Amity School of Engineering and Technology

Course Level: UG

Course Title: Cloud Computing Practitioner

Course Code: CSE314

Module-5

Puneet Sharma (AUUP, Lucknow)

Cloud Security for Industry

- 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.

Cloud Security for Industry

- As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Security in the cloud is much like security in your on-premises data centers—only without the costs of maintaining facilities and hardware. In the cloud, you don’t have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and of out of your cloud resources.

- An advantage of the AWS Cloud is that it allows you to scale and innovate, while maintaining a secure environment and paying only for the services you use. This means that you can have the security you need at a lower cost than in an on-premises environment.

- As an AWS customer you inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers. Get the flexibility and agility you need in security controls.

Cloud Security for Industry

- The AWS Cloud enables a shared responsibility model. While AWS manages security of the cloud, you are responsible for security in the cloud. This means that you retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data center.

- AWS provides you with guidance and expertise through online resources, personnel, and partners. AWS provides you with advisories for current issues, plus you have the opportunity to work with AWS when you encounter security issues.

- You get access to hundreds of tools and features to help you to meet your security objectives. AWS provides security-specific tools and features across network security, configuration management, access control, and data encryption.

- Finally, AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. In the AWS environment, you can take advantage of automated tools for asset inventory and privileged access reporting.

Benefits of AWS Security

- Benefits of AWS Security

- Keep Your Data Safe: The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.

- 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 centers. 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 your data safe.

Benefits of AWS Security

- **AWS Cloud Compliance:** enables you to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS Cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs. This helps customers to establish and operate in an AWS security control environment.

- The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards. The following is a partial list of assurance programs with which AWS complies:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

AWS

- **Availability**

- AWS delivers the highest network availability of any cloud provider, with 7x fewer down time hours than the next largest cloud provider.* Each region is fully isolated and comprised of multiple AZ’s, which are fully isolated partitions of our infrastructure. To better isolate any issues and achieve high availability, you can partition applications across multiple AZ’s in the same region. In addition, AWS control planes and the AWS management console are distributed across regions, and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.

AWS

- **Performance**

- The AWS Global Infrastructure is built for performance. AWS Regions offer low latency, low packet loss, and high overall network quality. This is achieved with a fully redundant 100 GbE fiber network backbone, often providing many terabits of capacity between Regions. AWS Local Zones and AWS Wavelength, with our telco providers, provide performance for applications that require single-digit millisecond latencies by delivering AWS infrastructure and services closer to end-users and 5G connected devices. Whatever your application needs, you can quickly spin up resources as you need them, deploying hundreds or even thousands of servers in minutes.

AWS

- **Global Footprint**

- AWS has the largest global infrastructure footprint of any provider, and this footprint is constantly increasing at a significant rate. When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure that is closest to your primary target of users. You can run your workloads on the cloud that delivers the best support for the broadest set of applications, even those with the highest throughput and lowest latency requirements. And If your data lives off this planet, you can use AWS Ground Station, which provides satellite antennas in close proximity to AWS infrastructure Regions.

AWS

- **Scalability**

- The AWS Global Infrastructure enables companies to be extremely flexible and take advantage of the conceptually infinite scalability of the cloud. Customers used to over provision to ensure they had enough capacity to handle their business operations at the peak level of activity. Now, they can provision the amount of resources that they actually need, knowing they can instantly scale up or down along with the needs of their business, which also reduces cost and improves the customer’s ability to meet their user’s demands. Companies can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.

AWS

- **Flexibility**

- The AWS Global Infrastructure gives you the flexibility of choosing how and where you want to run your workloads, and when you do you are using the same network, control plane, API's, and AWS services. If you would like to run your applications globally you can choose from any of the AWS Regions and AZ's. If you need to run your applications with single-digit millisecond latencies to mobile devices and end-users you can choose AWS Local Zones or AWS Wavelength. Or if you would like to run your applications on-premises you can choose AWS Outposts.

AWS global infrastructure

- The AWS Global Infrastructure consists of multiple geographical locations which are called Regions. AWS Regions are divided up in Availability Zones which consist of one or more psychically separated data centers. These Regions and Availability Zones provide a way to build highly available, fault tolerant, and scalable infrastructures.

- All Availability Zones (AZs) are connected through low latency, high throughput, and highly redundant networking. AZs are physically separated by an unknown minimum distance to ensure availability of the network even in the event of catastrophic events like extreme weather. As of April 2020, AWS spans 70 Availability Zones within 22 Regions around the world.

