**Lecture Notes for AWS Developer**

**Module-7**

**AWS COGNITO**

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.



**Secure and scalable user directory**

Amazon Cognito User Pools provide a secure user directory that scales to hundreds of millions of users. As a fully managed service, User Pools are easy to set up without any worries about standing up server infrastructure.



**Social and enterprise identity federation**

With Amazon Cognito, your users can sign in through social identity providers such as Apple, Google, Facebook, and Amazon, and through enterprise identity providers such as SAML and OpenID Connect.



**Standards-based authentication**

Amazon Cognito User Pools is a standards-based Identity Provider and supports identity and access management standards, such as Oauth 2.0, SAML 2.0, and OpenID Connect.



**Security for your apps and users**

Amazon Cognito supports multi-factor authentication and encryption of data-at-rest and in-transit. Amazon Cognito is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.



**Access control for AWS resources**

Amazon Cognito provides solutions to control access to AWS resources from your app. You can define roles and map users to different roles so your app can access only the resources that are authorized for each user. Alternatively, you can use attributes from identity providers in AWS Identity and Access Management permission policies, so you can control access to resources to users who meet specific attribute conditions.



**Easy integration with your app**

With a built-in UI and easy configuration for federating identity providers, you can integrate Amazon Cognito to add user sign-in, sign-up, and access control to your app in minutes. You can customize the UI to put your company branding front and center for all user interactions.

Amazon Cognito Federated Identities is a web service that delivers scoped temporary credentials to mobile devices and other untrusted environments. It uniquely identifies a device and supplies the user with a consistent identity over the lifetime of an application.

Using Amazon Cognito Federated Identities, you can enable authentication with one or more third-party identity providers (Facebook, Google, or Login with Amazon) or an Amazon Cognito user pool, and you can also choose to support unauthenticated access from your app. Cognito delivers a unique identifier for each user and acts as an OpenID token provider trusted by AWS Security Token Service (STS) to access temporary, limited-privilege AWS credentials.

**AWS Cloud Security**

**Raise your security posture with AWS infrastructure and services.**

Using AWS, you will gain the control and confidence you need to securely run your business with the most flexible and secure cloud computing environment available today. As an AWS customer, you will benefit from AWS data centers and a network architected to protect your information, identities, applications, and devices. With AWS, you can improve your ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality with our comprehensive services and features.

AWS allows you to automate manual security tasks so you can shift your focus to scaling and innovating your business. Plus, you pay only for the services that you use. All customers benefit from AWS being the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads.

**Benefits**

**Scale Securely with Superior Visibility and Control**

With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information ensures that the right resources have the right access at all times, wherever your information is stored.

**Automate and Reduce Risk with Deeply Integrated Services**

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways, making it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely.

**Build with the Highest Standards for Privacy and Data Security**

AWS is vigilant about your privacy. With AWS you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention. All data flowing across the AWS global network that interconnects our datacenters and regions is automatically encrypted at the physical layer before it leaves our secured facilities. Additional encryption layers exist as well; for example, all VPC cross-region peering traffic, and customer or service-to-service TLS connections.

**Largest Ecosystem of Security Partners and Solutions**

Extend the benefits of AWS by using security technology and consulting services from familiar solution providers you already know and trust. We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day to day management.

**Inherit the Most Comprehensive Security and Compliance Controls**

To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond.

**Strategic Security**

AWS is designed to help you build secure, high-performing, resilient, and efficient infrastructure for your applications. World-class security experts who monitor our infrastructure also build and maintain our broad selection of innovative security services, which can help you simplify meeting your own security and regulatory requirements. Our security services and solutions are focused on delivering the following key strategic benefits critical to helping you implement your organization’s optimal security posture:



**AWS Key Management Service (KMS)**

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

**Benefits**

**Fully managed**

You control access to your encrypted data by defining permissions to use keys while AWS KMS enforces your permissions and handles the durability and physical security of your keys.

**Centralized key management**

AWS KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications. You can easily create, import, rotate, delete, and manage permissions on keys from the AWS Management Console or by using the AWS SDK or CLI.

**Manage encryption for AWS services**

AWS KMS is integrated with AWS services to simplify using your keys to encrypt data across your AWS workloads. You choose the level of access control that you need, including the ability to share encrypted resources between accounts and services. KMS logs all use of keys to AWS CloudTrail to give you an independent view of who accessed your encrypted data, including AWS services using them on your behalf.

