloud Services

Document Links

Topics	URL	Notes
Cloud Application Architecture	http://www.cloudcomputingpatterns.org/cloud_application_architectures/	This link explains the cloud application architecture
Cloud Application Security	https://techbeacon.com/cloud-application-security-how-not-fail/	This link explains how to implement cloud application security
Data Protection plan	https://cloud.google.com/security/gdpr/	This link explains how to protect data in cloud
Cloud computing legal issues	https://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf	This link explains the Cloud computing legal issues

Security of Cloud Services

Video Links

Topics	URL	Notes
Categories of cloud security services	https://www.youtube.com/watch?v=L-cC-JjYos0	This video explains cloud security services
Cloud Application Architecture	https://channel9.msdn.com/Blogs/bobfamiliar/Cloud-Application-Architecture-Patterns-by-David-Platt	This video explains Cloud Application Architecture
Cloud application security	https://www.youtube.com/watch?v=DyUmFWfJQvU	Introducing Microsoft Cloud App Security
Multi-factor authentication	https://www.youtube.com/watch?v=nDmoMDSfJHc	Setting up an IAM user with MFA in AWS
Cloud security and data protection	https://www.youtube.com/watch?v=29dJTTOzvjU	Google Cloud: Data Protection and Regulatory Compliance
Cloud security compliance	https://www.youtube.com/watch?v=Rc55aYODnMI	AWS reinvent 2017: Compliance and Top Security Threats in the Cloud

Security of Cloud Services

E-Book Links

Topics	URL	Page Number
Cloud Security and Privacy	http://www.di.fc.ul.pt/~nuno/PAPERS/security3.pdf	All pages