Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: A **300 level** number requested**.**
2. Course Title: **Cloud Computing and Security**
3. No. of Lectures per week: 0 (L), Tutorial: 1 (T), Laboratory: 3 (P), Additional Hours: 3 (A),

   Credits (3*L+2*T+P+A): 08 Duration of Course: Full Semester
4. Proposing Department/IDP : WSAIS

   Other Departments/IDPs which may be interested in the proposed course: CSE

   Other faculty members interested in teaching the course: Somitra Sanadhya, Manindra Agrawal
5. Proposing Instructor: DUGC (WSAIS)
6. Course Description:

A) Objectives: The objective of this practical-based course is to impart hands-on training in deploying, securing, monitoring, and managing cloud infrastructure using Amazon Web Services (AWS). The course emphasizes practical implementation of cloud security controls, identity management, networking, encryption, monitoring, automation, and controlled penetration testing.

B) Contents: **(for 13 weeks of labs, tutorials, and additional work)**

S. No	Type	Broad Title	Topics	Tools	Duration
1	**Theory**	**Introduction to Cloud Computing & AWS Fundamentals**	**Introduction to Cloud Computing & AWS Fundamentals** • Cloud Computing Overview • Cloud Service Models (IaaS, PaaS, SaaS, FaaS) • Cloud Deployment Models • AWS Global Infrastructure • AWS Shared Responsibility Model	AWS Console	1 Hour
	Practical		**Introduction to Cloud Computing & AWS Fundamentals:** **Objectives** • To understand basic cloud computing concepts and AWS fundamentals. • To create and securely configure an AWS account. • To explore the AWS Management Console and core services. • To deploy and verify a basic Amazon EC2 instance**.**		3 Hour

			Tasks
			• Create an AWS account using a valid email address.
			• Log in to the AWS Management Console.
			• Enable Multi-Factor Authentication (MFA) for the root account.
			• Explore core AWS services:
			  • EC2
			  • S3
			  • IAM
			  • VPC
			• Navigate to the EC2 dashboard.
			• Launch a new EC2 instance.
			• Select a Free Tier eligible AMI (Amazon Linux 2 / Ubuntu).
			• Choose instance type t2.micro.
			• Create and download a key pair for SSH access.
			• Configure security group:
			  • Allow SSH (Port 22) from My IP only.
			• Launch the EC2 instance.
			• Note the instance's public IP address and availability zone.
			• Connect to the instance using SSH.
			• Verify successful instance access using:
			  • uname -a
			  • ip a
			  • whoami
			• Terminate the EC2 instance after completing the lab.		

2	**Theory**	**Identity & Access Management (IAM)**	**Identity & Access Management (IAM)** • IAM Architecture and Components • IAM Users, Groups, and Roles • IAM Policies and Permission Models • Principle of Least Privilege • Multi-Factor Authentication (MFA)	AWS IAM	1 Hour
	Practical		**Identity & Access Management (IAM) :** **Objectives** • To understand the role of Identity and Access Management in AWS security. • To create and manage IAM		3 Hour

			users, groups, and roles. • To implement the principle of least privilege using IAM policies. • To configure and enforce Multi-Factor Authentication (MFA). **Tasks** • Log in to the AWS Management Console using an IAM user or root account. • Navigate to the **IAM** service. • Create an IAM user with console access. • Create an IAM group. • Attach a limited permission policy (e.g., EC2 read-only) to the group. • Add the IAM user to the created group. • Verify user permissions by attempting restricted actions. • Create a custom IAM policy with limited permissions. • Attach the custom policy to a user or group. • Create an IAM role for EC2 service. • Attach appropriate permissions to the role. • Enable Multi-Factor Authentication (MFA) for the IAM user. • Log in using the IAM user and verify MFA enforcement. • Remove or modify permissions to observe access control behavior.		
3	**Theory**	**Securing Data in Amazon S3**	**Securing Data in Amazon S3** • Amazon S3 Overview • S3 Storage Classes • S3 Encryption Mechanisms (SSE-S3, SSE-KMS) • Bucket Policies and Access Control Lists (ACLs) • Versioning and Lifecycle Management	Amazon S3	1 Hour
	Practical		**Securing Data in Amazon S3:** **Objectives** • To understand Amazon S3 data storage and security mechanisms. • To create and configure a		3 Hour

			secure S3 bucket.
			• To implement encryption and access control for S3 objects.
			• To enable versioning and lifecycle management for data protection.
			
