DR. D.Y. PATIL INSTITUTE OF TECHNOLOGY, PUNE

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

LAB MANUAL

Mini Project
Subject Code: 317536

Prepared By:
Disha Sengupta
Apurva Kandelkar

DR. D.Y. PATIL INSTITUTE OF TECHNOLOGY, PUNE

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

Lab Manual

Third Year Engineering

Semester-VI

Cyber Security

Subject Code: 317536

Class: TE AI&DS

Academic Year 2024-25

Software Laboratory III
Subject Code: 317534

TeachingScheme	Credit	ExaminationScheme
PR: 02 Hours/Week	01	OR: 25 Marks TW: 50Marks

Guidelines for Instructor's Manual

The instructor‘s manual is to be developed as a reference and hands-on resource. It should include prologue (about University/program/ institute/ department/foreword/ preface), curriculum of the course, conduction and Assessment guidelines, topics under consideration, concept, objectives, outcomes, set of typical applications/assignments/ guidelines, and references

Guidelines for Student Journal

The laboratory assignments are to be submitted by student in the form of journal. Journal consists of Certificate, table of contents, and handwritten write-up of each assignment (Title, Date of Completion, Objectives, Problem Statement, Software and Hardware requirements, Assessment grade/marks and assessor's sign, Theory- Concept in brief, algorithm, flowchart, test cases, Test Data Set(if applicable), mathematical model (if applicable), conclusion/analysis. Program codes with sample output of all performed assignments are to be submitted as softcopy. As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal must be avoided. Use of DVD containing students programs maintained by Laboratory In-charge is highly encouraged. For reference one or two journals may be maintained with program prints in the Laboratory.

Guidelines for Laboratory /Term Work Assessment

Continuous assessment of laboratory work should be based on overall performance of Laboratory assignments by a student. Each Laboratory assignment assessment will assign grade/marks based on parameters, such as timely completion, performance, innovation, efficient codes, and punctuality.

Guidelines for Practical Examination

Problem statements must be decided jointly by the internal examiner and external examiner. During practical assessment, maximum weightage should be given to satisfactory implementation of the problem statement. Relevant questions may be asked at the time of evaluation to test the student's understanding of the fundamentals, effective and efficient implementation. This will encourage, transparent evaluation and fair approach, and hence will not create any uncertainty or doubt in the minds of the students. So, adhering to these principles will consummate our team efforts to the promising start of student's academics.

Guidelines for Laboratory Conduction

The instructor is expected to frame the assignments by understanding the prerequisites, technological aspects, utility and recent trends related to the topic. The assignment framing policy need to address the average students and inclusive of an element to attract and promote the intelligent students. Use of open source software is encouraged. Based on the concepts learned. Instructor may also set one assignment or mini-project that is suitable to AI & DS branch beyond the scope of the syllabus.

Practical No.	Assignment to be covered
Part A Cyber Security	
1	Implementation of S-DES
2	Implementation of S-AES
3	Implementation of Diffie-Hellman key exchange
4	Implementation of RSA.
5	Implementation of ECC algorithm.
Part B : Elective II : Cloud Computing	
1	Setting up AWS Environment: Create a new AWS account, Secure the root user, Create an IAM user to use in the account Set up the AWS CLI, Set up a Cloud9 environment.
2	Setup, Create and visualize data in an Amazon Relational Database (Amazon RDS) MS SQL Express server using Amazon Quick Sight
3	Setup, Create and connect your Word Press site to an object storage bucket using Lightsail service.

ASSIGNMENT 1

PROBLEM STATEMENT: -
Implementation of S-DES

OBJECTIVE:

1. To understand how encryption takes place using S-DES algorithm which uses 3 different types of keys to encrypted.

PREREQUISITE: -

1 Basic of Python Programming

THEORY:

Simplified Data Encryption Standard (S-DES) is equivalent to the DES algorithm. The SDES encryption algorithm produces an 8-bit block of plaintext (example: 10111101) and a 10-bit key as input and makes an 8-bit block of cipher text as output. The S-DES decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key can develop that cipher text as input and makes the initial 8-bit block of plaintext.

These algorithms generate a key and thus encapsulate the message with this key. There are two types of encryptions: asymmetric and symmetric, which are in vogue.

Presentation Layer

The presentation layer in S-DES manages the translation, encryption/decryption, authentication and compression. These are explained below −

Translation

It can transform the complex data structures used by an application string, integers, structures, etc., into a byte flow that can be shared across the network. The message is defined so that communicating devices agree to the structure of the data being transformed. For instance, ASCII or EBCDIC character sets.

Encryption/Decryption

It can handle security and privacy issues. Encryption can scramble the information so that only authorized persons can unscramble the conversation information. Decryption shifts the encryption procedure to interpret the message back into its original form.

There are two types of Encryption which are as follows −

- Asymmetric Encryption − There are two numerically associated keys, such as the name public key and private keys that are created to encrypt and decrypt the message. Asymmetric encryption is considered more secure than symmetric encryption.
- Symmetric Encryption − Symmetric encryption is also defined as conventional or single key Encryption. It is based on a secret key, which both communicating parties share. The sending party encrypts the plain text to cipher text messages using the secret key. The receiving party on receipt of the ciphertext message uses a similar secret key to decrypt it to plain text.

Authentication

It can test the antecedents of the remote party being the real party instead of an impostor. It represents that the message is received from an authentic person, not from an impostor. A digital signature is one of the multiple authentication methods that use the public key encryption method.