**Encrypt data in your applications**

AWS KMS is integrated with the AWS Encryption SDK to enable you to used KMS-protected data encryption keys to encrypt locally within your applications. Using simple APIs you can also build encryption and key management into your own applications wherever they run.

**Digitally sign data**

AWS KMS enables you to perform digital signing operations using asymmetric key pairs to ensure the integrity of your data. Recipients of digitally signed data can verify the signatures whether they have an AWS account or not.

**Low cost**

There is no commitment and no upfront charges to use AWS KMS. You only pay US $1/month to store any key that you create. AWS managed keys that are created on your behalf by AWS services are free to store. You are charged per-request when you use or manage your keys beyond the free tier.

**Secure**

AWS KMS uses hardware security modules (HSMs) that have been validated under FIPS 140-2, or are in the process of being validated, to generate and protect keys. Your keys are only used inside these devices and can never leave them unencrypted. KMS keys are never shared outside the AWS region in which they were created.

**Compliance**

The security and quality controls in AWS KMS have been certified under multiple compliance schemes to simplify your own compliance obligations. AWS KMS provides the option to store your keys in single-tenant HSMs in AWS CloudHSM instances that you control.

**Built-in auditing**

AWS KMS is integrated with AWS CloudTrail to record all API requests, including key management actions and usage of your keys. Logging API requests helps you manage risk, meet compliance requirements and conduct forensic analysis.

**AWS Systems Manager Parameter Store**

Parameter Store, a capability of AWS Systems Manager, provides secure, hierarchical storage for configuration data management and secrets management. You can store data such as passwords, database strings, Amazon Machine Image (AMI) IDs, and license codes as parameter values. You can store values as plain text or encrypted data. You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter.

Parameter Store is also integrated with Secrets Manager. You can retrieve Secrets Manager secrets when using other AWS services that already support references to Parameter Store parameters.

**Parameter Store offers these benefits:**

* Use a secure, scalable, hosted secrets management service with no servers to manage.
* Improve your security posture by separating your data from your code.
* Store configuration data and encrypted strings in hierarchies and track versions.
* Control and audit access at granular levels.

**What are the features of Parameter Store?**

**Change notification**

You can configure change notifications and invoke automated actions for both parameters and parameter policies.

**Organize and control access**

You can tag your parameters individually to help you identify one or more parameters based on the tags you've assigned to them. For example, you can tag parameters for specific environments, departments, users, groups, or periods. You can also restrict access to parameters by creating an AWS Identity and Access Management (IAM) policy that specifies the tags that a user or group can access.

**Label versions**

You can associate an alias for versions of your parameter by creating labels. Labels can help you remember the purpose of a parameter version when there are multiple versions.

**Data validation**

You can create parameters that point to an Amazon Elastic Compute Cloud (Amazon EC2) instance and Parameter Store validates these parameters to make sure that it references expected resource type, that the resource exists, and that the customer has permission to use the resource. For example, you can create a parameter with Amazon Machine Image (AMI) ID as a value with aws:ec2:image data type, and Parameter Store performs an asynchronous validation operation to make sure that the parameter value meets the formatting requirements for an AMI ID, and that the specified AMI is available in your AWS account.

**Reference secrets**

Parameter Store is integrated with AWS Secrets Manager so that you can retrieve Secrets Manager secrets when using other AWS services that already support references to Parameter Store parameters.

**Accessible from other AWS services**

You can use Parameter Store parameters with other Systems Manager capabilities and AWS services to retrieve secrets and configuration data from a central store. Parameters work with Systems Manager capabilities such as Run Command, Automation, and State Manager, capabilities of AWS Systems Manager. You can also reference parameters in a number of other AWS services, including the following:

* Amazon Elastic Compute Cloud (Amazon EC2)
* Amazon Elastic Container Service (Amazon ECS)
* AWS Secrets Manager
* AWS Lambda
* AWS CloudFormation
* AWS CodeBuild
* AWS CodePipeline
* AWS CodeDeploy

**Integrate with other AWS services**

Configure integration with the following AWS services for encryption, notification, monitoring, and

auditing:

* AWS Key Management Service (AWS KMS)
* Amazon Simple Notification Service (Amazon SNS)
* Amazon CloudWatch
* Amazon EventBridge
* AWS CloudTrail