AWS CLOUD SECURITY

Technical Report · November 2022

CITATIONS
0

READS
359

1 author:

Kommuri Saiteja
Sreenidhi Institute of Science & Technology
8 PUBLICATIONS **0** CITATIONS

SEE PROFILE

A SUMMER INDUSTRY INTERNSHIP - I REPORT ON

AWS CLOUD SECURITY

Submitted in partial fulfilment of the requirements for the Award of Degree in Bachelor of Technology in

ELECTRONICS AND COMMUNICATION ENGINEERING [ECE]

BY

KOMMURI SAITEJA (20311A0460)

NAREDLA SAI CHARAN (20311A0458)

GATLA ABHISHEK (20311A0455)

Department of Electronics and Communication Engineering (ECE)

Sreenidhi Institute of Science and Technology

HYDERABAD

November 2022

Affiliated to

Jawaharlal Nehru Technology University Hyderabad - 500085

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY

(AUTONOMOUS)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING (ECE)

CERTIFICATE

This is to certify that the A SUMMER INDUSTRY INTERNSHIP - I Report titled "**AWS CLOUD SECURITY** "submitted by **KOMMURI SAITEJA, NAREDLA SAI CHARAN, GATLA ABHISHEK** Bearing Roll-Number **20311A0460, 20311A0458, 20311A0455** Towards partial fulfilment for the award of Bachelor Of Technology in **ELECTRONICS AND COMMUNICATION ENGINEERING (ECE)** from Sreenidhi Institute of Science & Technology, Ghatkesar, Hyderabad, is a record of bonafide work summer industry internship that has been carried out during III B Tech ECE I-Semester, will be evaluated under our guidance.

The results embodied in the work are not submitted to any other University or Institute for award of any degree or diploma.

Project Coordinator
Mr.Chenchu Sreedhar Kakarla
Assistant Professor
CSE Department

Dr.S.P.V Subba Rao
Professor
HOD,ECE DEPARTMENT

External Examiner :

Date:


aws academy
KOMMURI SAITEJA
Certificate of Completion for
AWS Academy Graduate - AWS Academy Cloud Foundations
Course hours completed
20 hours
Issued on
09/20/2022
Digital badge
https://www.credly.com/go/W19saJqU


aws academy
KOMMURI SAITEJA
Certificate of Completion for
AWS Academy Graduate - AWS Academy Machine Learning Foundations
Course hours completed
20 hours
Issued on
10/10/2022
Digital badge
https://www.credly.com/go/pvBPpYV8

aws academy

NAREDLA SAICHARAN .

Certificate of Completion for
AWS Academy Graduate - AWS Academy Cloud Foundations

Course hours completed

20 hours

Issued on

09/23/2022

Digital badge

https://www.credly.com/go/u4GPguk5

aws academy

NAREDLA SAICHARAN .

Certificate of Completion for
AWS Academy Graduate - AWS Academy Machine Learning Foundations

Course hours completed

20 hours

Issued on

12/02/2022

Digital badge

https://www.credly.com/go/PFp96g91

aws academy

Abhishek Gatla

Certificate of Completion for
AWS Academy Graduate - AWS Academy Cloud Foundations

Course hours completed

20 hours

Issued on

09/24/2022

Digital badge

https://www.credly.com/go/9OzL8M8Y

aws academy

Abhishek Gatla

Certificate of Completion for
AWS Academy Graduate - AWS Academy Machine Learning Foundations

Course hours completed

20 hours

Issued on

11/03/2022

Digital badge

https://www.credly.com/go/k6iSRhAa

ACKNOWLEDGEMENT

I wish to express immense Gratitude to my Supervisor, Mr.Chenchu Sreedhar Kakarla , Assistant Professor, CSE Department, for his able guidance and useful suggestions, which helped me in completing my project . His valuable suggestions and comments towards this Project have been very much helpful in tackling various obstacles and accomplishing the major tasks.

I take immense pleasure in thanking HOD Dr.S.P.V Subba Rao, Principal Dr. Ch. Shiva Reddy and our Executive Director Dr.C.V.Tomy and all faculty members of ECE department for having permitted me to carry out this Project work.

Last but not least I would like to express my heartfelt thanks to my beloved Parents for their blessings, friends, and classmates for their help and wishes for the successful completion of Project.

KOMMURI SAITEJA
(20311A0460)
NAREDLA SAI CHARAN
(20311A0458)
GATLA ABHISHEK
(20311A0455)

DECLARATION

I **KOMMURI SAITEJA (20311A0460), NAREDLA SAI CHARAN(20311A0458), GATLA ABHISHEK(20311A0455)** students of **SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY, YAMNAMPET, GHATKESAR**, studying IIIrd Year Ist Semester, **ELECTRONICS AND COMMUNICATION ENGINEERING** solemnly declare that the Summer Industry Internship - I Report titled "**AWS CLOUD SECURITY** " is submitted to **SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY** for partial fulfilment for the award of degree of Bachelor of technology in **ELECTRONICS AND COMMUNICATION ENGINEERING**

It is declared to the best of our knowledge that the work reported does not form part of any dissertation submitted to any other University or Institute for award of any degree

KOMMURI SAITEJA
(20311A0460)
NAREDLA SAI CHARAN
(20311A0458)
GATLA ABHISHEK
(20311A0455)

AWS CLOUD SECURITY

ABSTRACT

Security is the highest priority at Amazon Web Services (AWS). AWS delivers a scalable cloud computing environment that is designed for high availability and dependability, while providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is critical to AWS, and so is maintaining customer trust and confidence. This module provides an introduction to the AWS approach to security, which includes both the controls in the AWS environment and some of the AWS products and features customers can use to meet their security objectives.

Security and compliance are a shared responsibility between AWS and the customer. This shared responsibility model is designed to help relieve the customer's operational burden. At the same time, to provide the flexibility and customer control that enables the deployment of customer solutions on AWS, the customer remains responsible for some aspects of the overall security. The differentiation of who is responsible for what is commonly referred to as security "of" the cloud versus security "in" the cloud.

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 centre's 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.

CONTENTS

1.INTRODUCTION

AWS provides services that help you protect your data, accounts, and workloads from unauthorised access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects your accounts and workloads. All data is stored in highly secure AWS data centre's. Meet compliance requirements AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed. Scale quickly Security scales with your AWS Cloud usage.These assessments include network access, common vulnerabilities and exposures (CVEs), Centre for Internet Security (CIS) benchmarks, and common best practices such as disabling root login for SSH and validating system directory permissions on your EC2 instances.

1.1 SCOPE

Cloud security at AWS is the highest priority. As organizations embrace the scalability and flexibility of the cloud, AWS is helping them evolve security, identity, and compliance into key business enablers. AWS builds security into the core of our cloud infrastructure, and offers foundational services to help organizations meet their unique security requirements in the cloud. As an AWS customer, you will benefit from a data centre 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 centre's 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 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. 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.In the AWS environment, you can take advantage of automated tools for asset inventory and privileged access reporting.

❖ BENEFITS OF AWS CLOUD 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 centre's.
- **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 centre's. 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.

1.2 EXISTING SYSTEM

FIRST-GENERATION PUBLIC CLOUDS

First-generation public clouds focused on the efficient use of hardware resources enabled by virtualisation and use of a hypervisor. These clouds were built on many of the same technologies and principles used in private clouds, which were designed so that expensive hardware resources didn’t remain idle. Security sometimes wasn’t a foundational principle of this design because private data centre's relied on perimeter defence's. As public cloud use became more common, so did concerns about attacks associated with hypervisor vulnerabilities. Security is a primary concern for enterprise customers, and the risk associated with the hypervisor design of first-generation public clouds was only growing.

1.3 PROPOSED SYSTEM

ORACLE CLOUD INFRASTRUCTURE [NEXT-GENERATION PUBLIC CLOUD]

OCI is a security-first public cloud infrastructure that Oracle built for enterprise critical workloads. Security-first means that Oracle redesigned the virtualization stack to reduce the risk from hypervisor-based attacks and increase tenant isolation. The result is a next-generation public cloud infrastructure design that provides significant security benefits over first generation cloud infrastructure designs. We’ve implemented this design in every data center and region. OCI is a complete IaaS platform. It provides the services needed to build and run applications in a highly secure, hosted environment with high performance and availability. Customers can run the Compute and Database services on bare metal instances, which are customer-dedicated physical servers, or as virtual machines (VM) instances, which are isolated computing environments on top of bare metal hardware.

Bare metal and VM instances run on the same types of server hardware, firmware, underlying software, and networking infrastructure, so both instance types have the OCI protections built into those layers.

❖ MERITS:

As cloud has become more common, security concerns have become more important. From its inception, Oracle Cloud Infrastructure prioritized solving the security issues that grew out of first-generation clouds.

2.SYSTEM ANALYSIS

This System Analysis is closely related to requirements analysis. It is also "an explicit formal inquiry carried out to help someone (referred to as the decision maker) identify a better course of action and make a better decision than he might otherwise have made." This step involves breaking down the system in different pieces to analyze the situation, analyzing project goals, breaking down what needs to be created and attempting to engage users so that definite requirements can be defined.

2.1 FUNCTIONAL REQUIREMENT SPECIFICATION

The System after careful analysis has been identified to be present with the following modules AWS operates, manages, and controls the components from the software virtualization layer down to the physical security of the facilities where AWS services operate.

