CS 4037
Introduction to Cloud Computing
Lecture 24

Danyal Farhat

FAST School of Computing

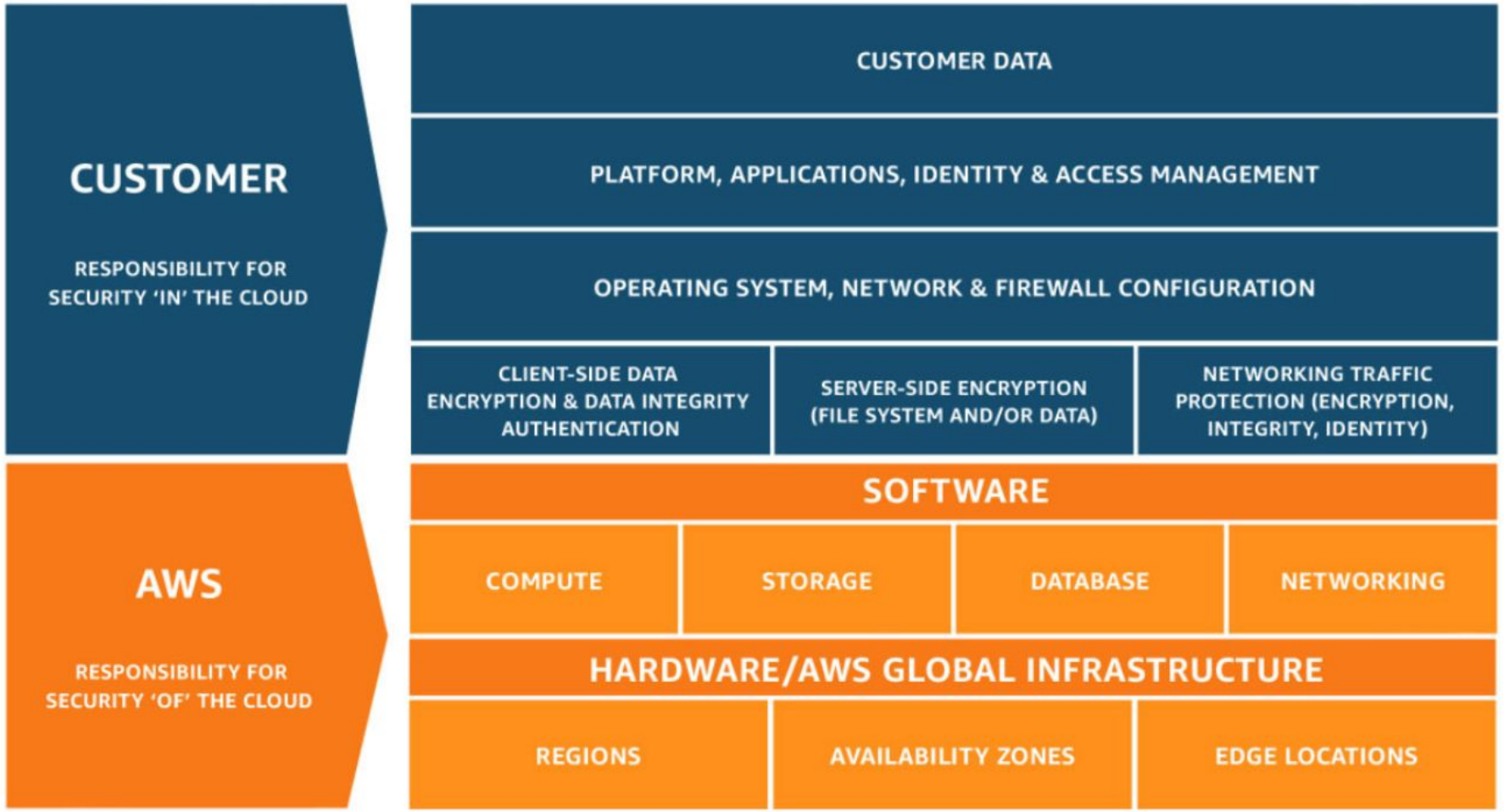
NUCES Lahore

AWS Security

Lecture's Agenda

- **Shared Responsibility Model**
- Identity and Access Management
- Securing a New AWS account
- Securing Data on Amazon Web Services
- AWS Security Services