AWS global infrastructure

- **Points of Presence**

- Another part of the AWS Global Infrastructure are Points of Presence (POP). The POPs are used for both AWS CloudFront to deliver content to end users at high speeds, and Lambda@Edge to run Lambda functions with the lowest possible latency. As of April 2020, there are 216 Points of Presence in 84 cities across 42 countries.

- **Designing for failure**

- Using the AWS Global Infrastructure, it's easy to design fault tolerant infrastructure. We can achieve this by having multiple EC2 instances in different Availability Zones or even Regions. In the unlikely event of an Availability Zone or entire Region failing, your applications are not impacted. Other services like Relational Database Service (RDS) can achieve fault tolerance because they have Multi-AZ deployment models built-in. Of course, there is always extra cost involved when having your servers and data stored in multiple AZs.

AWS global infrastructure

- Using Regions, you can also scale out your applications to make sure they are as close to your end-users as possible. If, for example, you have customers in both Europe and the United States you can easily replicate your infrastructure by launching it in a different region.

- **VPC Peering**

- VPC networks in different regions can be tied together using VPC Peering. Instances in either VPC can communicate with each other as if they are in the same private network. You can create VPC peering connections between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS region. It is neither a gateway nor a VPN connection and doesn't need physical hardware, mitigating the need for maintenance.

AWS global infrastructure

- **Risk and Compliance Overview**

- AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS' part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use.

- The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:
- •Obtaining industry certifications and independent third-party attestations described in this document
- •Publishing information about the AWS security and control practices in whitepapers and web site.
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

Shared Responsibility Environment

- Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

- The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

- It is possible for customers to enhance security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

AWS Organizations

- AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can programmatically create new AWS accounts and allocate resources, group accounts to organize your workflows, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts.

- In addition, AWS Organizations is integrated with other AWS services so you can define central configurations, security mechanisms, audit requirements, and resource sharing across accounts in your organization. AWS Organizations is available to all AWS customers at no additional charge.

AWS Support Plans

- At AWS, we want you to be successful. Our Support plans are designed to give you the right mix of tools and access to expertise so that you can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.

- Basic Support is included for all AWS customers and includes:

- Customer Service and Communities - 24x7 access to customer service, documentation, whitepapers, and support forums.
- AWS Trusted Advisor - Access to the 7 core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard - A personalized view of the health of AWS services, and alerts when your resources are impacted.

- Open the link: https://aws.amazon.com/premiumsupport/plans/

Connected Factory Solution based on AWS IoT for Industry 4.0

- For example,

Volkswagen Group is partnering with AWS to improve the productivity of their plants and save billions of euros when data from all 124 Volkswagen Group plants can be evaluated in a standardized way – “The Industrial Cloud will be a key lever for improving the productivity of plants by 30 percent” according to Head of Volkswagen Group Production Gerd Walker.

- **Introducing the AWS IoT Connected Factory Solution**
- **Unlock data to modernize manufacturing**

Vulnerability Reporting

- Amazon Web Services takes security very seriously, and investigates all reported vulnerabilities.

- **Reporting Suspected Vulnerabilities**
  - **Amazon Web Services (AWS):** If you would like to report a vulnerability or have a security concern regarding AWS cloud services or open source projects, please email aws-security@amazon.com. If you wish to protect your email, you may use our PGP key.

  - **AWS Customer Support Policy for Penetration Testing:** AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for listed services. Requesting Authorization for Other Simulated Events should be submitted via the Simulated Events form. For customers operating in the AWS China (Ningxia & Beijing) Region

Vulnerability Reporting

- **AWS Abuse:** If you suspect that AWS resources (such as an EC2 instance or S3 bucket) are being used for suspicious activity, you can report it to the AWS Abuse Team using the Report Amazon AWS abuse form, or by contacting abuse@amazonaws.com.

- **AWS Compliance Information:** Access to AWS compliance reports are available via AWS Artifact. If you have additional AWS Compliance-related questions, please contact them via their intake form.

- **Amazon.com (Retail):** If you have a security concern with Amazon.com (Retail), Seller Central, Amazon Payments, or other related issues such as suspicious orders, invalid credit card charges, suspicious emails, or vulnerability reporting, please visit our Security for Retail webpage.

AWS Manufacturing

- For more than 25 years, Amazon has designed and manufactured smart products and distributed billions of products through its globally connected distribution network using cutting edge automation, machine learning and AI, and robotics, with AWS at its core.

- **Explore manufacturing processes in the cloud**
  - **Product & Production Design**
  - **Smart Factory**
  - **Smart Products & Services**

Why AWS for manufacturing?

- AWS knows manufacturing
- Most comprehensive & advanced set of services
- Global scale reduces risk
- Advanced security built-in