❖ AWS SHARED RESPONSIBILITY MODEL:

AWS is responsible for protecting the infrastructure that runs all the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run the AWS Cloud services.The customer is responsible for the encryption of data at rest and data in transit. The customer should also ensure that the network is configured for security and that security credentials and logins are managed safely. Additionally, the customer is responsible for the configuration of security groups and the configuration of the operating system that run on compute instances that they launch (including updates and security patches).Under the AWS shared responsibility model, AWS operates, manages, and controls the components from the bare metal host operating system and hypervisor virtualization layer down to the physical security of the facilities where the services operate. It means that AWS is responsible for protecting the global infrastructure that runs all the services that are offered in the AWS Cloud

AWS is responsible for the physical infrastructure that hosts your resources including:

- **PHYSICAL SECURITY OF DATA CENTRE'S:** With controlled, need-based access located in nondescript facilities, with 24/7 security guards two-factor authentication access logging and review, video surveillance and disk degaussing and destruction.
- **HARDWARE INFRASTRUCTURE:** Such as servers, storage devices, and other appliances that AWS relies on.
- **SOFTWARE INFRASTRUCTURE:** Which hosts operating systems, service applications, and virtualization software.
- **NETWORK INFRASTRUCTURE:** Such as routers, switches, load balancers, firewalls, and cabling. AWS also continuously monitors the network at external boundaries, secures access points, and provides redundant infrastructure with intrusion detection

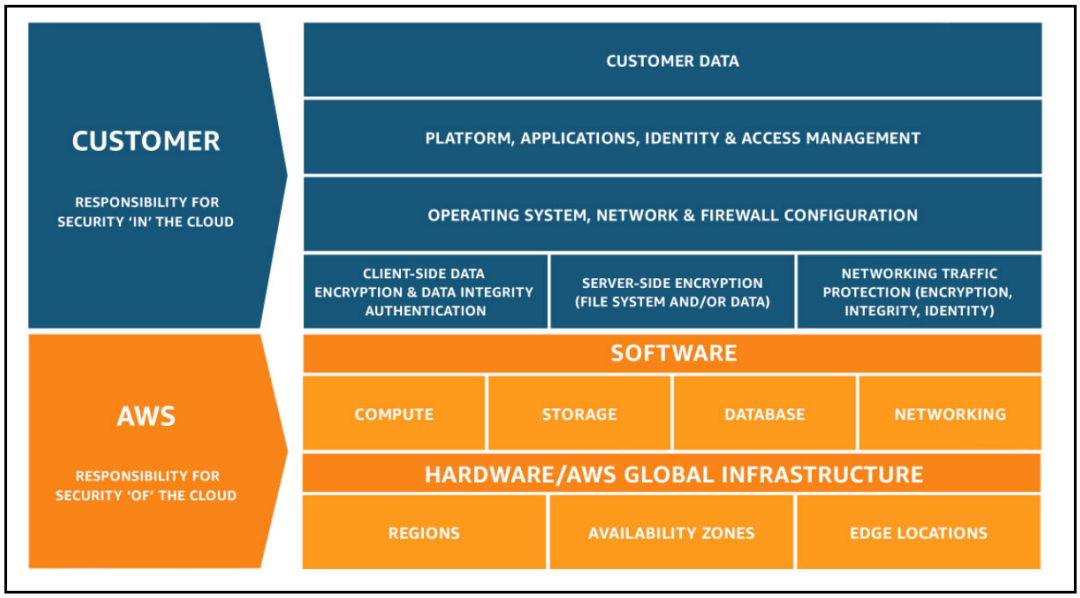


FIG-2.1 AWS SHARED RESPONSIBILITY MODEL

❖ AWS IDENTITY AND ACCESS MANAGEMENT (IAM):

AWS Identity and Access Management (IAM) allows you to control access to compute storage, database, and application services in the AWS Cloud. IAM can be used to handle authentication, and to specify and enforce authorization policies so that you can specify which users can access which services.AM is a tool that centrally manages access to launching, configuring, managing, and terminating resources in your AWS account. It provides granular control over access to resources, including the ability to specify exactly which API calls the user is authorized to make to each service. Whether you use the AWS Management Console, the AWS CLI, or the AWS software development kits (SDKs), every call to an AWS service is an API call

❖ IAM ESSENTIAL COMPONENTS:

IAM USER

IAM GROUP

IAM POLICY

IAM ROLE

AN IAM USER is a person or application that is defined in an AWS account, and that must make API calls to AWS products. Each user must have a unique name (with no spaces in the name) within the AWS account and a set of security credentials that is not shared with other users.

AN IAM GROUP is a collection of IAM users. You can use IAM groups to simplify specifying and managing permissions for multiple users. It is a collection of IAM users that are granted identical authorization.

AN IAM POLICY is a document that defines permissions to determine what users can do in the AWS account. A policy typically grants access to specific resources and specifies what the user can do with those resources. Policies can also explicitly deny access. It is a document that defines which resources can be accessed and the level of access to each resource.

AN IAM ROLE is a tool for granting temporary access to specific AWS resources in an AWS account. Useful mechanism to grant a set of permissions for making AWS service requests.With IAM, you can manage which resources can be accessed by who and how these resources can be accessed. You can grant different permissions to different people for different resources. For example, you might allow some users full access to Amazon EC2, Amazon S3, Amazon DynamoDB, Amazon Redshift, and other AWS services.

❖ SECURING A NEW AWS ACCOUNT:

When you first create an AWS account, you begin with a single sign in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and it is accessed by signing into the AWS Management Console with the email address and password that you used to create the account. AWS account root users have (and retain) full access to all resources in the account. Therefore, AWS strongly recommends that you do not use account root user credentials for day-to-day interactions with the account.AWS recommends that you use IAM to create additional users and assign permissions to these users, following the principle of least privilege. For example, if you require administrator-level permissions, you can create an IAM user, grant that user full access, and then use those credentials to interact with the account.

Later, if you need to revoke or modify your permissions you can delete or modify any policies that are associated with that IAM user.

❖ SECURING ACCOUNTS:

AWS ORGANIZATIONS is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. Here, the focus is on the security features that AWS Organizations provides.helpful security feature is that you can group accounts into organizational units (OU) and attach different access policies to each OU. For example, if you have accounts that should only be allowed to access AWS services that meet certain regulatory requirements, you can put those accounts into one OU. You then can define a policy that blocks OU access to services that do not meet those regulatory requirements, and then attach the policy to the OU.

Another security feature is that AWS Organizations integrates with and supports IAM. AWS Organizations expands that control to the account level by giving you control over what users and roles in an account or a group of accounts can do. The resulting permissions are the logical intersection of what is allowed by the AWS Organizations policy settings and what permissions are explicitly granted by IAM in the account for that user or role. The user can access only what is allowed by both the AWS Organizations policies and IAM policies.

AWS KEY MANAGEMENT SERVICE (AWS KMS) is a service that enables you to create and manage encryption keys, and to control the use of encryption across a wide range of AWS services and your applications. AWS KMS is a secure and resilient service that uses hardware security modules (HSMs) that were validated under Federal Information ProcessingStandards (FIPS) 140-2(or are in the process of being validated) to protect your keys. AWS KMS also integrates with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance.

AMAZON COGNITO provides solutions to control access to AWS resources from your application. You can define roles and map users to different roles so your application can access only the resources that are authorized for each user.

AWS SHIELD is a managed distributed denial of service (DDoS) protection service that safeguards applications that run on AWS. It provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

❖ SECURING DATA ON AWS:

DATA IN TRANSIT refers to data that is moving across the network. Encryption of data in transit is accomplished by using Transport Layer Security (TLS) 1.2 with an open standard AES-256 cipher.TLS was formerly called Secure Sockets Layer (SSL).

AWS CERTIFICATE MANAGER is a service that enables you to provision, manage, and deploy SSL or TLS certificates for use with AWS services and your internal connected resources. SSL or TLS certificates are used to secure network communications and establish the identity of websites over the internet, and also resources on private networks. With AWS Certificate Manager, you can request a certificate and then deploy it on AWS resources (such as load balancers or CloudFront distributions).AWS Certificate Manager also handles certificate renewals.

Web traffic that runs over HTTP is not secure. However, traffic that runs over **SECURE HTTP (HTTPS)** is encrypted by using TLS or SSL. HTTPS traffic is protected against eavesdropping and man-in-the-middle attacks because of the bidirectional encryption of the communication.

The second example shows the use of **AWS STORAGE GATEWAY**, a hybrid cloud storage service that provides on-premises access to AWS Cloud storage. In this example, the storage gateway is connected across the internet to Amazon S3, and the connection encrypts the data in transit.

❖ WORKING TO ENSURE COMPLIANCE:

AWS engages with external certifying bodies and independent auditors to provide customers with information about the policies, processes, and controls that are established and operated by AWS.WS also provides security features and legal agreements that are designed to help support customers with common regulations and laws. One example is the **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)** regulation. Another example, the European Union (EU) **GENERAL DATA PROTECTION REGULATION (GDPR)** protects European Union data subjects' fundamental right to privacy and the protection of personal data.

AWS CONFIG is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations, and it enables you to automate the evaluation of recorded configurations against desired configurations.

AWS ARTIFACT provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as audit artefacts) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls. AWS Artifact provides documents about AWS only. AWS customers are responsible for developing or obtaining documents that demonstrate the security and compliance of their companies.

2.2 PERFORMANCE REQUIREMENTS

Performance is measured in terms of the output provided by the application. Requirement specification plays an important part in the analysis of a system. Only when the requirement specifications are properly given, it is possible to design a system, which will fit into required environment. It rests largely with the users of the existing system to give the requirement specifications because they are the people who finally use the system. This is because the requirements have to be known during the initial stages so that the system can be designed according to those requirements. It is very difficult to change the system once it has been designed and on the other hand designing a system, which does not cater to the requirements of the user, is of no use.

The requirement specification for any system can be broadly stated as given below:

- The system should be able to interface with the existing system
- The system should be accurate
- The system should be better than the existing system

The existing system is completely dependent on the user to perform all the duties.

2.3 SOFTWARE REQUIREMENTS

- **OPERATING SYSTEM:** Microsoft Windows XP.
- **TECHNOLOGY:** Java Server Pages.
- **FRONT-END:** HTML,CSS.
- **BACK-END:** ORACLE 10g.
- **WEB-SERVER:** Apache-Tomcat 6.0.32.
- **PLATFORM:** Advanced Java Concepts (J2EE).

2.4 HARDWARE REQUIREMENTS

- **PROCESSOR :** Intel P-IV based system.
- **RAM :** Min. 512 MB.

3.SYSTEM DESIGN

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. Object-oriented analysis and design methods are becoming the most widely used methods for computer systems design.