Shared Responsibility Model

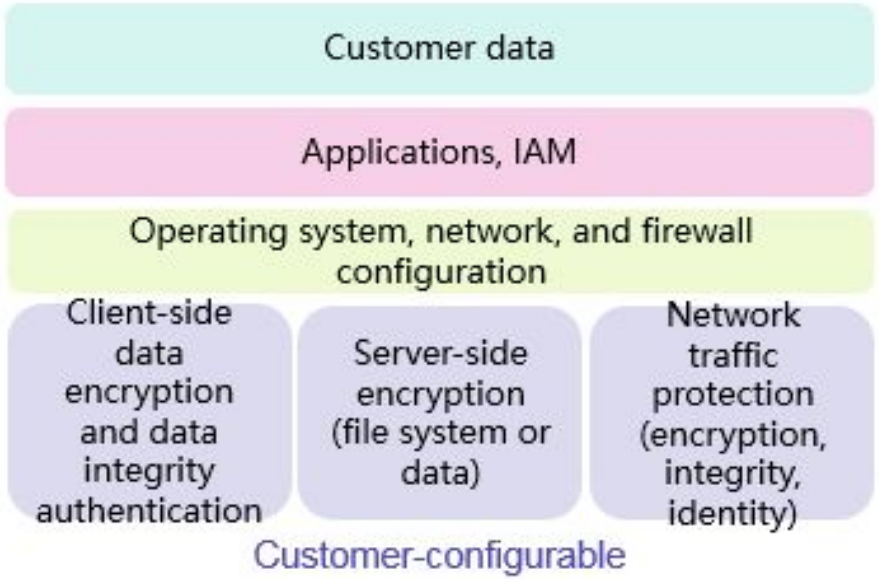


AWS Responsibility: Security of the cloud

- Physical security of data centers
  - Controlled, need-based access
- HW and SW infrastructure
  - Host operating system installation, access logging and patch update
  - Storage nodes addition
- Network infrastructure
  - Routers, switches, load balancers, firewalls, and cabling
- Virtualization infrastructure
  - Instance isolation
- Redundant infrastructure and Intrusion detection

Customer Responsibility: Security in the cloud

- **Account** management
  - Login and permission settings for each user
- **Network** configurations
  - Virtual Private Cloud settings
- EC2 instance **operating system**
  - Including patching, maintenance
- **Security group** configuration
  - OS / Host-based firewall settings
- **Applications** inside EC2
  - Passwords, role-based access etc.

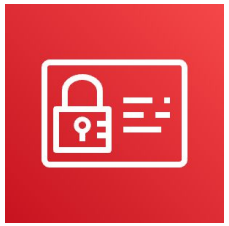


Lecture's Agenda

- Shared Responsibility Model
- **Identity and Access Management**
- Securing a New AWS account
- Securing Data on Amazon Web Services
- AWS Security Services

Identity and Access Management (IAM)

- Use IAM to manage access to AWS resources
  - A resource is an entity in an AWS account that you can work with
    - ✔ Example: EC2 instance, S3 bucket, DynamoDB database
  - Control who can terminate EC2 instances
- Define fine-grained access rights
  - Who can access the resource
  - Which resources can be accessed and what can the user do to the resource
  - How resources can be accessed (Mgt. Console / CLI / SDK)
- Provides authentication and authorization
  - Authentication: User's username and password.
  - Authorization: Access rights of user.
- IAM is a no-cost AWS account feature



AWS Identity and Access Management (IAM)

IAM Essential Components

IAM User

- "A person or application that can authenticate with an AWS account."

IAM Group

- "A collection of IAM users that are granted identical authorization."
  - Example: Departments of an organization

IAM Essential Components (Cont.)

IAM Policy

- "The document that defines which resources can be accessed and the level of access to each resource."

IAM Role

- "Useful mechanism to grant a set of permissions for making AWS service requests."
  - Example: DB Administrator, Developer etc.