Algorithm:

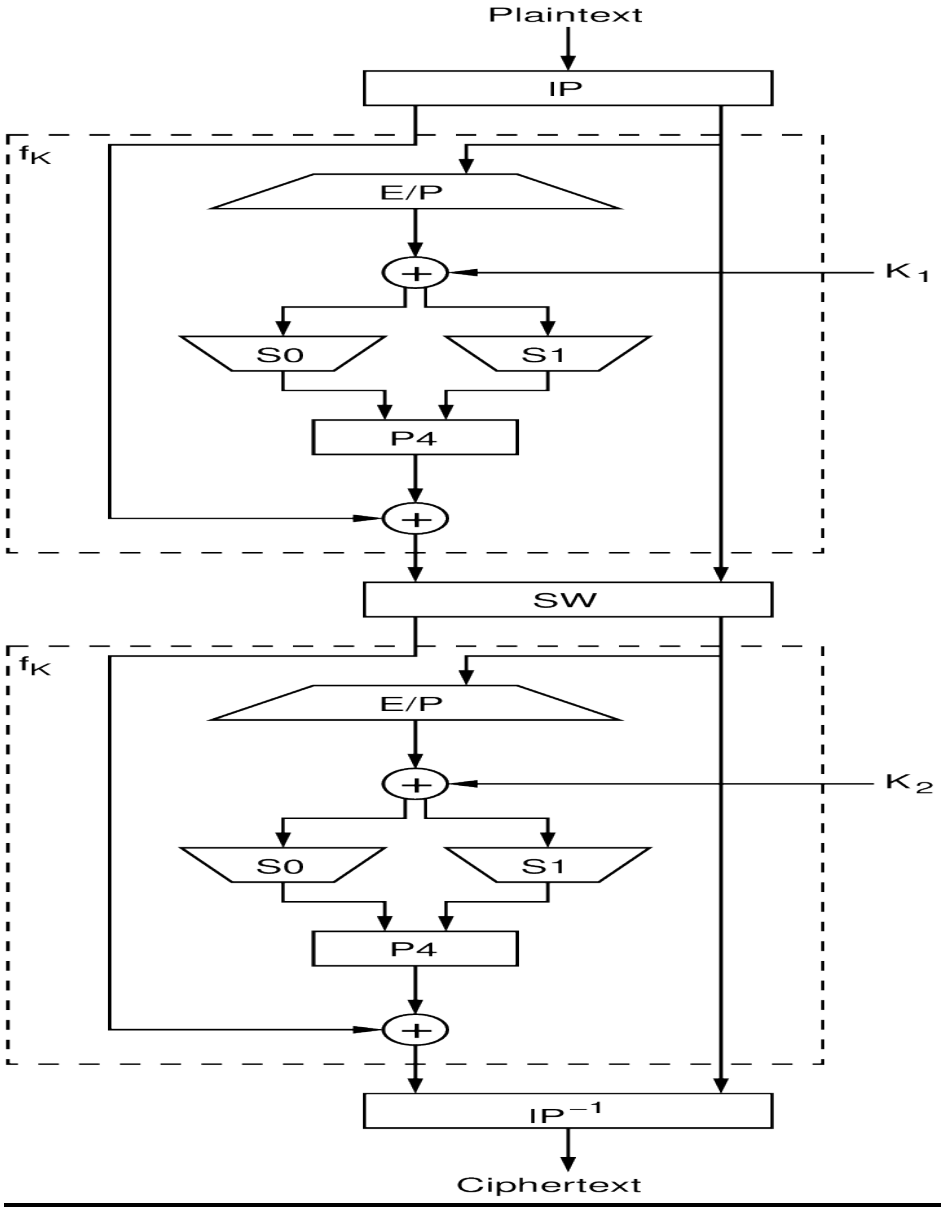
DES encrypts 64-bit blocks using a 56-bit key and produces 64-bit ciphertext through a series of steps.

S-DES or Simplified Data Encryption Standard is a simplified version of DES algorithm which is a block cipher that inputs 8-bit plaintext or ciphertext and uses 10-bit key for encryption and decryption. S-DES was designed for educational purposes only, to help students learn about modern cryptanalytic techniques. SDES has similar properties and structure as DES, but has been simplified to make it much easier to perform encryption and decryption by hand with pencil and paper.

The Encryption Processing of plaintext proceeds in 3 phases:-

1. First, the plaintext passes through an initial permutation (IP) that rearranges the bits to produce permutted output.
2. The permutted output is then passed through 16 rounds of both Permutation and Substitution functions. The left and right halves of output are swapped to produce the preoutput.
3. Finally, preoutput is passed through a permutation (IP-1) that is inverse of initial permutation function, to produce ciphertext.

The key is passed through a permutation function. Then a subkey is produced for each 16 rounds by combination of left circular swift and a permutation. The permutation function is the same for every round, but a different subkey is produced because of the repeated shifts of key bits.



CONCLUSION:

The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system.

ASSIGNMENT QUESTION

1. What is the key length of S-DES algorithm?
2. What is the difference between a block cipher and a stream cipher?
3. What is some common application of S-DES?
4. What happens when you use a weak key with DES?

ASSIGNMENT 2

PROBLEM STATEMENT: - Implementation of S-AES

OBJECTIVE:

1 To understand how encryption takes place using S-DES algorithm which uses 3 different types of keys to encrypted

PREREQUISITE: -

1. Basic of Python Programming

THEORY:

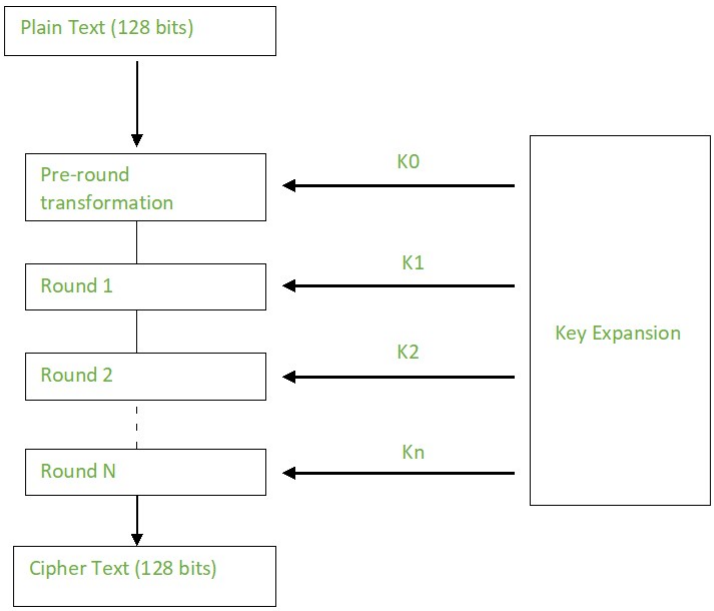
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows:

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Creation of Round keys:

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.