3.1 ARCHITECTURAL DESIGN

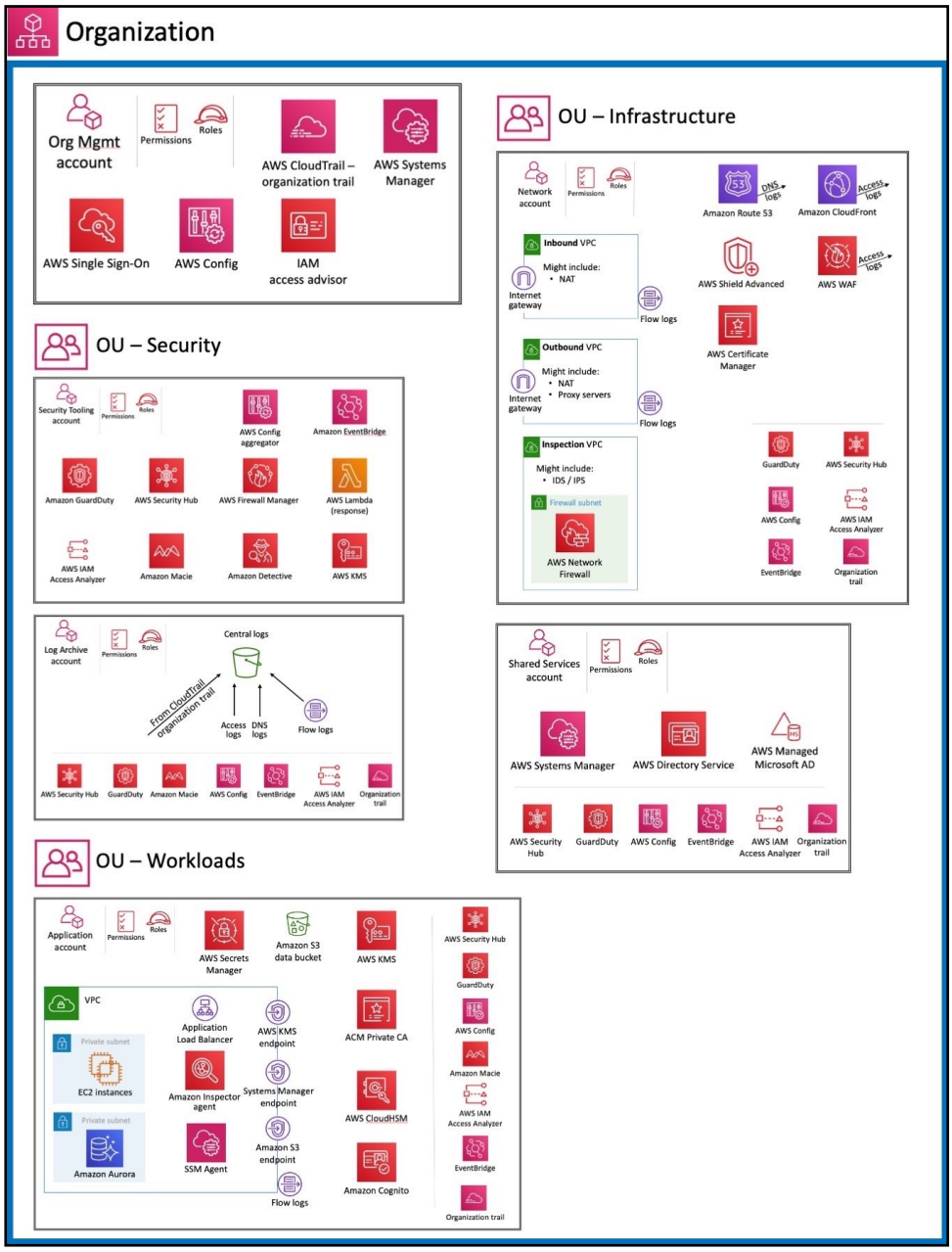


FIG-3.1 ARCHITECTURAL DESIGN

The following diagram illustrates the AWS SRA. This architectural diagram brings together all the AWS security-related services. It is built around a simple, three-tier web architecture that can fit on a single page. In such a workload, there is a web tier through which users connect and interact with the application tier, which handles the actual business logic of the application: taking inputs from the user, doing some computation, and generating outputs. The application tier stores and retrieves information from the data tier. The architecture is purposefully modular and provides high-level abstraction for many modern web applications. For this reference architecture, the actual web application and data tier are deliberately represented as simply as possible, through Amazon Elastic Compute Cloud (Amazon EC2) instances and an Amazon Aurora database, respectively. Most architecture diagrams focus and dive deep on the web, application, and data tiers. For readability, they often omit the security controls. This diagram flips that emphasis to show security wherever possible, and keeps the application and data tiers as simple as necessary to show security features meaningfully. The AWS SRA contains all AWS security-related services available at the time of publication. (See Document history.) However, not every workload or environment, based on its unique threat exposure, has to deploy every security service. Our goal is to provide a reference for a range of options, including descriptions of how these services fit together architecturally, so that your business can make decisions that are most appropriate for your infrastructure, workload, and security needs, based on risk.

❖ ORG MANAGEMENT ACCOUNT:

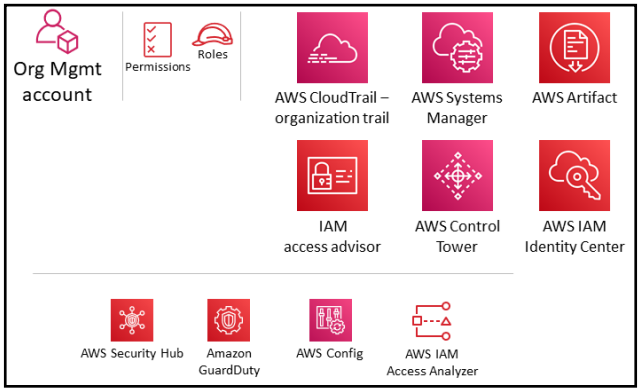
The sections Using AWS Organizations for security and The management account, trusted access, and delegated administrators earlier in this guide discussed the purpose and security objectives of the Org Management account in depth. Follow the security best practices for your Org Management account. These include using an email address that is managed by your business, maintaining the correct administrative and security contact information (such as attaching a phone number to the account in the event AWS needs to contact the owner of the account), enabling multi-factor authentication (MFA) for the all users, and regularly reviewing who has access to the Org Management account. Services deployed in the Org Management account should be configured with appropriate roles, trust policies, and other permissions so that the administrators of those services (who must access them in the Org Management account) cannot also inappropriately access other services.

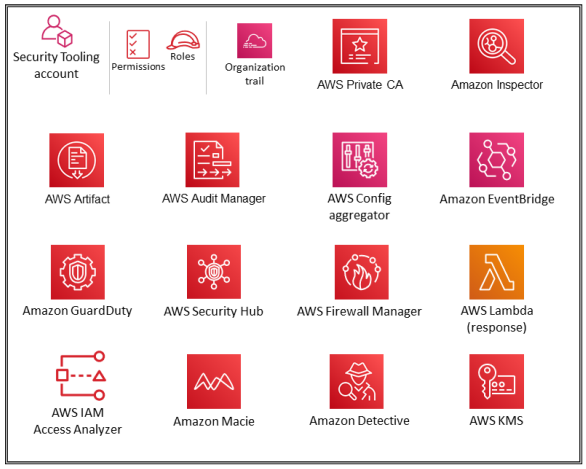
AWS CLOUDTRAIL is a service that supports governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail is integrated with AWS Organizations, and that integration can be used to create a single trail that logs all events for all accounts in the AWS organization.

❖ SECURITY OU - SECURITY TOOLING ACCOUNT:

The Security Tooling account is dedicated to operating security services, monitoring AWS accounts, and automating security alerting and response. The security objectives include the following:

- Provide a dedicated account with controlled access to manage access to the security guardrails, monitoring, and response.
- Maintain the appropriate centralized security infrastructure to monitor security operations data and maintain traceability. Detection, investigation, and response are essential parts of the security lifecycle and can be used to support a quality process, a legal or compliance obligation, and for threat identification and response efforts.
- Further support a defence-in-depth organization strategy by maintaining another layer of control over appropriate security configuration and operations such as encryption keys and security group settings. This is an account where security operators work. Read-only/audit roles to view AWS organization-wide information are typical, whereas write/modify roles are limited in number, tightly controlled, monitored, and logged.

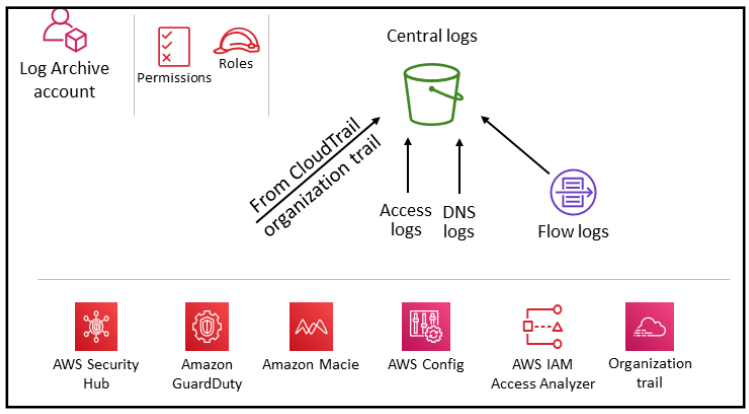




AWS Control Tower names the account under the Security OU the Audit Account by default. You can rename the account during the AWS Control Tower setup. It might be appropriate to have more than one Security Tooling account.