			Tasks
			• Log in to the AWS Management Console.
			• Navigate to the **Amazon S3** service.
			• Create a new S3 bucket with a unique name.
			• Select the appropriate AWS region.
			• Enable **Block All Public Access** for the bucket.
			• Enable server-side encryption:
			  • SSE-S3 or SSE-KMS.
			• Upload sample objects to the bucket.
			• Attempt to access the object publicly and verify access denial.
			• Configure bucket permissions using:
			  • Bucket policies
			  • Access Control Lists (ACLs) (if required).
			• Enable **versioning** for the bucket.
			• Upload multiple versions of the same object.
			• Configure a **lifecycle rule** to manage object storage or expiration.
			• Verify encryption status and object versions.
			• Delete the bucket and objects after completing the lab to avoid charges.		

4	**Theory**	**Virtual Private Cloud (VPC) Security & Networking**	**Virtual Private Cloud (VPC) Security & Networking** • VPC Architecture and Design • Subnets and IP Addressing • Route Tables and Traffic Flow • Internet Gateway and NAT Gateway • Security Groups and Network ACLs	AWS VPC	1 Hour
	Practical		**Virtual Private Cloud (VPC) Security & Networking:** **Objectives**		3 Hour

			• To understand the architecture and components of an Amazon VPC.
			• To create a custom VPC with public and private subnets.
			• To configure routing using route tables, Internet Gateway, and NAT.
			• To implement network security using Security Groups and Network ACLs.
			
			Tasks
			• Log in to the AWS Management Console.
			• Navigate to the **VPC** service.
			• Create a custom VPC with a CIDR block.
			• Create a **public subnet** and a **private subnet** within the VPC.
			• Create and attach an **Internet Gateway (IGW)** to the VPC.
			• Create route tables for:
			  • Public subnet (route to IGW)
			  • Private subnet (no direct internet access / NAT if required).
			• Associate subnets with appropriate route tables.
			• Create a **Security Group**:
			  • Allow SSH (Port 22) from My IP.
			  • Allow HTTP (Port 80) if required.
			• Create a **Network ACL (NACL)**:
			  • Allow inbound and outbound rules for required ports.
			• Launch an EC2 instance in the public subnet.
			• Verify internet connectivity from the public subnet.
			• Launch an EC2 instance in the private subnet (if applicable).
			• Verify restricted internet access for the private subnet.
			• Document VPC CIDR, subnet details, and security rules.
			• Delete VPC resources after completing the lab to avoid charges.		

5	**Theory**	**Database Security – RDS**	**Database Security – RDS & DynamoDB**	Amazon RDS	1 Hour

		& DynamoDB	• Managed Database Services Overview • Amazon RDS Architecture • Amazon DynamoDB Overview • Encryption at Rest and In Transit • Database Access Control and Security		
	Practical		**Database Security – RDS & DynamoDB:** **Objectives** • To understand security concepts for managed cloud databases. • To launch and configure an encrypted Amazon RDS database instance. • To implement secure connectivity and access control for databases. **Tasks** • Log in to the AWS Management Console. • Navigate to the **Amazon RDS** service. • Create a new RDS database instance. • Select a database engine (MySQL/PostgreSQL). • Enable **encryption at rest** during database creation. • Configure database credentials securely. • Choose appropriate VPC and subnet group. • Configure security group to allow database access only from authorized sources. • Launch the RDS instance. • Note the database endpoint and port. • Connect securely to the database using a database client. • Verify successful database access. • Delete the RDS instance after completing the lab to avoid charges.		3 Hour
6	**Theory**	**Monitoring,**	**Monitoring, Logging & Incident Response**	CloudWatch, CloudTrail	1 Hour

		Logging & Incident Response	• AWS CloudWatch Overview • AWS CloudTrail Overview • AWS Config Basics • Logging, Metrics, and Dashboards • Incident Detection and Response		

	Practical		**Monitoring, Logging & Incident Response:**
			
			Objectives
			• To monitor AWS resources using CloudWatch.
			• To enable logging and auditing using CloudTrail.
			• To detect security-related events using metrics and alarms.
			