Algorithm:

Encryption:

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |

| b1 | b5 | b9 | b13 |

| b2 | b6 | b10| b14 |

| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes :

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]

| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |

| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |

[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

MixColumns:

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

[c0] [2 3 1 1] [b0]

| c1 | = | 1 2 3 1 | | b1 |

| c2 | | 1 1 2 3 | | b2 |

[c3] [3 1 1 2] [b3]

Add Round Keys:

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

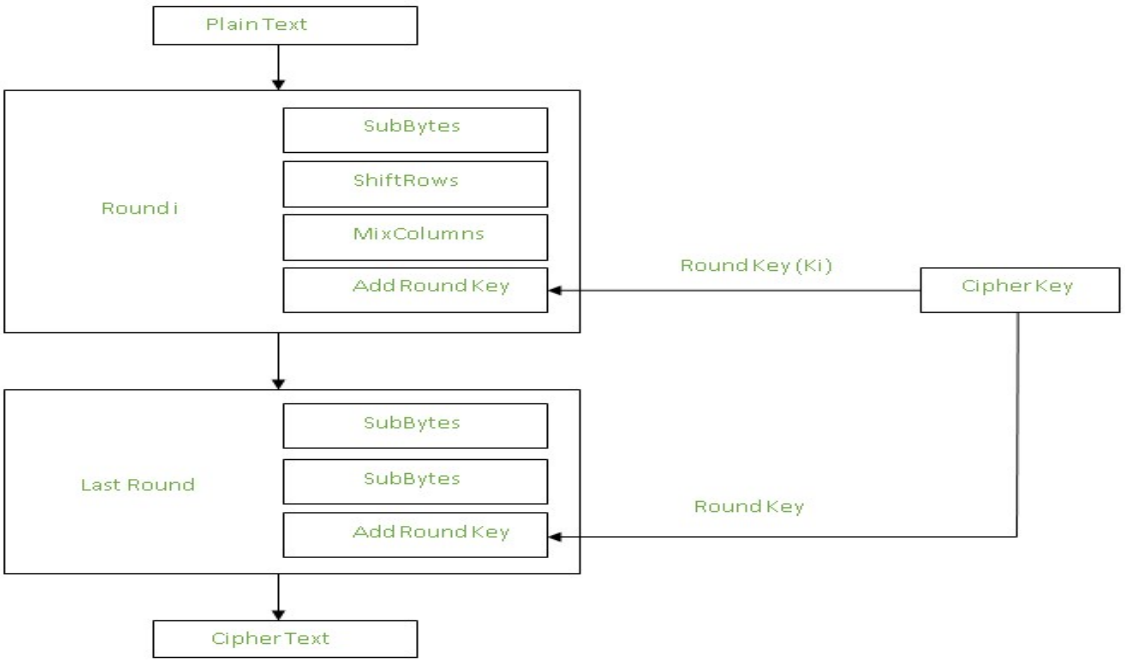
Decryption:

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.



Inverse MixColumns:

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

Applications:

AES is widely used for encryption in various applications and industries due to its strong security, efficiency, and versatility. Some common applications of AES encryption include: File, Database, and Standalone Encryption: AES is most often used to encrypt data at rest.

Conclusion:

AES is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Assignment Question:

1. Describe the process of AES key generation.
2. What are the main stages of the AES algorithm?
3. How does key expansion work in AES?
4. What differences exist between the three AES variants, AES-128, AES-192, and AES-256?

.

ASSIGNMENT 3

PROBLEM STATEMENT: -
Implementation of Diffie-Hellman key exchange

OBJECTIVE:

1. To analyze and demonstrate knowledge of Diffie-Hellman key exchange.

PREREQUISITE: -

1. Basic of Computer Networking and Python

THEORY:
The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

Step-by-Step explanation is as follows:

Alice	Bob
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =

Alice	Bob
Algebraically, it can be shown that	
Users now have a symmetric secret key to encrypt	

Algorithm:

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and

Bob selected a private key b = 3

Step 3: Alice and Bob compute public values

Alice: x =(9^4 mod 23) = (6561 mod 23) = 6

Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and

Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys

Alice: ka = y^a mod p = 65536 mod 23 = 9

Bob: kb = x^b mod p = 216 mod 23 = 9

Step 7: 9 is the shared secret.

Conclusion: The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

Assignment Question:

1. Explain "Diffie-Hellmen key exchange algorithm with suitable example
2. What is Man in the middle attack?
3. How to Preventing a Man-in Middle Attack?

ASSIGNMENT 4

PROBLEM STATEMENT: Implementation of RSA

OBJECTIVE OF THE ASSIGNMENT:

1. To understand how RSA enables public key encryption and is widely used to secure sensitive data.

PREREQUISITE:

1. Basics of Python

Theory:

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and the Private key is kept private.

An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client's public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasibl

Algorithm:

Select two prime no's. Suppose **P = 53 and Q = 59.**
Now First part of the Public key : n = P*Q = 3127.
We also need a small exponent say **e :**
But e Must be
An integer.

Not be a factor of Φ(n).
1 < e < Φ(n) [Φ(n) is discussed below],
Let us now consider it to be equal to 3.
Our Public Key is made of n and e

Generating Private Key:
We need to calculate Φ(n) :
Such that **Φ(n) = (P-1)(Q-1)**
so, Φ(n) = 3016
Now calculate Private Key, **d :**
d = (k*Φ(n) + 1) / e for some integer k
For k = 2, value of d is 2011.

ow we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011) Now we will encrypt **"HI"**:
Convert letters to numbers : H = 8 and I = 9
Thus **Encrypted Data c = (89e)mod n**
Thus our Encrypted Data comes out to be 1394

Now we will decrypt **1394** :
Decrypted Data = (cd)mod n
Thus our Encrypted Data comes out to be 89
8 = H and I = 9 i.e. "HI"

Conclusion:

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key

Assignment Question:

1. Are strong primes necessary in RSA?
2. How fast RSA is?
3. What would it take to break RSA?
4. How is RSA used for authentication in practice?

