

Configuration Manual

MSc Research Project
MSc Cloud Computing

Sai Siddharth Manik
Student ID: 23289678

School of Computing
National College of Ireland

Supervisor: Shaguna Gupta

National College of Ireland
MSc Project Submission Sheet



School of Computing

Student Name: Sai Siddharth Manik
Student ID: X23289678
Programme: MSc Cloud Computing **Year:** 2024-25
Module: MSc Research Project
Supervisor: Shaguna Gupta
Submission Due Date: 02-01-2026
Project Title: Enhancing Cloud Security: A Hybrid PGP-Inspired Encryption System Using ECDH and AES-GCM
Word Count: 299 **Page Count:** 06

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sai Siddharth Manik
Date: 02/01/2026

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Title : Enhancing Cloud Security: A Hybrid PGP AES-GSM and Symmetric Encryption Framework

1. Introduction

This configuration manual describes the complete system setup, tools, and deployment environment used to implement a PGP-inspired hybrid encryption framework for secure cloud-based data protection. The system combines modern asymmetric key exchange using X25519 with symmetric encryption using AES-GCM and DES-CBC, exposed through a Flask web application.

The configuration supports performance evaluation, system resource monitoring, and scalability testing using Locust on AWS infrastructure.

2. Hardware Requirements

1. **Processor:** Dual-core CPU or higher
2. **Architecture:** x86_64
3. **RAM:** Minimum 2 GB (Recommended 4 GB)
4. **Storage:** Minimum 15 GB free disk space
5. **Network:** Stable internet connection

3. Software Requirements

3.1 Operating System

Amazon Linux 2 (AWS managed)

3.2 Programming Language

Python Version: Python 3.9 or higher

3.3 Python Libraries and Dependencies

```
cryptography
pycryptodome
flask
psutil
locust
hashlib
time
os
json
```

3.4 Cryptographic Primitives

Asymmetric: X25519 (ECDH)

Key Derivation: HKDF with SHA-256

Symmetric: AES-GCM, DES-CBC

Hashing: SHA-256

3.5 Testing

Locust

4. AWS Services Used

4.1 AWS Cloud9

Integrated development environment

Used for:

- ← Writing and testing cryptographic modules
- ← Performance benchmarking
- ← Locust load-testing script execution

4.2 AWS Elastic Beanstalk

Manages deployment of Flask web application

Handles:

- ← EC2 provisioning
- ← Application runtime
- ← Environment configuration

4.3 AWS EC2

Underlying compute service

Executes:

- ← Key generation
- ← Encryption and decryption



5. System Architecture Configuration

5.1 Application Architecture

Frontend: HTML and CSS

Backend: Flask (Python)

Design: Stateless request-based processing

5.2 Supported Encryption Modes

PGP-style encryption using AES-GCM

PGP-style encryption using DES-CBC (legacy comparison)

Each request generates fresh cryptographic material to simulate real PGP behaviour.

AWS Deployment

The screenshot shows the AWS Cloud9 console interface. On the left is a sidebar with 'AWS Cloud9' and navigation links for 'My environments', 'Shared with me', 'All account environments', and 'Documentation'. The main area displays the environment 'thesis-project-cloud9-x23289678'. At the top, there are two status messages: a green one stating 'Successfully created thesis-project-cloud9-x23289678' and a blue one about AWS Toolkits. Below these are 'Delete' and 'Open in Cloud9' buttons. The 'Details' section shows a table with the following information:

Details		
Name	thesis-project-cloud9-x23289678	Owner ARN
Description	-	arn:aws:sts::125642630269:assumed-role/voclabs/user3537829=x23289678@student.ncirl.ie
Environment type	EC2 instance	Number of members
		1
		Status
		Ready
		Lifecycle status
		Created

At the bottom, there are tabs for 'EC2 instance', 'Network settings', and 'Tags'.