❖ SECURITY OU - LOG ARCHIVE ACCOUNT:

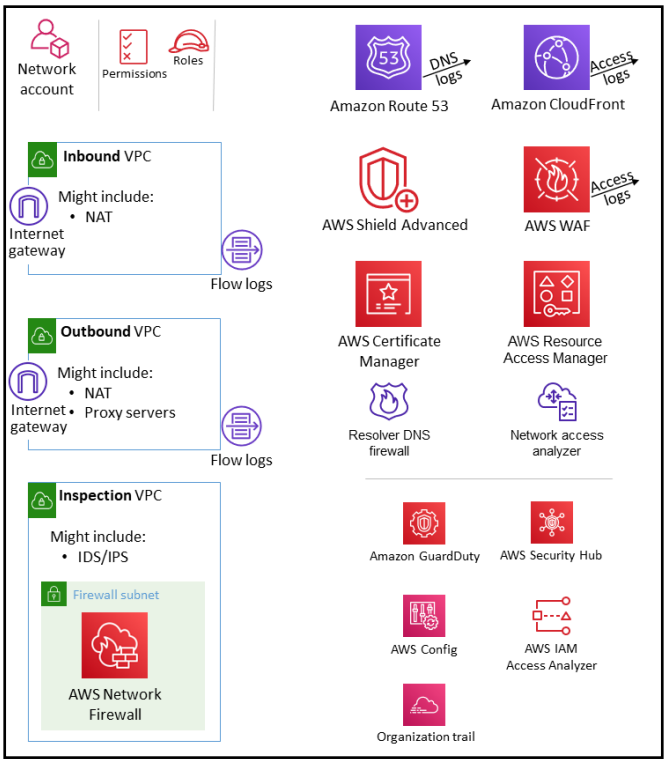
The Log Archive account is dedicated to ingesting and archiving all security-related logs and backups. With centralized logs in place, you can monitor, audit, and alert on Amazon S3 object access, unauthorized activity by identities, IAM policy changes, and other critical activities performed on sensitive resources. The security objectives are straightforward: This should be immutable storage, accessed only by controlled, automated, and monitored mechanisms, and built for durability (for example, by using the appropriate replication and archival processes). Controls can be implemented at depth to protect the integrity and availability of the logs and log management process. In addition to preventive controls, such as assigning least privilege roles to be used for access and encrypting logs with a controlled AWS KMS key, use detective controls such as AWS Config to monitor (and alert and remediate) this collection of permissions for unexpected changes.



❖ INFRASTRUCTURE OU - NETWORK ACCOUNT:

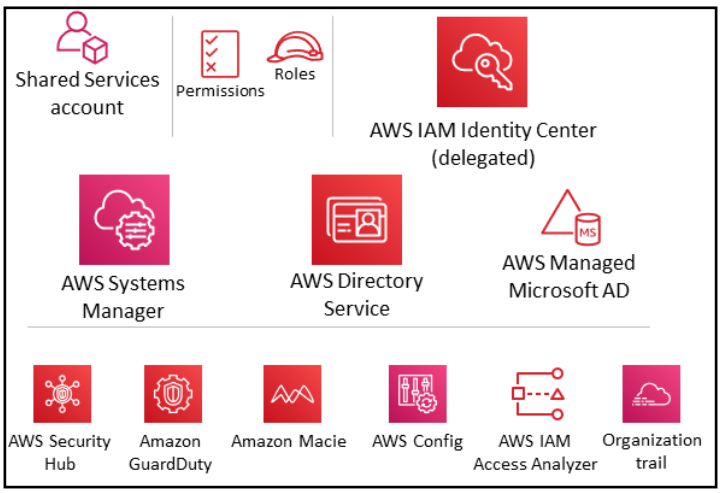
The Network account manages the gateway between your application and the broader internet. It is important to protect that two-way interface. The Network account isolates the networking services, configuration, and operation from the individual application workloads, security, and other infrastructure. This arrangement not only limits connectivity, permissions, and data flow, but also supports separation of duties and least privilege for the teams that need to operate in these accounts. By splitting network flow into separate inbound and outbound virtual private clouds (VPCs), you can protect sensitive infrastructure and traffic from undesired access. The inbound network is generally considered higher risk and deserves appropriate routing, monitoring, and potential issue mitigations. These infrastructure accounts will inherit permission guardrails from the Org Management account and the Infrastructure OU. Networking (and security) teams manage the majority of the infrastructure in this account.

Although network design and specifics are beyond the scope of this document, we recommend these three options for network connectivity between the various accounts: VPC peering, AWS PrivateLink, and AWS Transit Gateway. Important considerations in choosing among these are operational norms, budgets, and specific bandwidth needs.



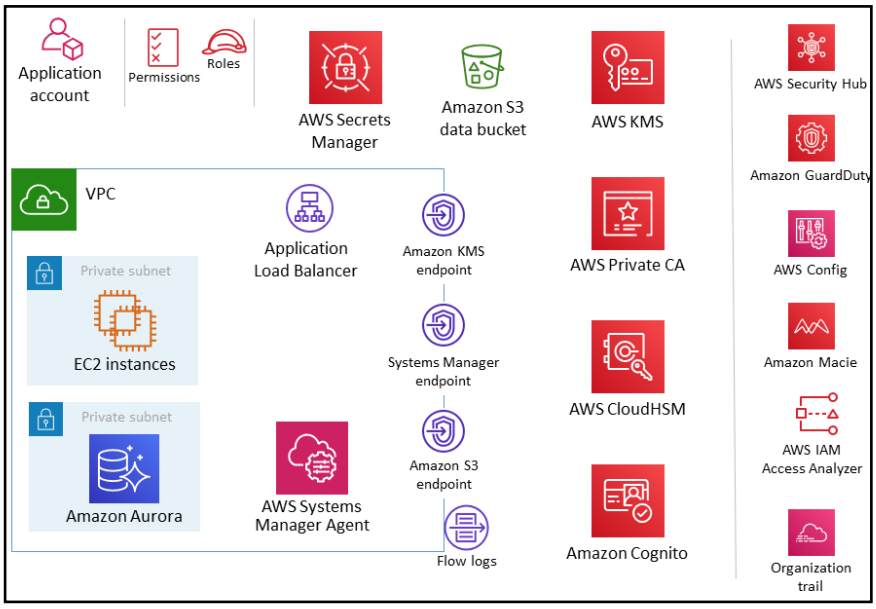
❖ INFRASTRUCTURE OU - SHARED SERVICES ACCOUNT:

The Shared Services account is part of the Infrastructure OU, and its purpose is to support the services that multiple applications and teams use to deliver their outcomes. For example, directory services (Active Directory), messaging services, and metadata services are in this category. The AWS SRA highlights the shared services that support security controls. Although the Network accounts are also part of the Infrastructure OU, they are removed from the Shared Services account to support the separation of duties. The teams that will manage these services don't need permissions or access to the Network accounts.



❖ WORKLOADS OU - APPLICATION ACCOUNT:

The Application account hosts the primary infrastructure and services to run and maintain an enterprise application. The Application account and Workloads OU serve a few primary security objectives. First, you create a separate account for each application to provide boundaries and controls between workloads so that you can avoid issues of commingling roles, permissions, data, and encryption keys. You want to provide a separate account container where the application team can be given broad rights to manage their own infrastructure without affecting others. Next, you add a layer of protection by providing a mechanism for the security operations team to monitor and collect security data. Employ an organization trail and local deployments of account security services (Amazon GuardDuty, AWS Config, AWS Security Hub, Amazon EventBridge, AWS IAM Access Analyzer), which are configured and monitored by the security team. Finally, you enable your enterprise to set controls centrally. You align the application account to the broader security structure by making it a member of the Workloads OU through which it inherits appropriate service permissions, constraints, and guardrails.



4.SYSTEM IMPLEMENTATION

The implementation stage of any project is a true display of the defining moments that make a project a success or a failure. The implementation stage is defined as the system or system modifications being installed and made operational in a production environment. The phase is initiated after the system has been tested and accepted by the user. This phase continues until the system is operating in production in accordance with the defined user requirements.

4.1 PROCEDURE

❖ TASK 1: EXPLORE THE USERS AND GROUPS

In this task, you will explore the Users and Groups that have already been created for you in **IAM**.

1.In the **AWS Management Console**, on the Services menu, click **IAM**.

2.In the navigation pane on the left, click **Users**.

The following IAM Users have been created for you:

- user-1
- user-2
- user-3

3.Click **user-1**.

This will bring to a summary page for **user-1**. The Permissions tab will be displayed.

4.Notice that **user-1** does not have any permissions.

5.Click the **Groups** tab.

user-1 also is not a member of any groups.

6.Click the **Security credentials tab.**

user-1 is assigned a **Console password**

7.In the navigation pane on the left, click **Groups**.

The following groups have already been created for you:

- EC2-Admin
- EC2-Support
- S3-Support

8.Click the **EC2-Support group**.

This will bring you to the summary page for the EC2-Support group.

9.Click the **Permissions** tab.

This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. Managed Policies are pre-built policies (built either by AWS or by your administrators) that can be attached to lAM Users and Groups. When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.

10.Under **Actions**, click the **Show Policy** link.

A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe information about EC2, Elastic Load Balancing,

CloudWatch and Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a Support role.

The basic structure of the statements in an IAM Policy is:

- **Effect** says whether to Allow or Deny the permissions.
- **Action** specifies the API calls that can be made against an AWS Service.
- **Resource** defines the scope of entities covered by the policy rule (eg a specific Amazon S3 bucket or Amazon EC2 instance, or * which means any resource).

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

11.Close **X** the **Show Policy** window.

12.In the navigation pane on the left, click **Groups**.

13.Click the **S3-Support** group.

14.Below the **Actions** menu, click the **Show Policy** link.

This policy has permissions to Get and List resources in Amazon S3.

15.Close × the Show Policy window.

16.In the navigation pane on the left, click **Groups**.

17.Click the **EC2-Admin** group.

This Group is slightly different from the other two. Instead of a Managed Policy, it has an **Inline Policy**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.

18.Under **Actions**, click **Show Policy** to view the policy.

This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.

19.At the bottom of the screen, click **Cancel** to close the policy.

❖ BUSINESS SCENARIO

For the remainder of this lab, you will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many Amazon EC2 instances and a great deal of Amazon **S3** storage. You wish to give access to new staff depending upon their job function:

USER	IN GROUP	PERMISSIONS
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

❖ TASK 2: ADD USERS TO GROUPS

You have recently hired user-1 into a role where they will provide support for Amazon S3. You will add them to the S3-Support group so that they inherit the necessary permissions via the attached AmazonS3ReadOnlyAccess policy.