ASSIGNMENT 5

PROBLEM STATEMENT:- Implementation of ECC algorithm.

OBJECTIVE: Students should be able to understand ECC algorithm using Python.

PREREQUISITE:

1. Basics of Python programming.

Theory:

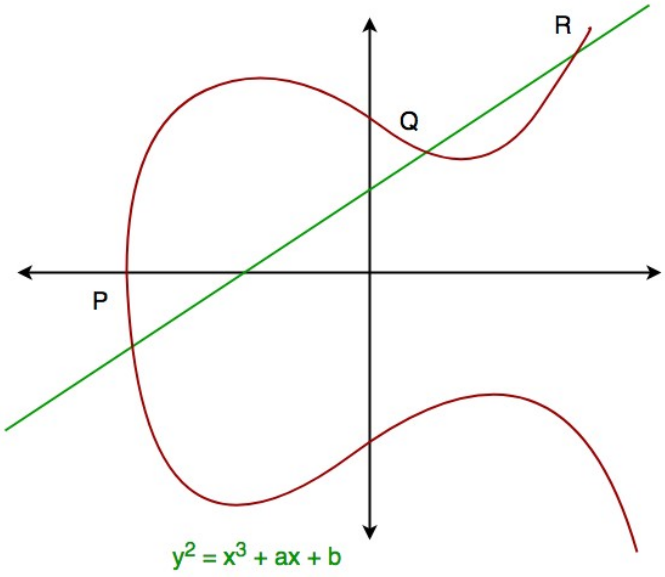
ECC is an approach to public-key cryptography, based on the algebraic structure of elliptic curves over finite fields. ECC requires a smaller key as compared to non-ECC cryptography to provide equivalent security (a 256-bit ECC security has equivalent security attained by 3072-bit RSA cryptography).

For a better understanding of Elliptic Curve Cryptography, it is very important to understand the basics of the Elliptic Curve. An elliptic curve is a planar algebraic curve defined by an equation of the form

Where ‘a’ is the co-efficient of x and ‘b’ is the constant of the equation

The curve is non-singular; that is, its graph has no cusps or self-intersections (when the characteristic of the Coefficient field is equal to 2 or 3).

In general, an elliptic curve looks like as shown below. Elliptic curves can intersect almost 3 points when a straight line is drawn intersecting the curve. As we can see, the elliptic curve is symmetric about the x-axis. This property plays a key role in the algorithm.



This approach uses six tuple {P, a, b, G, n, h}

P = Field that the curve is define over

G = Generator point

a, b = Values define the curve

h = Co- factor

n = Prime order of G

Conclusion:

This an approach to public-key cryptography, based on the algebraic structure of elliptic curves over finite fields.

DR. D.Y. PATIL INSTITUTE OF TECHNOLOGY, PUNE

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATA SCIENCE

Lab Manual

Third Year Engineering

Semester-VI

Cloud Computing

Subject Code: 317536

Class: TE AI&DS

Academic Year 2024-25

ASSIGNMENT 1

TITLE: AWS

Problem Statement: Setting up AWS Environment: Create a new AWS account, Secure the root user, Create an IAM user to use in the account Set up the AWS CLI, Set up a Cloud9 environment.

Objective: Students will learn how to create and AWS account and its usage.

Theory:

1 Create a new AWS account

To create an AWS account follow below steps:

1. Open the Amazon Web Services home page.
2. Choose Create an AWS account.

   Note: If you signed in to AWS recently, that option might not be there. Instead, choose Sign in to the Console. Then, if Create a new AWS account still isn't visible, first choose Sign in to a different account, and then choose Create a new AWS account.

3. Enter your account information, and then choose Verify email address. This will send a verification code to your specified email address.

   Important: Because of the critical nature of the root user of the account, we strongly recommend that you use an email address that can be accessed by a group, rather than only an individual. That way, if the person who signed up for the AWS account leaves the company, the AWS account can still be used because the email address is still accessible.

   If you lose access to the email address associated with the AWS account, then you can't recover access to the account if you ever lose the password.

4. Enter your verification code, and then choose Verify.
5. Enter a strong password for your root user, confirm it, and then choose Continue. AWS requires that your password meet the following conditions:

   - It must have a minimum of 8 characters and a maximum of 128 characters.

- It must include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * () <> [] {} | _+-= symbols.

- It must not be identical to your AWS account name or email address.

6. Choose Business or Personal. Personal accounts and business accounts have the same features and functions.

7. Enter your company or personal information.

   Important: For business AWS accounts, it's a best practice to enter:

   - A company phone number rather than a number for a personal phone.

   - An e-mail address with a domain name that belongs to the company or organization that will be using the account.

   Configuring the account's root user with an individual email address or a personal phone number can make your account insecure.

8. Read and accept the AWS Customer Agreement. Be sure that you read and understand the terms of the AWS Customer Agreement.

9. Choose Continue. At this point, you'll receive an email message to confirm that your AWS account is ready to use. You can sign in to your new account by using the email address and password you provided during sign up. However, you can't use any AWS services until you finish activating your account.

10. Enter the information about your payment method, and then choose Verify and Continue. If you want to use a different billing address for your AWS billing information, choose Use a new address.

    You can't proceed with the sign-up process until you add a valid payment method.

11. Enter your country or region code from the list, and then enter a phone number where you can be reached in the next few minutes.

12. Enter the code displayed in the CAPTCHA, and then submit.

13. When the automated system contacts you, enter the PIN you receive and then submit.

14. Select one of the available AWS Support plans. For a description of the available Support plans and their benefits, see Compare AWS Support plans.