			Tasks
			• Log in to the AWS Management Console.
			• Navigate to **AWS CloudWatch**.
			• Enable monitoring for EC2 or RDS resources.
			• Create CloudWatch dashboards to view key metrics.
			• Configure CloudWatch alarms for:
			  • High CPU usage
			  • Network anomalies
			• Navigate to **AWS CloudTrail**.
			• Enable CloudTrail logging for the AWS account.
			• Review API activity logs in CloudTrail.
			• Generate sample activity and observe logs.
			• Analyze metrics and logs to identify potential incidents.
			• Disable or clean up monitoring resources after the lab.
					3 Hour

7	**Theory**	**DDoS Protection & Application Security**	**DDoS Protection & Application Security** • DDoS Attack Fundamentals • AWS Shield (Standard and Advanced) • AWS Web Application Firewall (WAF) • Rate Limiting and Traffic Filtering • Application Layer Security	AWS Shield, AWS WAF	1 Hour

	Practical		**DDoS Protection & Application Security:**
			
			Objectives
			• To understand DDoS threats and application-layer attacks.
			• To protect an EC2-hosted application using AWS Shield and AWS WAF.
			• To apply rate limiting and traffic filtering rules.
			
			Tasks
			• Log in to the AWS Management Console.
			• Launch or identify an EC2 instance hosting a web application.
			• Verify that the application is accessible over HTTP/HTTPS.
			• Navigate to **AWS Shield** and confirm Shield Standard is enabled.
			• Navigate to **AWS WAF**.
			• Create a **Web ACL**.
			• Add managed rule groups:
			  • IP reputation list
			  • Common rule set
			  • SQL injection protection
			• Configure rate-based rules.
			• Associate the Web ACL with:
			  • Application Load Balancer (ALB) or EC2 resource.
			• Generate test traffic to the application.
			• Monitor allowed and blocked requests in AWS WAF.
			• Review WAF metrics and logs.
			• Remove WAF resources after completing the lab.
					3 Hour

8	**Theory**	**Encryption Key Management with AWS KMS**	**Encryption Key Management with AWS KMS** • AWS KMS Overview • Customer Managed Keys (CMKs) • Key Policies and Grants • Envelope Encryption • Automatic Key Rotation	AWS KMS	1 Hour

	Practical		**Encryption Key Management with AWS KMS:** **Objectives** • To create and manage encryption keys using AWS KMS. • To understand key rotation and envelope encryption. • To apply KMS-based encryption to AWS services. **Tasks** • Log in to the AWS Management Console. • Navigate to **AWS Key Management Service (KMS)**. • Create a **Customer Managed Key (CMK)**. • Configure key administrators and key users. • Enable automatic key rotation. • Encrypt an Amazon S3 bucket using SSE-KMS. • Upload objects and verify encryption status. • Enable KMS encryption for an Amazon RDS instance. • Verify data encryption at rest. • Schedule deletion of the CMK after lab completion.		3 Hour
9	**Theory**	**Security Automation & Compliance**	**Security Automation & Compliance** • AWS Inspector Overview • AWS Security Hub Overview • Vulnerability and Compliance Assessment • Security Automation Concepts • Incident Response Playbooks	AWS Inspector, Lambda	1 Hour
	Practical		**Security Automation & Compliance:** **Objectives** • To assess cloud resource security using automated tools. • To identify vulnerabilities and compliance issues. • To automate alerts and remediation actions. **Tasks** • Log in to the AWS Management Console. • Navigate to **AWS Inspector**. • Enable Inspector for EC2		3 Hour

			resources. • Perform a vulnerability scan on selected instances. • Review identified vulnerabilities and risk severity. • Navigate to **AWS Security Hub**. • Enable Security Hub and review security findings. • Create an AWS Lambda function for automated alerting. • Configure CloudWatch/EventBridge rules to trigger Lambda. • Verify automated alerts for detected security events. • Disable Inspector, Security Hub, and Lambda after the lab.		
10	**Theory**	**Containerization & Infrastructure Automation**	**Containerization & Infrastructure Automation** • Containerization Concepts • Docker Architecture and Workflow • Docker Hub and Image Management • AWS CLI Basics • Infrastructure as Code (Terraform)	Docker, AWS CLI, Terraform	1 Hour
	Practical		**Containerization & Infrastructure Automation:** **Objectives** • To understand containerization using Docker. • To deploy containerized applications on AWS EC2. • To automate infrastructure provisioning using AWS CLI and Terraform. **Tasks** • Log in to the AWS Management Console. • Launch an EC2 instance for container deployment. • Connect to the EC2 instance using SSH. • Install Docker on the EC2 instance. • Verify Docker installation using docker --version. • Pull a container image from Docker Hub.		3 Hour