You can ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

❖ ADD USER-1 TO THE S3-SUPPORT GROUP

1.In the left navigation pane, click **Groups**.

2.Click the **S3-Support** group.

3.Click the **Users** tab.

4.In the **Users** tab, click **Add Users to Group**.

5.In the **Add Users to Group** window, configure the following:

- Select **user-1**.
- At the bottom of the screen, click **Add Users**.

In the **Users** tab you will see that **user-1** has been added to the **Group**.

❖ ADD USER-2 TO THE EC2-SUPPORT GROUP

1.You have hired **user-2** into a role where they will provide support for **Amazon EC2**.

2.Using similar steps to the ones above, add **user-2** to the **EC2-Support group**.

user-2 should now be part of the **EC2-Support group**.

❖ ADD USER-3 TO THE EC2-ADMIN GROUP

1.You have hired **user-3** as your **Amazon EC2** administrator, who manage your **EC2** instances.

Using similar steps to the ones above, add **user-3** to the **EC2-Admin group**.

2.**user-3** should now be part of the **EC2-Admin group**.

3.In the navigation pane on the left, click **Groups**.

Each Group should have one in the Users column for the number of Users in each Group. If you do not have one beside each group, revisit the above instructions above to ensure that each user is assigned to a Group, as shown in the table in the Business Scenario section.

❖ TASK 3: SIGN-IN AND TEST USERS

1.In this task, you will test the permissions of each **IAM** User.

In the navigation pane on the left, click **Dashboard**.

2.An **IAM users sign-in link** is displayed It will look similar to:

https://123456789012.signin.aws.amazon.com/console

This link can be used to sign-in to the AWS Account you are currently using.

3.Copy the **IAM users sign-in link** to a text editor.

Open a private window.

MOZILLA FIREFOX

- Click the menu bars at the top-right of the screen
- Select New **Private Window**

GOOGLE CHROME

- Click the ellipsis; at the top-right of the screen
- Click New **incognito** window

MICROSOFT EDGE

- Click the ellipsis at the top-right of the screen
- Click New **InPrivate** window

MICROSOFT INTERNET EXPLORER

- Click the **Tools** menu option
- Click **InPrivate** Browsing

4.Paste the **IAM** users sign-in link into your private window and press **Enter**.

You will now sign-in as **user-1**, who has been hired as your **Amazon S3** storage support staff.

5.Sign-in with:

- **IAM user name:** `user-1`
- **Password:** `Lab-Password1`

6.In the **Services** menu, click **S3**.

Click the name of one of your buckets and browse the contents.

Since your user is part of the **S3-Support Group** in **IAM**, they have permission to view a list of Amazon **S3** buckets and their contents.

Now, test whether they have access to **Amazon EC2**.

7.In the **Services** menu, click **EC2**.

8.In the left navigation pane, click **Instances**.

You cannot see any instances! Instead, it says You do not have any instances in this region. This is because your user has not been assigned any permissions to use **Amazon EC2**.

You will now sign-in as **user-2**, who has been hired as your **Amazon EC2** support person.

9.Sign **user-1** out of the AWS Management Console by configuring the following:

- At the top of the screen, click **user-1**
- Click **Sign Out**

10**.**Paste the **IAM users sign-in link** into your **private window** and press **Enter**.

11.Paste the sign-in link into the address bar of your private web browser tab again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

12. Sign-in with:

- **IAM user name:** `user –3`
- **Password:** `Lab–Password3`

13.In the **Services** menu, choose **EC2**.

14. In the navigation pane on the left, choose **Instances**.

As an **EC2** Administrator, you should now have permissions to Stop the **Amazon EC2 instance.**

Select the instance named `LobHost`.

If you cannot see an **Amazon EC2 instance**, then your Region may be incorrect. in the top-right of the screen, pull-down the Region menu and select the region that you noted at the start of the lab (for example, N. Virginia).

15.. In the **Instance** state menu, choose **Stop instance**.

16.. In the **Stop instance** window, choose **Stop**.

The **instance** will enter the stopping state and will **shutdown**.