15. Choose Complete sign up. A confirmation page appears that indicates that your account is being activated.

16. Check your email and spam folder for an email message that confirms your account was activated. Activation usually takes a few minutes but can sometimes take up to 24 hours.

    After you receive the activation message, you have full access to all AWS services.

2 Create an IAM user to use in the account

The process of creating a user and enabling that user to perform work tasks consists of the following steps:

1. Create the user in the AWS Management Console, the AWS CLI, Tools for Windows PowerShell, or using an AWS API operation. If you create the user in the AWS Management Console, then steps 1–4 are handled automatically, based on your choices. If you create the users programmatically, then you must perform each of those steps individually.

2. Create credentials for the user, depending on the type of access the user requires:

    - Enable console access – optional: If the user needs to access the AWS Management Console, create a password for the user. Disabling console access for a user prevents them from signing in to the AWS Management Console using their user name and password. It does not change their permissions or prevent them from accessing the console using an assumed role.

    Tip: Create only the credentials that the user needs. For example, for a user who requires access only through the AWS Management Console, do not create access keys.

3. Give the user permissions to perform the required tasks by adding the user to one or more groups. You can also grant permissions by attaching permissions policies directly to the user. However, we recommend instead that you put your users in groups and manage permissions through policies that are attached to those groups. You can also use a permissions boundary to limit the permissions that a user can have, though this is not common.

4. (Optional) Add metadata to the user by attaching tags. For more information about using tags in IAM, see Tagging IAM resources.

5. Provide the user with the necessary sign-in information. This includes the password and the console URL for the account sign-in page where the user provides those credentials. For more information, see How IAM users sign in to AWS.

6. (Optional) Configure multi-factor authentication (MFA) for the user. MFA requires the user to provide a one-time-use code each time he or she signs into the AWS Management Console.

7. (Optional) Give users permissions to manage their own security credentials. (By default, users do not have permissions to manage their own credentials.) For more information, see Permitting IAM users to change their own passwords.

3 Set up the AWS CLI

The AWS CLI stores your configuration and credential information in a *profile* (a collection of settings) in the credentials and config files.

There are primarily two methods to quickly get setup:

- Configuring using AWS CLI commands
- Manually editing the credentials and config files

The following examples use sample values for each of the authentication methods. Replace sample values with your own.

Configuring using AWS CLI commands

For general use, the aws configure or aws configure sso commands in your preferred terminal are the fastest way to set up your AWS CLI installation. Based on the credential method you prefer, the AWS CLI prompts you for the relevant information. By default, the information in this profile is used when you run an AWS CLI command that doesn't explicitly specify a profile to use.

- IAM Identity Center (SSO)
- IAM Identity Center (Legacy SSO)
- Short-term credentials
- IAM role
- Amazon EC2 instance metadata credentials

- Long-term credentials

This example is for AWS IAM Identity Center using the aws configure sso wizard. For more information, see Token provider configuration with automatic authentication refresh for IAM Identity Center.

$ **aws configure sso**

SSO session name (Recommended): ***my-sso***

SSO start URL [None]: ***https://my-sso-portal.awsapps.com/start***

SSO region [None]:***us-east-1***

Attempting to automatically open the SSO authorization page in your default browser.

There are 2 AWS accounts available to you.

> DeveloperAccount, developer-account-admin@example.com (*111122223333*)

ProductionAccount, production-account-admin@example.com (*444455556666*)

Using the account ID *111122223333*

There are 2 roles available to you.

> ReadOnly

FullAccess

Using the role name "ReadOnly"

CLI default client Region [None]: ***us-west-2***

CLI default output format [None]: ***json***

CLI profile name [123456789011_ReadOnly]: ***user1***

Manually editing the credentials and config files

When copy and pasting information, we suggest manually editing the config and credentials file. Based on the credential method you prefer, the files are setup in a different way.

The files are stored in your home directory under the .aws folder. Where you find your home directory location varies based on the operating system, but is referred to using the

environment variables %UserProfile% in Windows and $HOME or ~ (tilde) in Unix-based systems. For more information on where these settings are stored, see Where are configuration settings stored?.

The following examples show a default profile and a profile named user1 and use sample values. Replace sample values with your own. For more information on the credentials and config files, see Configuration and credential file settings.

- IAM Identity Center (SSO)
- IAM Identity Center (Legacy SSO)
- Short-term credentials
- IAM role
- Amazon EC2 instance metadata credentials
- Long-term credentials

This example is for AWS IAM Identity Center. For more information, see Token provider configuration with automatic authentication refresh for IAM Identity Center.

Credentials file

The credentials file is not used for this authentication method.

Config file

[default]

sso_session = *my-sso*

sso_account_id = *111122223333*

sso_role_name = *readOnly*

region = *us-west-2*

output = *text*

[profile user1]

sso_session = *my-sso*

sso_account_id = *444455556666*

sso_role_name = *readOnly*

region = *us-east-1*

output = *json*

[sso-session *my-sso*]

sso_region = *us-east-1*

sso_start_url = *https://my-sso-portal.awsapps.com/start*

sso_registration_scopes = *sso:account:access*

For more detailed information on authentication and credential methods see Authentication and access credentials.

Using existing configuration and credentials files

If you have existing configuration and credentials files, these can be used for the AWS CLI.

To use the config and credentials files, move them to the folder named .aws in your home directory. Where you find your home directory location varies based on the operating system, but is referred to using the environment variables %UserProfile% in Windows and $HOME or ~ (tilde) in Unix-based systems.

You can specify a non-default location for the config and credentials files by setting the AWS_CONFIG_FILE and AWS_SHARED_CREDENTIALS_FILE environment variables to another local path.