EC2:

EC2 > Instances > i-05652404a4db74a78

EC2

- Dashboard
- EC2 Global View
- Events
- ▼ Instances
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
 - Capacity Manager
- ▼ Images
 - AMIs

Instance summary for i-05652404a4db74a78 (aws-cloud9-thesis-project-cloud9-x23289678-b0b9ce6d0b414ef39385173f8d9daf49)

Updated less than a minute ago

[Connect](#) [Instance state](#) [Actions](#)

Instance ID i-05652404a4db74a78	Public IPv4 address 3.234.207.253 open address	Private IPv4 addresses 172.31.14.191
IPv6 address -	Instance state Running	Public DNS ec2-3-234-207-253.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-14-191.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-14-191.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t3.medium	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 3.234.207.253 [Public IP]	VPC ID vpc-09dcfd1355107b7fc	

Elastic beanstalk :

Elastic Beanstalk > Environments > Thesis-eb-x23289678-env

Elastic Beanstalk

- Applications
- Environments
- Change history
- ▼ Application: thesis-eb-x23289678
 - Application versions
 - Saved configurations
- ▼ Environment: Thesis-eb-x23289678-env
 - Go to environment
 - Configuration
 - Events
 - Health
 - Logs

Thesis-eb-x23289678-env

[Actions](#) [Upload and deploy](#)

Environment overview

Health
No Data - 1 health issue

Domain
pgp-encryption.us-east-1.elasticbeanstalk.com

Environment ID
e-dmqc2j4kma

Application name
thesis-eb-x23289678

Platform [Change version](#)

Platform
Python 3.11 running on 64bit Amazon Linux 2023/4.8.0

Running version
app-251215_110945812372

Platform state
Supported

[Events](#) [Health](#) [Logs](#) [Monitoring](#) [Alarms](#) [Managed updates](#) [Tags](#)

Events (38) [Info](#)

Filter events by text, property or value

Output screens :



PGP Hybrid Encryption

ECDH + Symmetric Encryption (AES-GCM / DES)

This application demonstrates PGP-style hybrid encryption using ECDH for secure session key exchange and AES-GCM or DES for data encryption.

Select Encryption Algorithm

PGP + AES-GCM

Enter Your Message

Type your secret message here...

PGP Encryption Result

Encryption & Decryption Successful

Messages

ORIGINAL MESSAGE

hii how are you ?

DECRYPTED MESSAGE

hii how are you ?

Cryptographic Details

RECEIVER PUBLIC KEY

887b4100a9d1ad87b84e14e4105cfe899cf68
3cf810ba03ebf8d2288cf189619

EPHEMERAL PUBLIC KEY

950ce62bba0478421b9a80241859c5c7c1376
7bbc009799eef512e6030fd4739

ENCRYPTED SESSION KEY

6b8f1321fc07c88c060c102f8cad31dffe489
125000ce03002cd601b988b0bde

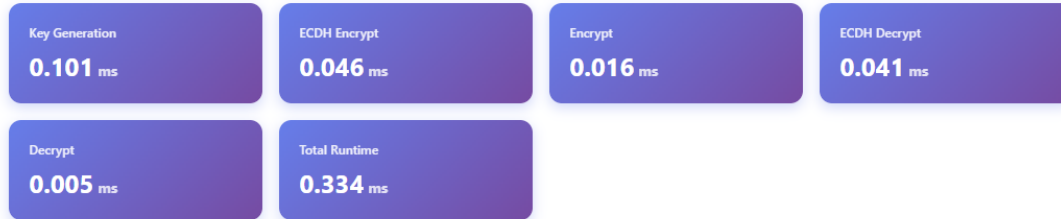
INITIALIZATION VECTOR (IV)

14017439784bd904c811f51f

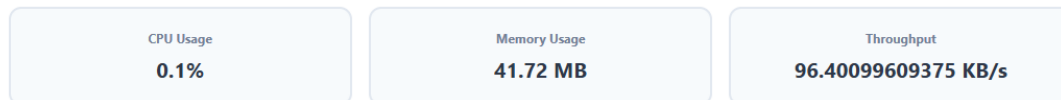
Ciphertext

990793acf6879898da518d6f90a105a59fead0c1d4f1e01ef86a3c0b8c4cdfcaae

Performance Metrics



System Metrics



References:

References :

1] <https://www.python.org/downloads/release/python-390/>

2]

<https://cryptography.io/en/latest/hazmat/primitives/aead/#cryptography.hazmat.primitives.ciphers.aead.AESGCM>

3] https://docs.openssl.org/3.5/man7/des_modes/#name

4] <https://pypi.org/project/cryptography/>

5] <https://docs.aws.amazon.com/>