17. Close your **private browser** window.

LAB COMPLETE 

5. OUTPUT SCREENS

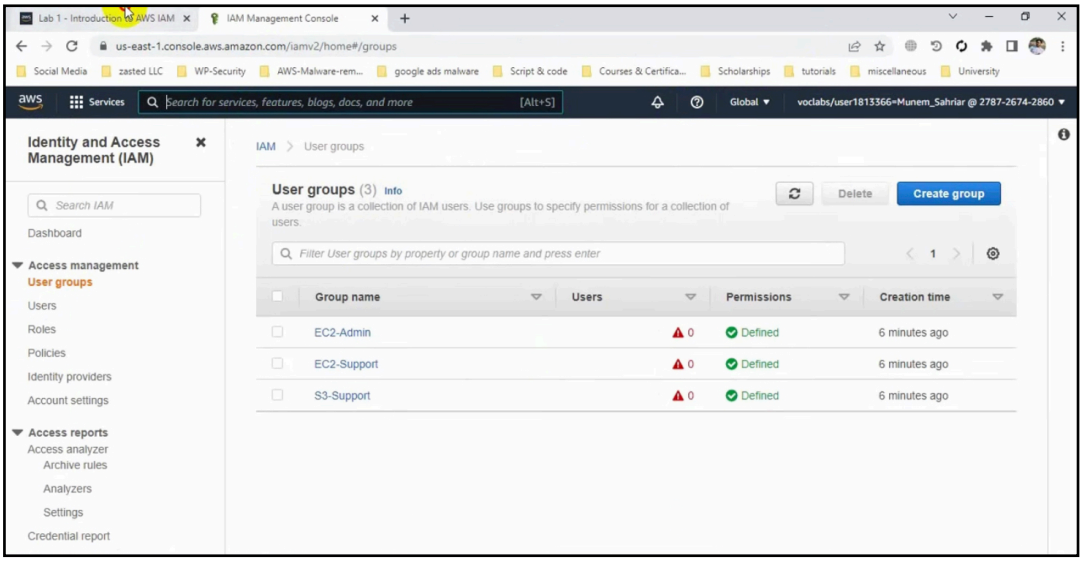


FIG 5.1

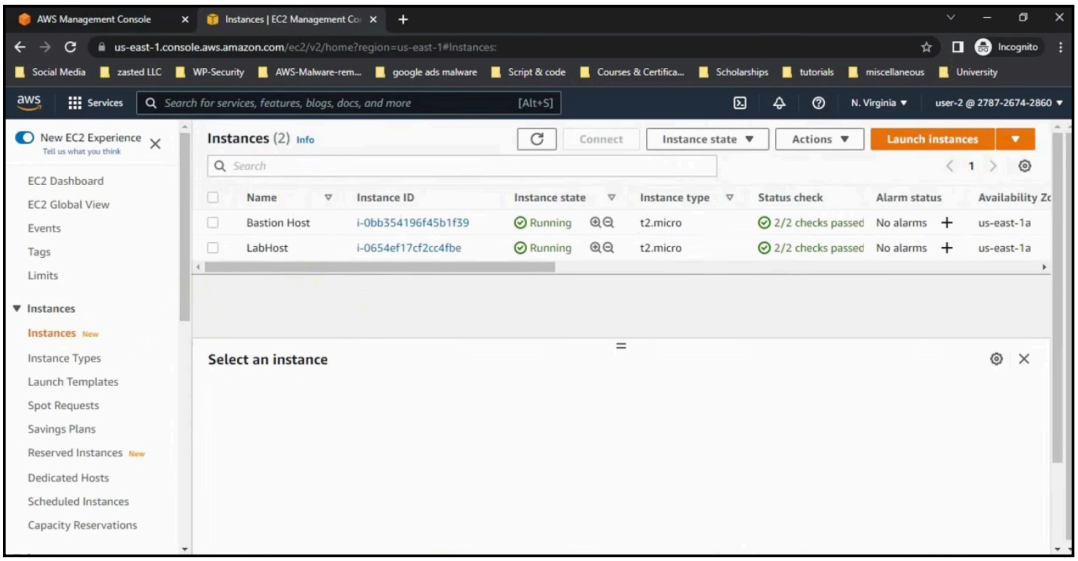


FIG 5.2

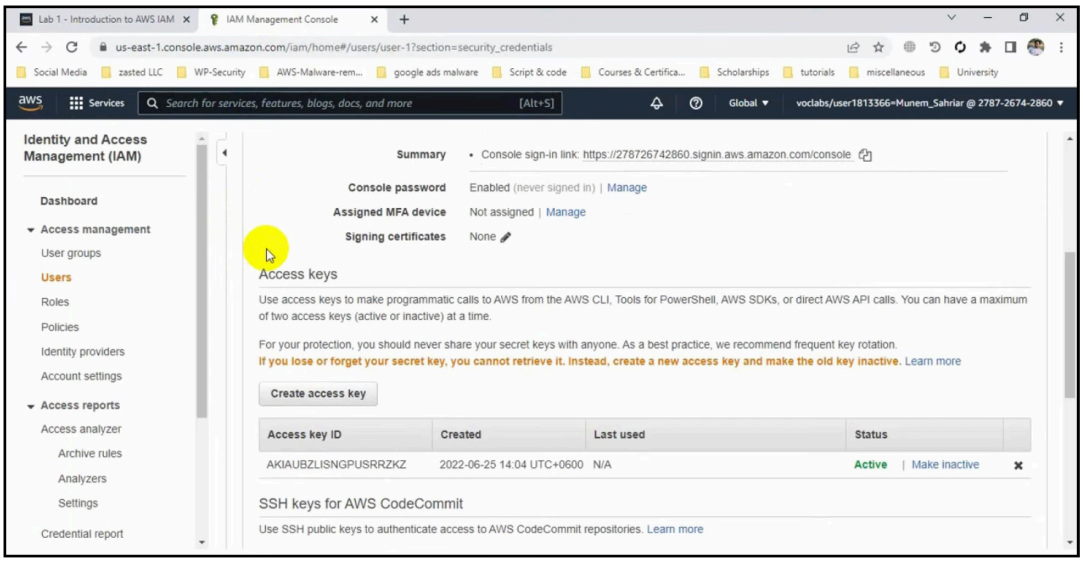


FIG 5.3

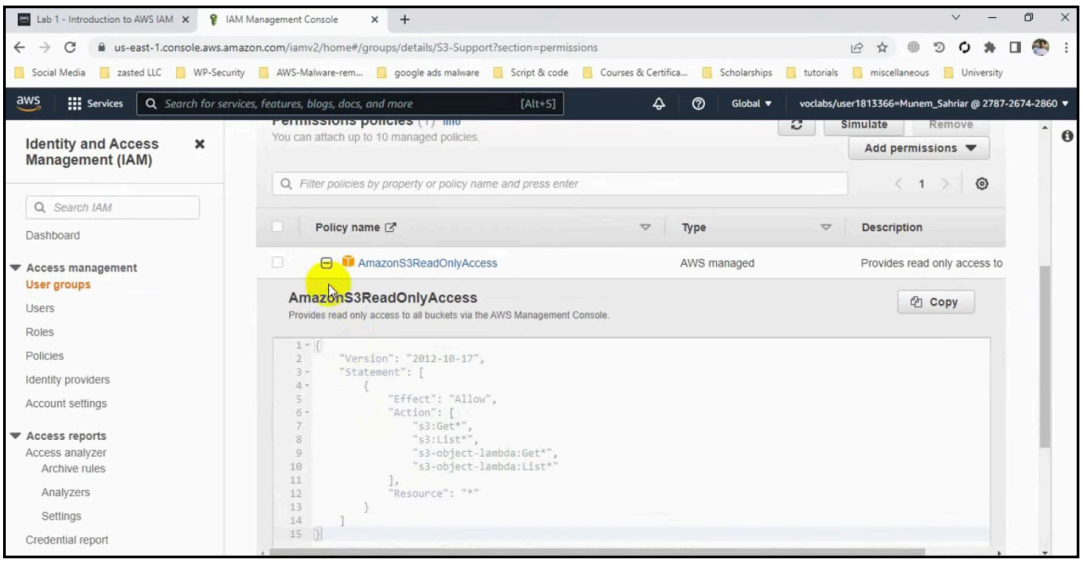


FIG 5.4

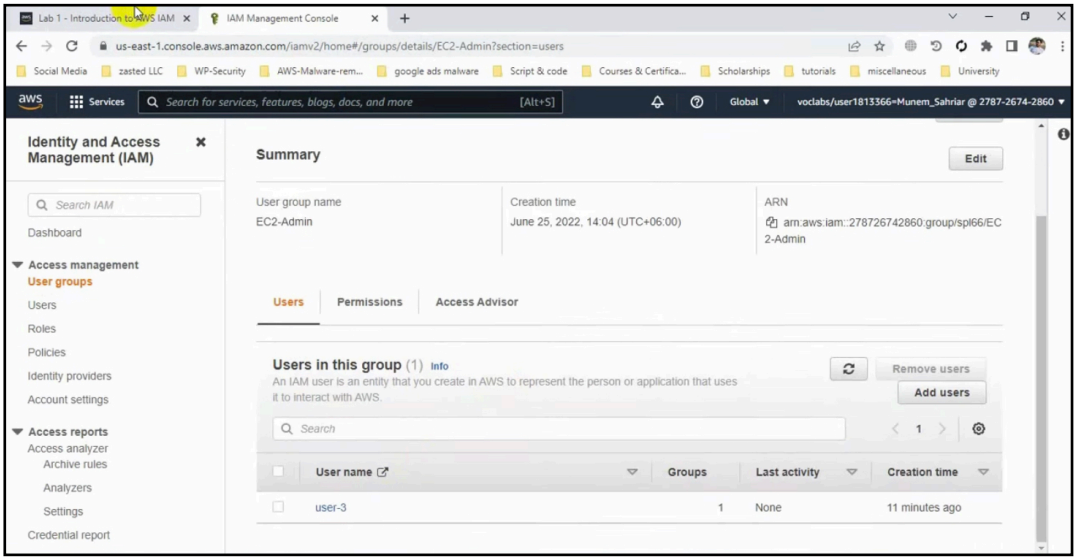


FIG 5.5

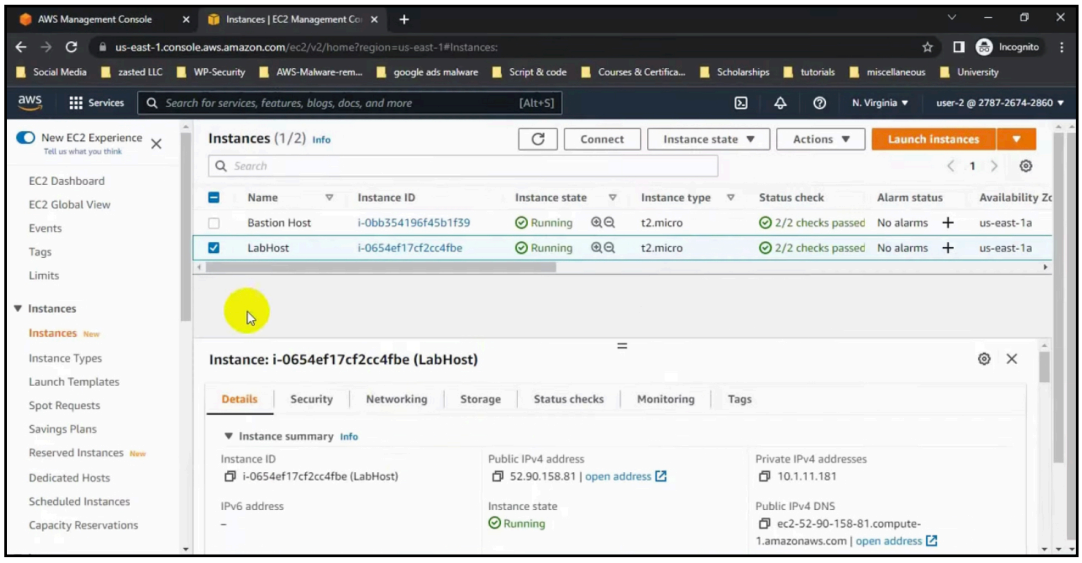


FIG 5.6

6. INTERNSHIP FEEDBACK

6.1 CHALLENGES FACED

It was a good experience performing all the lab activities and also referring the keen power point presentations provided . Also it was a new experience for us to enhance your skills by using all the applications provided in the internship. we have got hands-on experience to use each and every tool in AWS platform by performing various lab activities . The guided labs were the building blocks which are to be learnt to perform the challenging labs which were really challenging and compact.

7.CONCLUSION

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 centre's 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.

8.FUTURE SCOPE

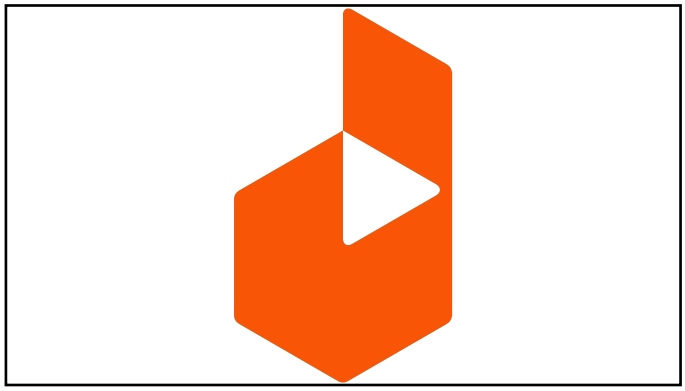
There is no doubt that cloud services have grown at a stupendous rate in the last decade as it promises a lot of flexibility to organizations and individuals. In today’s market, the scope of cloud security is just great.Earlier organizations used to store/host all the data on their own storage devices and servers(we call this on-premise). To be able to do this, one needs to buy storage devices and servers whenever they are needed. However, the cloud is more flexible, you need to pay only for the services which you use for a given period of time.When more and more organizations are switching to cloud and putting their data on cloud platforms, the security of cloud services becomes more and more important. This is where cloud security comes into the picture.

9.CASE STUDIES

DARAZ which is which is one of the leading online shopping stores in sub-continent says that their customer satisfaction level has increased by 26% by using AWS.In 2016, on the busiest day of the year Black Frida a disaster happened all of the servers of Daraz crashed and its mobile application became extremely slow due to system workload. Daraz was basically relying on a Portugal company for its data management and their infrastructure was not strong enough to carry such loads and thus system became vulnerable to hackers a lot goods were stolen and customers cards were hijacked while the transfer of money was taking place. The personal information of some the customers. When the report came out the managers decided to give service to AWS before the next sale. Daraz uses Amazon Elastic Compute Cloud (Amazon EC2) for all kinds of workloads. Elastic Load Balancing (ELB) is also deployed to efficiently distribute the incoming traffic. Daraz has simplified its daily working routine by using Amazon Relational Database Service (Amazon RDS).

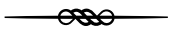
As Daraz is a customer-oriented company so its major concern is to satisfy its customers at all costs. Before adopting AWS, the order inquiry calls were manually answered, and it took a lot of time but after the implementation of AWS these types of calls were automated with the help of chatbots thus resulting in increased productivity.

Mr. Umair CEO of Daraz says that after adopting AWS their workload is reduced to a great extent now he is able to handle the whole IT operation with a team of just 8 engineers because they do not have to take care of the normal routine tasks. He further says that the support provided by AWS was unmatched in the beginning when they did not have proper AWS training they faced some issues and when they contacted Amazon team they were kind enough to respond quickly and resolve the problem in no time. Once Daraz had to spend almost a week to identify a problem but they were not able to do so, they contacted Amazon and their team was not only able to identify the problem but were also able to solve it.