IAM Authentication

- **User Credentials** (username and password)
- **User Credentials with Multi-factor Authentication (MFA)**
  - Provides increased security
  - In addition to username and password, MFA requires a unique authentication code to access AWS services

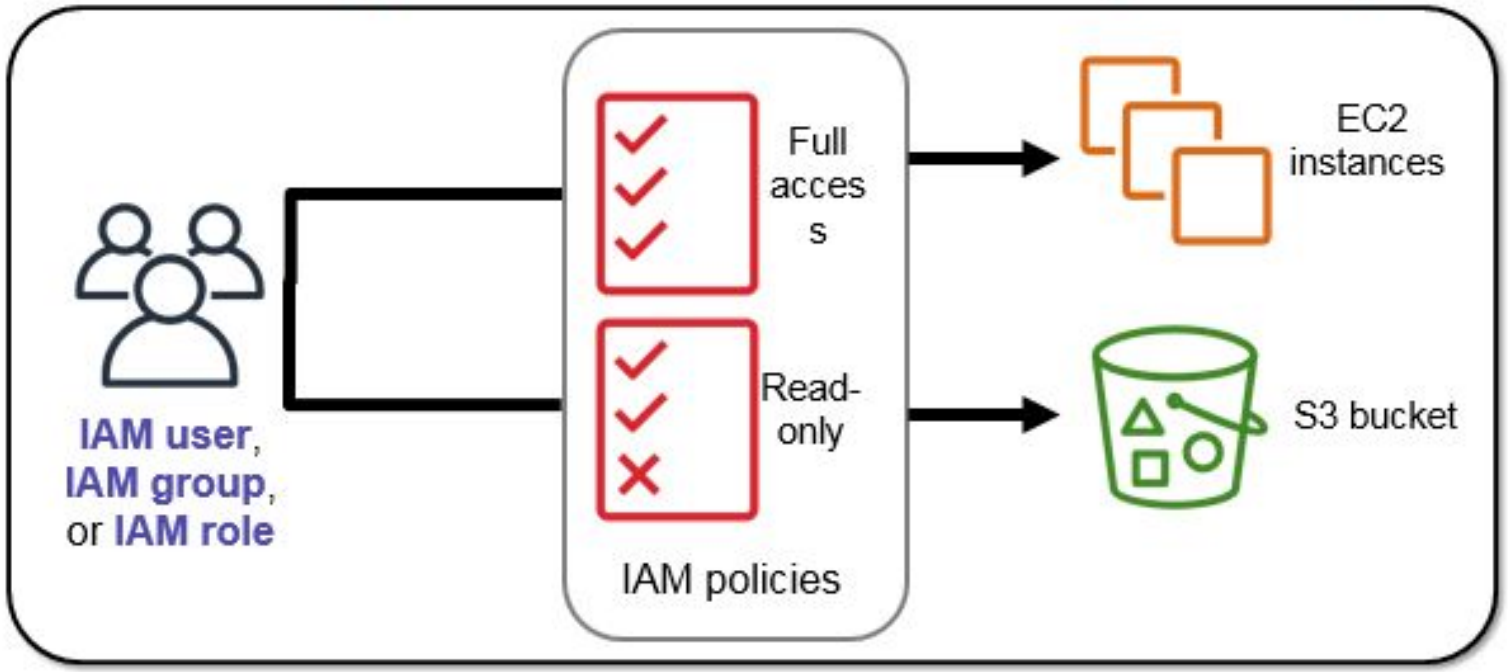
AWS Management Console

IAM Authorization

- Assign permissions by creating an IAM policy
- Permissions determine which resources and operations are allowed
  - All permissions are implicitly denied by default
  - If something is explicitly denied, it is never allowed
- Best practice: Follow the principle of least privilege
- The scope of IAM service configurations is global
  - Settings apply across all AWS Regions

IAM Authorization (Cont.)

After the user or application is connected to the AWS account, what are they allowed to do?



IAM Policy

- An IAM policy is a document that defines permissions
  - Enables fine-grained access control using JSON

Identity Based Policies

- Attach a policy to any IAM entity
  - An IAM user, an IAM group, or an IAM role
- Policies specify:
  - Actions that may be performed by the entity
  - Actions that may not be performed by the entity
- A single policy can be attached to multiple entities
- A single entity can have multiple policies attached to it

IAM Policy (Cont.)