			• Run a containerized application. • Verify application accessibility using the EC2 public IP. • Install and configure AWS CLI on the instance. • Install Terraform on the local system or EC2. • Write a basic Terraform configuration to deploy an EC2 instance. • Initialize and apply Terraform configuration. • Verify automated resource deployment. • Destroy Terraform-managed resources after the lab.		
11	**Theory**	**Cloud Penetration Testing & Risk Assessment**	**Cloud Penetration Testing & Risk Assessment** • Cloud Penetration Testing Concepts • AWS Penetration Testing Policy • Vulnerability Assessment Methodology • Risk Identification and Analysis • Remediation and Re-Testing	AWS Inspector, OWASP ZAP	1 Hour
	Practical		**Cloud Penetration Testing & Risk Assessment:** **Objectives** • To understand AWS penetration testing policies. • To identify vulnerabilities in cloud-hosted applications. • To analyze and remediate identified security risks. **Tasks** • Log in to the AWS Management Console. • Launch an EC2 instance hosting a test web application. • Review AWS penetration testing policy guidelines. • Enable **AWS Inspector** for the EC2 instance. • Run a vulnerability scan. • Review findings and risk severity. • Install and launch **OWASP ZAP**.		3 Hour

			• Perform a web application vulnerability scan. • Analyze identified vulnerabilities. • Apply remediation steps. • Re-run scans to verify risk reduction. • Terminate test resources after the lab.		
12	**Theory**	**Integrated Cloud Security Case Study**	**Integrated Cloud Security Case Study** • Secure Cloud Architecture Design • Security Control Integration • Event Correlation and Analysis • Security Validation Techniques • Documentation and Reporting	AWS Services	1 Hour
	Practical		**Integrated Cloud Security Case Study:** **Objectives** • To apply cloud security concepts in an integrated environment. • To correlate security events and validate configurations. • To evaluate end-to-end cloud security posture. **Tasks** • Design a secure cloud architecture using AWS services. • Deploy EC2, S3, IAM, and VPC components securely. • Apply IAM least privilege policies. • Enable encryption for data storage. • Configure logging and monitoring services. • Simulate a security event. • Analyze logs and alerts. • Validate compliance with security best practices. • Document observations and findings. • Clean up deployed resources.		3 Hour
13	**Theory**	**Backup, Disaster Recovery &**	**Backup, Disaster Recovery & High Availability in AWS** • Backup and Recovery Concepts	AWS Backup	1 Hour

		High Availability in AWS	• Disaster Recovery Strategies • High Availability Architectures • RTO and RPO Concepts • AWS Backup Overview		
	Practical		**Backup, Disaster Recovery & High Availability in AWS:** **Objectives** • To understand backup and disaster recovery strategies. • To implement automated backups for EC2 instances. • To test recovery from backup in AWS. **Tasks** • Log in to the AWS Management Console. • Navigate to AWS Backup service. • Create a backup vault. • Define a backup plan with schedule and retention policy. • Assign EC2 instances to the backup plan. • Perform an on-demand backup. • Verify backup completion. • Restore EC2 instance from backup. • Validate instance recovery. • Delete backup resources after completing the lab.		3 Hour

C) Pre-requisites:

- Working knowledge of Windows and Linux OS
- Basic networking concepts
- Familiarity with virtual machines and virtualization
- Introductory cloud computing knowledge

D) Short summary for including in the Courses of Study Booklet: This course provides practical training to the students on cloud computing and security. Students will be able to create and secure AWS accounts and resources, implement identity and access management using IAM, monitor cloud resources, and detect security incidents. The course will also enable students to perform controlled penetration testing in cloud environments.

7. Recommended books:
   • The following tools and technologies will be used in the labs:

   - AWS Console, AWS IAM, Amazon S3, AWS VPC, Amazon RDS
   - CloudWatch, CloudTrail, MobaXterm, AWS Shield, AWS WAF, AWS KMS, AWS Inspector
   - Lambda, Docker, AWS CLI, Terraform, OWASP ZAP, AWS Services, AWS Backup

---

Dated: 13 August 2026; Proposer: DUGC, WSAIS

Dated: ; DUGC Convener (WSAIS):_____

The course is approved / not approved

_____

Chairperson, SUGC

Dated:_____