BIBLIOGRAPHY

- https://www.researchgate net/publication/348237177_Security_with_AWS.
- Cloud Computing Security: Amazon Web Service Publisher: IEEE.
- Herbert Schildt, The Complete Reference Java2 Fifth Edition, Tata McGraw-Hill Edition 2002.
- WIKIPEDIA .
- GOOGLE.
- IEEE.
- RESEARCH GATE.



APPENDIX-A:JAVA TECHNOLOGY

❖ JAVA:

Initially the language was called as "**oak**" but it was renamed as "**java**" in 1995.The primary motivation of this language was the need for a platform-independent language that could be used to create software to be embedded in various consumer electronic devices.

- Java is a programmer's language.
- Java is cohesive and consistent.
- Except for those constraint imposed by the Internet environment. Java gives the programmer full control.

❖ SERVLETS/JSP:

A Servlet Is a generic server extension. a Java class that can be loaded dynamically to expand the functionality of a server. Servlets are commonly used with web servers. Where they can take the place CGI scripts.A servlet is similar to proprietary server extension, except that it runs inside a Java Virtual Machine (JVM) on the server, so it is safe and portable .Servlets operate solely within the domain of the server.

❖ FEATURES OF SERVLETS:

- Servlets are persistent.Servlet are loaded only by the web server and can maintain services between requests.
- Servlets are fast. Since servlets only need to be loaded once, they offer much better performance over their CGI counterparts.
- Servlets are platform independent.
- Servlets are extensible Java is a robust, object-oriented programming language,
- which easily can be extended to suit your needs.
- Servlets are secure
- Servlets are used with a variety of client.

❖ INVOKING SERVLETS:

A servlet invoker is a servlet that invokes the "server" method on a named servlet.If the servlet is not loaded in the server then the invoker first loads the servlet(either form local disk or from the network) and the then invokes the "service" method.Also like applets local servlets in the server can be identified by just the class name.In other words, if a servlet name is not absolute.it is treated as local.

A Client can Invoke Servlets in the Following Ways:

- The client can ask for a document that is served by the servlet.
- The client(browser) can invoke the servlet directly using a URL, once it has been mapped using the SERVLET ALIASES Section of the admin GUI.
- The servlet can be invoked through server side include tags.
- The servlet can be invoked by placing it in the servlets/directory.

❖ THE SERVLET LIFE CYCLE:

The Servlet life cycle is one of the most exciting features of Servlets.This life cycle is a powerful hybrid of the life cycles used in CGI programming and lower-level NSAPI and ISAPI programming. The servlet life cycle allows servlet engines to address both the performance and resource problems of CGI and the security contents of low level server API programming.Servlet life cycle is highly flexible Servers java significant leeway in how they choose to support servlets.The only hard and fast rule is that a servlet engine must conform to the following life cycle contact:

- Create and initialize the servlets
- Handle zero or more service from clients
- Destroy the servlet and then garbage Collects it.

It's perfectly legal for a servlet to be loaded, created and initialzed in its own to be destroyed and garbage collected without handling any client request or after handling just one request.

❖ INIT AND DESTROY:

Just like Applets servlets can define init() and destroy() methods, A servlets init(ServiceConfig) method is called by the server immediately after the server constructs the servlet's instance. Depending on the server and its configuration, this can be at any of these times

- When the server states
- When the servlet is first requested, just before the service method is invoked
- At the request of the server administrator.

In any case, init() is guaranteed to be called before the servlet handles its first request. The init() method is typically used to perform servlet initialization creating or loading objects that are used by the servlet in handling of its request.

In order to providing a new servlet any information about itself and its environment, a server has to call a servelts init() method and pass an object that implement the Servlet Config interface.This ServletConfig object supplies a servlet with information about its initialization parameters.These parameters are given to the servlets and are not associated with any single request.They can specify initial values, such as where a counter should begin counting, or default values, perhaps a template to use when not specified by the request.

The server calls a servlet's destroy() method when the servlet is about to be unloaded. In the destroy() method, a servlet should free any resources it has acquired that will not be garbage collected. The destroy() method also gives a servlet a chance to write out its unsaved. cached information or any persistent information that should be read during the next call to init().

❖ SESSION TRACKING:

HTTP is a stateless protocol, it provides no way for a server to recognize that sequence of requests is all from the same client. The solution for this is for client to introduce itself as it makes each request, Each clients needs to provide a unique identifier that lets the server identify it, or it needs to give some information that the server can use to properly handle the request, There are several ways to send this introductory information with each request such as:

❖ USER AUTHENTICATION:

One way to perform session tracking is to leverage the information that comes with user authorization. When a web server restricts access to some of its resources to only those clients that log in using a recognized username and password. After the client logs in, the username is available to a servlet through getRemoteUser(). The biggest advantage of using user authorization to perform session tracking is that it's easy to implement and easy to identify each client.Another advantage is that the technique works even when the user accesses your site form or exists her browser before coming back.

❖ HIDDEN FORM FIELDS:

One way to support anonymous session tracking is to use hidden from fields. As the name implies, these are fields added to an HTML, form that are not displayed in the client's browser, They are sent back to the server when the form that contains them is submitted.

In a sense, hidden form fields define constant variables for a form. To a servlet receiving a submitted form, there is no difference between a hidden fields and a visible filed.

As more and more information is associated with a clients session . It can become burdensome to pass it all using hidden form fields. In these situations it's possible to pass on just a unique session ID that identifies as particular clients session.That session ID can be associated with complete information about its session that is stored on the server.

- The **advantage** of hidden form fields is their ubiquity and support for anonymity. Hidden fields are supported in all the popular browsers, they demand on special server requirements and they can be used with clients that haven't registered or logged in.
- The major **disadvantage** with this technique, however is that works only for a sequence of dynamically generated forms, The technique breaks down immediately with static documents emailed documents book marked documents and browser shutdowns.

❖ URL REWRITING:

URL rewriting is another way to support anonymous session tracking, With URL rewriting every local URL the user might click on is dynamically modified. or rewritten, to include extra information. The extra information can be in the deform of extra path information, added parameters, or some custom, server-specific.URL change. Due to the limited space available in rewriting a URL, the extra information is usually limited to a unique session. Each rewriting technique has its own advantage and disadvantage. Using extra path information works on all servers, and it works as a target for forms that use both the Get and Post methods. It does not work well if the servlet has to use the extra path information as true path information

- The **advantages** and **disadvantages** of URL rewriting closely match those of hidden form fields. The major difference is that URL rewriting works for all dynamically created documents, such as the Help servlet, not just forms. With the right server support, custom URL rewriting can even work for static documents.

❖ PERSISTENT COOKIES:

A fourth technique to perform session tracking involves persistent cookies. A cookie is a bit of information sent by a web server to a browser that can later be read back form that browser When a browser receives a cookie, it saves the cookie and there after sends the cookie back to the server each time it accesses a page on that server, subject to certain rules. Because a cookie's value can uniquely identify a client, cookies are often used for session tracking Persistent cookies offer an elegant, efficient easy way to implement session tracking. Cookies provide as automatic an introduction for each request as we could hope for.

For each request, a cookie can automatically provide a client's session ID or perhaps a list of clients performance. The ability to customize cookies gives them extra power and versatility.

❖ JDBC:

JDBC is a Java **API** for executing **SQL** Statements.As a point of interest **JDBC** is trademarked name and is not an acronym nevertheless **JDBC** is often thought of as standing for Java Database Connectivity. It consists of a set of classes and interfaces written in the Java Programming language **JDBC** provides a standard **API** fortool database developers and makes it possible to write database applications using a pure Java **API**.

Using **JDBC**, it is easy to send **SQL** statements to virtually program will be able to send SQL statements to the appropriate database. The Combination of Java and **JDBC** lets a programmer write it once and run it anywhere and **JDBC** Does the Following:

- Establish a connection with a database.
- Send **SQL** statements.
- Process the results.
- **JDBC** Driver Types

An individual database system is accessed via a specific **JDBC** driver that implements the java.sql.Driver interface. Drivers exist for nearly all-popular **RDBMS** systems, through few are available for free. Sun bundles a free **JDBC-ODBC** bridge driver with the **JDK** to allow access to a standard **ODBC** data sources, such as a Microsoft Access database such advises against using the bridge driver for anything other than development and very limited development. **JDBC** drivers are available for most database platforms, from a number of vendors and in a number of different flavours. There are four driver categories:

❖ TYPE 01-JDBC-ODBC BRIDGE DRIVER:

Type-01 drivers use a bridge technology to connect a java client to an **ODBC** database service. Sun's **JDBC-ODBC** bridge is the most common Type-01 driver. These drivers implemented using native code.

❖ TYPE 02-NATIVE-API PARTY-JAVA DRIVER:

Type-02 drivers wrap a thin layer of java around database-specific native code libraries for Oracle databases, the native code libraries might be based on the **OCI**(Oracle call Interface) libraries, which were originally designed for **C/C++** programmers, Because Type- 02 drivers are implemented using native code, in some cases they have better performance than their all- java counter parts. They add an element of risk, however, because a defect in a driver's native code section can crash the entire server

❖ TYPE-03-NET-PROTOCOL ALL-JAVA DRIVER:

Type-03 drivers communicate via a generic network protocol to a piece of custom middleware.The middleware component might use any type of driver to provide the actual database access. These drivers are all java, which makes them useful for applet deployment and safe for servlet deployment.

❖ TYPE-04-NATIVE-PROTOCOL ALL-JAVA DRIVER:

Type-04 drivers are the most direct of the lot. Written entirely in java, Type-04 drivers understand database-specific networking. protocols and can access the database directly without any additional software.

❖ ORACLE:

Oracle is a relational database management system, which organizes data in the form of tables. Oracle is one of many database servers based on RDBMS model, which manages a seer of data that attends three specific things-data structures, data integrity and data manipulation. With oracle cooperative server technology we can realize the benefits of open relational systems for all the applications. Oracle makes efficient use of all systems resources on all hardware architecture; to deliver unmatched performance, price performance and scalability. Any DBMS to be called as RDBMS has to satisfy Dr.E.F.Codd's rules.