Resource Based Policies

- Attached to a resource (such as an S3 bucket)
- Specifies who has access to the resource and what actions they can perform on it
- Resource based policies are inline only, not managed
  - Inline means policies are defined on the resource itself, instead of creating a separate IAM policy document that customer attach

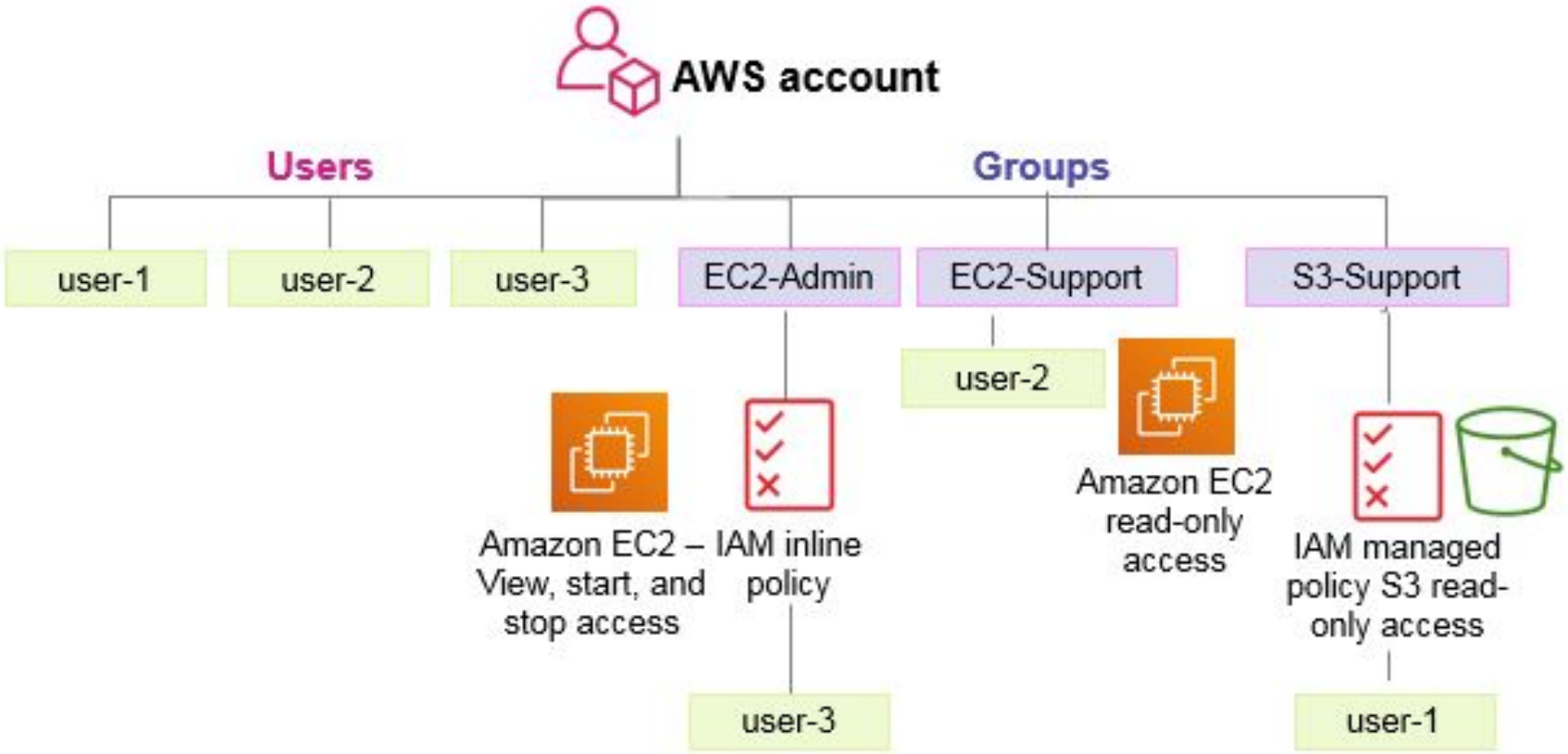
Lab 1: Introduction to IAM

Lab 1 Tasks:

- Task 1: Explore the Users and Groups
- Task 2: Add Users to Groups
- Task 3: Sign-In and Test Users

Lab 1: Introduction to IAM

Final Product:



Lecture's Agenda

- Shared Responsibility Model
- Identity and Access Management
- **Securing a New AWS Account**
- Securing Data on Amazon Web Services
- AWS Security Services

Step 1: Stop Using the Account Root User

- Stop using the account root user as soon as possible
  - The account root user has unrestricted access to customer's all resources
- To stop using the account root user:
  - While logged in as the account root user, create an new IAM user
    - ✔ Save the IAM access keys if needed
  - Create an IAM group, give it full administrator permissions, and add the IAM user to the group
  - Disable and remove your account root user access keys, if they exist
  - Enable a password policy for users
  - Sign in with your new IAM user credentials
  - Store your account root user credentials in a secure place