4 Setup the Cloud9 Development Environment

- Go to the AWS Management Console, click **Services** then select **Cloud9** under Developer Tools.
- Click **Create environment**.
- Enter workshop into **Name** and optionally provide a **Description**.
- Click **Next step**.
- You may leave **Environment settings** at their defaults of launching a new **t2.micro** EC2 instance which will be paused after **30 minutes** of inactivity.
- Click **Next step**.
- Review the environment settings and click **Create environment**. It will take several minutes for your environment to be provisioned and prepared.
- Once ready, your IDE will open to a welcome screen. The central panel of the IDE has two parts: a text/code editor in the upper half, and a terminal window in the lower half. Below the welcome screen in the editor, you should see a terminal prompt

similar to the following (you may need to scroll down below the welcome screen to see it):

- You can run AWS CLI commands in here just like you would on your local computer. Verify that your user is logged in by running `aws sts get-caller-identity` as follows at the terminal prompt:

```
aws sts get-caller-identity
```

- You'll see output indicating your account and user information:

```
Admin:~/environment $ aws sts get-caller-identity

{
  "Account": "123456789012",
  "UserId": "AKIAI44QH8DHBEXAMPLE",
  "Arn": "arn:aws:iam::123456789012:user/Alice"
}
```

- To create a new text/code file, just click the + symbol in the tabs section of the editor part of the IDE. You can do that now, and close the wecome screen by clicking the **x** symbol in the welcome screen tab.
- Keep your AWS Cloud9 IDE opened in a browser tab throughout this workshop as we'll use it for activities like using the AWS CLI and running Bash scripts.

Conclusion: In this assignment student will be able to learn about the AWS environment and other related aspects.

Assignment 2

TITLE: Amazon Relational Database

Problem Statement: Setup, Create and visualize data in an Amazon Relational Database (Amazon RDS) MS SQL Express server using Amazon Quick Sight.

Objective: Students will be able to understand Amazon Relational Database and how to use it.

Prerequisite: Knowledge of Database Management System.

Theory:

Amazon RDS for SQL Server makes it easy to set up, operate, and scale SQL Server deployments in the cloud.

Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered Business Intelligence (BI) service built for the cloud. Using the Amazon RDS connector in Amazon QuickSight, organizations can seamlessly gather insights from RDS data without a single line of code.

Step 1. Create an AWS Account: The resources created and used in this tutorial are AWS Free Tier eligible.

Already have an account? Sign-in

Step 2. Create a Microsoft SQL Server Express Edition database in Amazon RDS

Complete the following steps to connect to a Database Engine in Amazon RDS.

a. Open the Amazon RDS console and choose the Region where you want to create the Database.

b. In the Create Database section, choose Create Database.

c. On the Create database page, in the Choose a database creation method section, choose Easy Create.

d. In the Configuration section, make the following changes:

For Engine type, choose Microsoft SQL Server.

For DB instance size, choose Free tier.

For DB instance identifier, type qsdatabase.

For Master username, enter admin.

For Master password, type a unique password, and confirm password.

e. In the View default settings for Easy create drop down, leave the default settings. Then, choose Create database.

Note: It may take several minutes for the database to be created.

Step 3. Download and connect to a Microsoft SQL Server client

Complete the following steps to download Microsoft SQL Server Management Studio, and create tables to run queries against the database.

a. Open the Download Microsoft SQL Server Management Studio page, choose the link under the Download SSMS section.

b. Open the Amazon RDS console, in the left-hand navigation pane, choose Databases. Then, choose the qsdatabase.

c. On the qsdatabase page, choose Modify.

d. On the ModifyDB instance: qsdatabase page, in the Connectivity section, choose Additional Configuration. Then, choose Publicly accessible, and choose Continue.

e. On the ModifyDB instance: qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.

f. On the left-hand navigation, choose Databases. Then, choose qsdatabase.

g. On the qsdatabase page, in the Connectivity & security section, choose the VPC security groups link.

h. On the Security groups page, choose the Security group ID.

i. On the sg-default page, in the Inbound rules section, choose Edit inbound rules.

j. On the edit inbound rules page, in the Inbound rules section, choose Add rule, and make the following changes.

For Type, choose All TCP from the drop-down list.

For Source, choose My IP.

k. Then, choose Save rules.

l. Verify that the SSMS Client download has completed. Then, install and open the software.

m. In the SQL Server pop up window, enter the following details.

For Server Name, paste the qsdatabase Endpoint and Port separated by commas. Example: qdatabase.abc.us-east-1.rds.amazonaws.com,1433.

Note: To find the endpoint, open the Amazon RDS console, and choose qsdatabase. On the qsdatabase page, in the Connectivity & Security section, copy the Endpoint and Port.

For Login, type the username you entered when creating the qsdatabase.

For Password, type the password you entered when creating the qsdatabase.

n. Then, choose Connect.

Step 4. Create a sample database and tables, and load sample data

Complete the following steps to create a sample database, create and load tables that can be accessed in Amazon QuickSight.

a. Open SQL Server Management Studio, in the left-hand navigation, choose Databases. Then, right click and choose Create Database.

b. On the New database page, for Database name, type Visualize. Then, choose OK.

c. Choose Visualize, and choose New Query.

d. In the Query editor, copy and paste the following script.