❖ FEATURES OF ORACLE:

▸ PORTABLE;

The Oracle RDBMS is available on wide range of platforms ranging from PCs to super computers and as a multi user loadable module for Novel NetWare, if you develop application on system you can run the same application on other systems without any modifications.

▸ COMPATIBLE:

Oracle commands can be used for communicating with IBM DB2 mainframe RDBMS that is different from Oracle, which is Oracle compatible with DB2. Oracle RDBMSis a high performance fault tolerant DBMS, which is specially designed for online transaction processing and for handling large database applications.

▸ MULTITHREADED SERVER ARCHITECTURE:

Oracle adaptable multithreaded server architecture delivers scalable high performance for very large number of users on all hardware architecture including symmetric multiprocessors (sumps) and loosely coupled multiprocessors.

Performance is achieved by eliminating CPU, I/O, memory and operating system bottlenecks and by optimizing the Oracle DBMS server code to eliminate all internal bottlenecks.

Oracle has become the most popular RDBMS in the market because of its ease of use

- Client/server architecture.
- Data independence.
- Ensuring data integrity and data security.
- Managing data concurrency.
- Parallel processing support for speed up data entry and online transaction processing used for applications.
- DB procedures, functions and packages.

❖ HTML:

Hypertext Markup Language(HTML) the languages of the world wide web(WWW) allows users to produces web pages that included text, graphics and pointer to other web pages (Hyperlinks).HTML is not a programming language but it is an application of ISO Standard 8879,SGML(Standard Generalized Markup Language),but specialized to hypertext and adapted to the Web. We can navigate through the information based on out interest and preference. A markup language is simply a series of items enclosed within the elements should be displayed.Hyperlinks are underlined or emphasized works that load to other documents or some portions of the same document.HTML can be used to display any type of document on the host computer, which can be geographically at a different location. It is a versatile language and can be used on any platform or desktop.HTML provides tags(special codes) to make the document look attractive.HTML provides are not case sensitive. Using graphics,fonts,different sizes, colour, etc.. can enhance the presentation of the document. Anything that is not a tag is part of the document itself.

❖ BASIC HTML TAGS:

TAGS	OPERATIONS
<!-- -->	**Specific Comments.**
<A>.....</A>	**Creates Hypertext links.**
<B>.....</B>	**Text is changed to bold**
<Body>.....</Body>	**Contains all tags and text in the Html-document**
<DD>.....</DD>	**Definition of a term.**

TAGS	OPERATIONS
<TABLE>.....<TABLE>	Creates table
<Td>.....</Td>	Indicates table data in a table.
<Tr>.....</Tr>	Designates a table row
<Th>.....</Th>	Creates a heading in a table.

❖ **ADVANTAGES**:

- A HTML document is small and hence easy to send over the net.It is small because it does not include formatted information.
- HTML is platform independent.
- HTML tags are not case-sensitive.

❖ **JAVA SCRIPT:**

JavaScript is a compact , object-based scripting language for developing client and server internet applications. Netscape Navigator 2.0 interprets JavaScript statements embedded directly in an HTML page. and Liveware enables you to create server-based applications similar to common gateway interface(CGI) programs.In a client application for Navigator JavaScript statements embedded in an HTML page can recognize and respond to user events such as mouse clicks form Input, and page navigation.For example, you can write a JavaScript function to verify that users enter valid information into a form requesting a telephone number or zip code . Without any network transmission, an HTML page with embedded Java Script can interpret the entered text and alert the user with a message dialog if the input is invalid or you can use JavaScript to perform an action (such as play an audio file execute an applet, or communicate with a plug-in) in response to the user opening or exiting a page.

APPENDIX-B:UNIFIED MODELING LANGUAGE

The Unified Modeling Language (UML) is a general-purpose visual modeling language that is used to specify, visualize, construct, and document the artifacts of a software system. It captures decisions and understanding about systems that must be constructed. It is used to understand, design, browse, configure, maintain, and control information about such systems. It is intended for use with all development methods, lifecycle stages, application domains, and media. The modeling language is intended to unify past experience about modeling techniques and to incorporate current software best practices into a standard approach.

UML includes semantic concepts, notation, and guidelines. It has static, dynamic environmental, and organizational parts. It is intended to be supported by interactive visual modeling tools that have code generators and report writers. The UML specification does not define a standard process but is intended to be useful with an iterative development process. It is intended to support most existing object oriented development processes.

The UML captures information about the static structure and dynamic behaviour of a system. A system is modelled as a collection of discrete objects that interact to perform work that ultimately benefits an outside user. The static structure defines the kinds of objects important to a system and to its implementation, as well as the relationships among the objects. The dynamic behaviour defines the history of objects over time and the communications among objects to accomplish goals.

Modeling a system from several separate but related viewpoints permits it to be understood for different purposes.The UML also contains organizational constructs for arranging models into packages that permit software teams to partition large systems into workable pieces, to understand and control dependencies among the packages, and to manage the versioning of model units in a complex development environment. It contains constructs for representing implementation decisions and for organizing run-time elements into components.

UML is not a programming language. Tools can provide code generators from UML into a variety of programming languages, as well as construct reverse engineered models from existing programs. The UML is not a highly formal language intended for theorem proving There are a number of such languages, but they are not easy to understand or to use for most purposes. The UML is a general-purpose modeling language. For specialized domains, such as GUI layout, VLSI circuit design, or rule-based artificial intelligence, a more specialized tool with a special language might be appropriate. UML is a discrete modeling language.It is not intended to model continuous systems such as those found in engineering and physics UML is intended to be a universal general-purpose modeling language for discrete systems such as those made of software, firmware, or digital logic.

APPENDIX C: ABSTRACT

Sreenidhi Institute of Science and Technology
Department of Electronics and Communication Engineering
Summer Industry Internship-1

BATCH NO:		
ROLL NO	**NAME**	**TITLE**
20311A0460	**KOMMURI SAITEJA**	**AWS CLOUD SECURITY**
20311A0458	**NAREDLA SAI CHARAN**	
20311A0455	**GATLA ABHISHEK**	

Security is the highest priority at Amazon Web Services (AWS). AWS delivers a scalable cloud computing environment that is designed for high availability and dependability, while providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is critical to AWS, and so is maintaining customer trust and confidence. This module provides an introduction to the AWS approach to security, which includes both the controls in the AWS environment and some of the AWS products and features customers can use to meet their security objectives. Security and compliance are a shared responsibility between AWS and the customer. This shared responsibility model is designed to help relieve the customer's operational burden. At the same time, to provide the flexibility and customer control that enables the deployment of customer solutions on AWS, the customer remains responsible for some aspects of the overall security. The differentiation of who is responsible for what is commonly referred to as security "of" the cloud versus security "in" the cloud. 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 centre's 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.

STUDENT-1:KOMMURI SAITEJA
STUDENT-2:NAREDLA SAI CHARAN
STUDENT-3:GATLA ABHISHEK

Project Coordinator
Mr.Chenchu Sreedhar Kakarla
Assistant Professor
CSE Department

Dr.S.P.V Subba Rao
Professor
HOD,ECE DEPARTMENT

APPENDIX-D: CORRELATION BETWEEN THE SUMMER INDUSTRY INTERNSHIP-I AND THE PROGRAM OUTCOMES (PO's), PROGRAM SPECIFIC OUTCOMES (PSO's)

BATCH NO:		
ROLL NO	**NAME**	**TITLE**
20311A0460	KOMMURI SAITEJA	AWS CLOUD SECURITY
20311A0458	NAREDLA SAI CHARAN	
20311A0455	GATLA ABHISHEK	

Table 1: Project/Internship correlation with appropriate POs/PSOs (Please specify level of Correlation, H/M/L against POs/PSOs)

H	HIGH	M	MODERATE	L	LOW

Sreenidhi Institute of Science and Technology

Department of Electronics and Communication Engineering

Projects Correlation with PO's/PSO's

PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8	PO-9	PO-10	PO-11	PO-12	PSO-1	PSO-2	PSO-3
M	L	L	H	H	L	M	H	M	H	H	H	H	H	M

STUDENT-1:KOMMURI SAITEJA

STUDENT-2:NAREDLA SAI CHARAN

STUDENT-3:GATLA ABHISHEK

Project Coordinator
Mr.Chenchu Sreedhar Kakarla
Assistant Professor
CSE Department

Dr.S.P.V Subba Rao
Professor
HOD,ECE DEPARTMENT

APPENDIX-E: DOMAIN OF INTERNSHIP AND NATURE OF INTERNSHIP

BATCH NO:		
ROLL NO	**NAME**	**TITLE**
20311A0460	KOMMURI SAITEJA	AWS CLOUD SECURITY
20311A0458	NAREDLA SAI CHARAN	
20311A0455	GATLA ABHISHEK	

Table 2: Nature of the Project/Internship work (Please tick ✓ Appropriate for your project)

BATCH.NO	TITLE	NATURE OF PROJECT			
	AWS CLOUD SECURITY	PRODUCT	APPLICATION	RESEARCH	OTHERS
				✓	

STUDENT-1:KOMMURI SAITEJA

STUDENT-2:NAREDLA SAI CHARAN

STUDENT-3:GATLA ABHISHEK

Project Coordinator
Mr.Chenchu Sreedhar Kakarla
Assistant Professor
CSE Department

Dr.S.P.V Subba Rao
Professor
HOD,ECE DEPARTMENT

Table 3: Domain of the Project/ Internship work (Please tick ✓ Appropriate for your project)

BATCH.NO	TITLE	DOMAIN OF THE PROJECT			
	AWS CLOUD SECURITY	AI & ML	CYBER SECURITY	IMAGE PROCESSING	CLOUD FOUNDATIONS
					✓

STUDENT-1:KOMMURI SAITEJA

STUDENT-2:NAREDLA SAI CHARAN

STUDENT-3:GATLA ABHISHEK

Project Coordinator
Mr.Chenchu Sreedhar Kakarla
Assistant Professor
CSE Department

Dr.S.P.V Subba Rao
Professor
HOD,ECE DEPARTMENT