Step 2: Enable MFA

- Enable multi-factor authentication (MFA)
  - Require MFA for your account root user and for all IAM users
  - You can also use MFA to control access to AWS service APIs
- Options for retrieving the MFA token
  - Virtual MFA-compliant applications
    - ✔ Google Authenticator
    - ✔ Authy Authenticator (Windows phone app)
  - Universal Second Factor (U2F) security key devices
    - ✔ YubiKey
  - Hardware MFA options
    - ✔ Key fob or display card offered by Gemalto

Step 3: Use AWS CloudTrail

- **Use AWS CloudTrail**
  - CloudTrail tracks user activity on the account
  - Logs all API requests to resources and supported services
    - ✔ All actions performed on the cloud are being done at the backend using API calls
  - Enables operational auditing on the account

- **Basic CloudTrail events history is enabled by default**
  - User does not pay for basic CloudTrail events history
  - It contains all management event data on latest 90 days of account activity

Step 4: Enable a Billing Report

- **Enable a billing report**
  - Billing reports provide information about use of resources and estimated costs for that use
  - Example: AWS Cost and Usage Report tracks AWS usage and provides estimated charges associated with AWS account
    - ✔ Either by the hour or by the day

- **AWS delivers reports to a S3 bucket that customer specify**
  - Report is updated at least once per day
  - Relation with securing a new AWS account

Lecture's Agenda

- Shared Responsibility Model
- Identity and Access Management
- Securing a New AWS Account
- **Securing Data on Amazon Web Services**
- AWS Security Services

Encryption of Data at Rest

- Encryption encodes data with a secret key, which makes it unreadable
  - Only those who have the secret key can decode the data
  - AWS KMS can manage your secret keys
- AWS supports encryption of data at rest
  - Data at rest means data stored physically (on disk or on tape)
- Customer can encrypt data stored in any service that is supported by AWS KMS, including
  - Simple Storage Service
  - Elastic Block Store
  - Elastic File Service
  - Relational Database Service

Encryption of Data in Transit

- AWS services support encryption of data in transit using TLS
  - Data in transit means data moving across a network
  - Transport Layer Security (TLS – formerly SSL) is an open-standard protocol

- AWS Certificate Manager provides a way to deploy, manage, and renew TLS or SSL certificates

- HTTPS creates a secure tunnel
  - Uses TLS or SSL for the bidirectional exchange of data

Lecture's Agenda

- Shared Responsibility Model
- Identity and Access Management
- Securing a New AWS Account
- Securing Data on Amazon Web Services
- **AWS Security Services**

IAM and Security Services

AWS Key Management Service (AWS KMS):

- Enables to create and manage encryption keys
- Integrates with AWS CloudTrail to log all key usage

IAM and Security Services (Cont.)

Amazon Cognito:

- Adds user sign-up, sign-in, and access control to web and mobile applications
- Supports sign-in with social identity providers
  - Facebook, Google, and Amazon
- Supports sign-in with enterprise identity providers
  - Microsoft Active Directory via SAML 2.0
    - ✔ SAML is an open standard for exchanging identity and security information with applications and service providers

AWS IAM and Security Services (Cont.)

AWS Artifact:

- Provide access to security and compliance reports
  - AWS related ISO certifications
  - Payment Card Industry (PCI) report
  - Service Organization Control (SOC) report

- Customers use these reports for auditing and compliance standards imposed by Government regulatory authorities
  - Example: As per State Bank of Pakistan's policy, all banks in the country must be PCI compliant

AWS IAM and Security Services (Cont.)

AWS Shield:

- Managed DDoS protection service
  - Safeguards applications running on AWS
- Provides always-on detection
- Provides automatic inline mitigations
- Used to minimize application downtime and latency

AWS IAM and Security Services (Cont.)

Amazon Inspector:

- Define standards and best practices for applications
- Validate adherence to the defined standards

Amazon GuardDuty:

- Provides intelligent threat detection and continuous monitoring to protect AWS accounts and workloads

Additional Resources

- AWS Cloud Security
  - https://aws.amazon.com/security/
- AWS Security Blogs
  - https://aws.amazon.com/blogs/security/
- Vulnerability and Penetration Testing
  - https://aws.amazon.com/security/penetration-testing/
- AWS documentation - IAM Best Practices:
  - https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Questions?