Once the script is successfully run, the tables will be created and loaded with the sample data.

```
CREATE TABLE newhire(

empno INT PRIMARY KEY,

ename VARCHAR(10),

job VARCHAR(9),

manager INT NULL,

hiredate DATETIME,
```

```
salary NUMERIC(7,2),
comm NUMERIC(7,2) NULL,
department INT)
begin
insert into newhire values
   (1,'JOHNSON','ADMIN',6,'12-17-1990',18000,NULL,4)
insert into newhire values
   (2,'HARDING','MANAGER',9,'02-02-1998',52000,300,3)
insert into newhire values
   (3,'TAFT','SALES I',2,'01-02-1996',25000,500,3)
insert into newhire values
   (4,'HOOVER','SALES I',2,'04-02-1990',27000,NULL,3)
insert into newhire values
   (5,'LINCOLN','TECH',6,'06-23-1994',22500,1400,4)
insert into newhire values
   (6,'GARFIELD','MANAGER',9,'05-01-1993',54000,NULL,4)
insert into newhire values
   (7,'POLK','TECH',6,'09-22-1997',25000,NULL,4)
insert into newhire values
   (8,'GRANT','ENGINEER',10,'03-30-1997',32000,NULL,2)
insert into newhire values
   (9,'JACKSON','CEO',NULL,'01-01-1990',75000,NULL,4)
insert into newhire values
```

```
   (10,'FILLMORE','MANAGER',9,'08-09-1994',56000,NULL,2)
insert into newhire values
   (11,'ADAMS','ENGINEER',10,'03-15-1996',34000,NULL,2)
insert into newhire values
   (12,'WASHINGTON','ADMIN',6,'04-16-1998',18000,NULL,4)
insert into newhire values
   (13,'MONROE','ENGINEER',10,'12-03-2000',30000,NULL,2)
insert into newhire values
   (14,'ROOSEVELT','CPA',9,'10-12-1995',35000,NULL,1)
end
CREATE TABLE department(
deptno INT NOT NULL,
dname VARCHAR(14),
loc VARCHAR(13))
begin
insert into department values (1,'ACCOUNTING','ST LOUIS')
insert into department values (2,'RESEARCH','NEW YORK')
insert into department values (3,'SALES','ATLANTA')
insert into department values (4, 'OPERATIONS','SEATTLE')
end
```

Step 5. Make the database instance Not publicly accessible

The database no longer needs to be publicly accessible; the previous script downloaded the required scripts from the client.

Complete these steps to connect Amazon QuickSight to RDS within a VPC.

a. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.

b. On the qsdatabase page, choose Modify.

c. On the ModifyDB instance:qsdatabase page, in the Connectivity section, choose Additional Configuration. Then, choose Not publicly accessible, and choose Continue.

d. On the ModifyDB instance:qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.

Step 6. Enable the RDS database instance for access to Amazon QuickSight

Follow these steps to create a security group for Amazon QuickSight to access the RDS database in a VPC.

a. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.

b. On the qsdatabase page, in the Connectivity & security section, copy the VPC id.

c. Under Security, choose the VPC security groups link.

d. On the Security Groups page, choose Create security group.

e. On the Create security group page, in the Basic details section, enter the following details.

For Name, type RDS SecGP

For Description, type for QS

For VPC, choose the VPC id for your RDS instance.

f. Then, choose Create security group.

g. On the Security Groups page, copy the Security group ID.

h. On the Security Groups page, choose Create security group.

i. On the Create security group page, in the Basic details section, enter the following details.

For Name, type QS SecGP

For Description, type for RDS

For VPC, choose the VPC id for your RDS instance.

j. In the Inbound rules section, choose Add rule.

For Type, choose All traffic

For Source, choose Custom

In the search box, paste the security group id you copied in step 6.g.

k. Choose Create security group.

l. On the sg-QS SecGp page, copy the security group id. This security group is needed for Amazon QuickSight to connect to Amazon RDS.

m. On the Security Groups page, choose the security group you created in step 6.g.

n. In the Inbound rules section, choose Edit inbound rules.

o. On the Edit inbound rules page, in the Inbound rules section, choose Add rule. Then, enter the following details.

For Type, choose MSSQL

For Source, choose Custom

In the search box, paste the security group id you copied in Step 6.l

p. Choose Save rules. This security group is needed for Amazon RDS to connect Amazon QuickSight.

q. Open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.

r. On the qsdatabase page, choose Modify.

s. On the Modify DB instance: qsdatabase page, in the Connectivity section, for Security group, choose RDS SecGP (for QS). Then, choose Continue.

t. On the Modify DB instance: qsdatabase page, in the Scheduling of modifications section, choose Apply immediately. Then, choose Modify DB instance.

Step 7. Create your Amazon QuickSight account

Complete the following steps to create your Amazon QuickSight account.

Note: For more information, see Setting up Amazon QuickSight in the Amazon QuickSight documentation.

a. Open the Amazon QuickSight landing page, and choose Sign up for QuickSight.

b. On the Create you QuickSight account page, for Edition, choose Enterprise, and choose Continue.

c. On the Create your QuickSight account page, in the Edition section, choose Use IAM federated identities and QuickSight-managed users.

d. In the QuickSight region section, enter the following details.

Select a region from the drop-down list.

For QuickSight account name, type a unique account name.

For Notification email address, type an email address where you will receive notifications.

e. Then, choose Finish.

f. Choose Go to Amazon QuickSight, to open the Amazon QuickSight console.

Step 8. Enable Amazon QuickSight to connect to Amazon RDS and create a dataset for visualization

Complete the following steps to create a secure private connection to an Amazon VPC, and visualize the Amazon RDS data.

Note: For more information, see Configuring the VPC Connection in the QuickSight Console in the Amazon QuickSight documentation.

a. On the Analyses page, in the top right corner of the screen, and choose your username. Then, from the drop-down list, choose Manage QuickSight.

b. On the left navigation pane, choose Manage VPC connections. Then, choose Add VPC connection.

c. In your web browser, open a new tab. Then, open the Amazon RDS console, in the left-hand navigation, choose Databases. Then, choose the qsdatabase.

d. On the qsdatabase page, in the Connectivity & security section, under VPC, copy the id. Then, under Subnets, copy one of the ids.

d. Navigate back to the Adding VPC connection page, and enter the following details.

For VPC connection name, type RDSVPC

For VPC ID, choose the id you copied in Step 8.e

For Subnet ID, paste the id you copied in Step 8.e

For Security group ID, paste the id you copied in Step 6.g

e. Then, choose Create.

f. On the top left corner of your screen, choose the QuickSight icon. Then, in the left navigation, choose Datasets.

g. On the Datasets page, choose New dataset.

h. On the Create a Datasets page, choose RDS.

i. On the New RDS data source page, enter the following details.

For Data source name, type DataFromRDS

For Instance ID, choose qsdatabase

For Connection type, choose RDSVPC

For Database name, type Visualize

For Username, type the username you entered when creating the Visualize database

For Password, type the password you entered when creating the Visualize database

j. Then, choose Validate connection. If the connection was successful, choose Create data source.

k. On the Choose your table page, in the Schema section, choose dbo.

l. In the Tables section, choose newhire. Then, choose Select.

m. On the Finish dataset creation page, leave the default selections, and choose Visualize.

n. On the Visualize page, in the Visual types section, choose the Stacked Area Line Chart.

o. In the Fields list section, drag and drop ename and salary to the Field Wells section.

Note: For more information, see Working with Visuals in the Amazon QuickSight documentation.

Step 09. Clean up

In this step, you delete the resources you used in this lab.

Important: Deleting resources that are not actively being used reduces costs and is a best practice. Not deleting your resources will result in charges to your account.

Conclusion: Students are able to understand about the Amazon relational database, its connectivity and how to use it.

ASSIGNMENT 03

TITLE: Wordpress

Problem Statement: Setup, Create and connect your Word Press site to an object storage bucket using Lightsail service.

Objective: Students when get to know how we have to connect Word Press site to Amazon lightsail and its importance.

Prerequisite: Basics of Word Press site.

Theory:

Amazon Lightsail is an easy-to-use virtual private server provider. Lightsail recently launched an object storage service. This tutorial walks you through the steps required to set up your WordPress site on Amazon Lightsail and connect the website to a Lightsail bucket to store website images and attachments.

To do this, you install the WP Offload Media Lite plugin on your WordPress website and configure it to connect to your Lightsail bucket. After the plugin is configured, all media that you upload to your WordPress website will be automatically added to your bucket instead instance's disk.

Following are the steps we will follow:

Step 1: Prerequisites

Complete the following prerequisites.

1.1 —Sign up for an AWS account and navigate to the Lightsail console.

1.2 — Create a WordPress website on Amazon Lightsail.

1.3 — Create a bucket in the Lightsail object storage service. For more information, see Creating buckets in Amazon Lightsail.

Step 2: Modify your bucket permissions

Complete the following procedure to change the permissions of your bucket to give access to your WordPress instance and the Offload Media Lite plugin. The access permissions of your bucket must be set to Individual objects can be made public (read-only). You must also attach

the WordPress instance to the access role of your bucket. For more information about bucket permissions, see Understanding bucket permissions in Amazon Lightsail.

2.1 — On the Lightsail home page, choose the Storage tab and choose the name of the bucket that you want to use with your WordPress website.

2.2 — Choose the Permissions tab on the Bucket management page.

Choose Change permissions under the Bucket access permissions section of the page.

2.3 — Choose Individual objects can be made public and read only.

Choose Save.

2.4 — Choose Yes, save in the confirmation prompts that appear.

After a few moments, your bucket will be configured to allow for individual object access. This ensures that objects uploaded to your bucket from your WordPress website using the Offload Media Lite plugin are readable to your customers.

2.8 — Scroll to the Resource access section of the page, and choose Attach instance.

2.9 — Choose the name of your WordPress instance in the drop-down that appears, and then choose Attach.

After a few moments, your WordPress instance will be attached to the access role of your bucket. This ensures that your WordPress instance has access to manage objects in your bucket.

Step 3: Install the WP Offload Media Lite plugin on your WordPress website

Complete the following procedure to install the WP Offload Media Lite plugin on your WordPress website. This plugin automatically copies images, videos, documents, and any other media added through WordPress' media uploader to your Lightsail bucket, For more information, see WP Offload Media Lite in the WordPress website.

3.1 — Sign in to the dashboard of your WordPress website as an administrator.

3.2 — Pause on Plugins in the left navigation menu, and choose Add New.

3.3 — Search for WP Offload Media Lite.

3.4 — In the search results, choose Install Now next to the WP Offload Media plugin.

3.5 — Choose Activate after the plugin is done installing.

3.6 — In the left navigation menu, choose Settings, then choose Offload Media.

3.7 — In the Offload Media page, choose Amazon S3 as the storage provider.

3.8 — Choose My server is on Amazon Web Services and I'd like to use IAM Roles.

Choose Next.

3.9 — Choose Browse existing buckets in the What bucket would you like to use? page that appears.

3.10 — Choose the name of the bucket that you want to use with your WordPress instance.

3.11 — In the Offload Media Lite Settings page that appears, make sure to enable Force HTTPS and Remove Files From Server.

- The Force HTTPS setting must be enabled because Lightsail buckets use HTTPS by default to serve media files. If you don't enable this feature, media files that are uploaded to your Lightsail bucket from your WordPress website will not be be served correctly to your customers when they visit your website.

- The Remove Files From Server setting ensures that media that is uploaded to your Lightsail bucket isn't also stored on your instance's disk. If you don't enable this feature, media files that are uploaded to your Lightsail bucket will also be stored on the local storage of your WordPress instance.

3.12 —Choose Save Changes.

Note: To return to the Offload Media Lite Settings page later, pause on Settings in the left navigation menu, and choose Offload Media Lite.

Your WordPress website is now configured to use the Media Lite Plugin. The next time you upload a media file through WordPress, that file is automatically uploaded to your Lightsail bucket, and is served by the bucket. To test the configuration, continue to the next section of this tutorial.

Step 4: Test the connection between your WordPress website and your Lightsail bucket

Complete the following procedure to upload a media file to your WordPress instance and confirm that it is uploaded to your Lightsail bucket and is served from your bucket.

4.1 — Pause on Media in the left navigation menu of the WordPress dashboard, and choose Add New.

4.2 — Choose Select Files on the Upload New Media page that appears.

4.3 — Choose a media file to upload from your local computer, and choose Open.

4.4 —When the file is done uploading, choose Library under Media in the left navigation menu.

4.5 — Choose the file that you recently uploaded.

4.6 —In the details panel of the file, you should see the name of your bucket in the Bucket and File URL fields.

4.7 — When you go to the Objects tab of the Lightsail bucket management page, you should see a wp-content folder. This folder is created by the Offload Media Lite plugin, and will be used to store your uploaded media files.

Conclusion: We have successfully connected your WordPress website running on an Amazon Lightsail instance to a Lightsail bucket to store website images and attachments.