

Configuration Manual

MSc Research Project
MSc Cloud Computing

Sai Gowtham Emani
Student ID: 23337818

School of Computing
National College of Ireland

Supervisor: Shreyas Setlur Arun

National College of Ireland
MSc Project Submission Sheet



School of Computing

Sai Gowtham Emani

Student Name:	Sai Gowtham Emani		
Student ID:	23337818		
Programme:	Msc Cloud Computing	Year:	2025-2026
Module:	Msc Research Project		
Lecturer:	Shreyas Setlur Arun		
Submission Due Date:	02-01-2026		
Project Title:	A Hybrid Lightweight Cryptographic Framework with Parallel Processing on Cloud for Secure and Low-Latency IoT Data Transmission		
Word Count:	869	Page Count:	8

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:	
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

Sai Gowtham Emani

Student ID:23337818

Title: Cryptography System in Cloud using Hybrid Lightweight Techniques and Diffusion Optimization for IoT Systems

1 1. Introduction

This configuration manual outlines the system setup, tools and deployment environment utilized to develop and test a hybrid lightweight cryptographic system to the IoT-cloud environment. The proposed system connects the lightweight encryption used in the IoT layer with the more advanced symmetric cryptography used in the cloud layer which is optimized through parallel processing to enhance latency, throughput, and diffusion performance.

The configuration supports experimental comparison between hybrid ASCON + ChaCha20 and ASCON + DES approaches against standalone AES-based systems.

2 2. Hardware Requirements

3 2.1 Minimum Hardware Specifications

- **Processor:** Dual-core CPU or better.
- **Architecture:** x86_64
- **RAM:** Minimum 2 GB & Recommended: 4 GB
- **Storage:** Minimum 15 GB free disk space
- **Network:** The network is stable with internet

4 3. Software Requirements

5 3.1 Operating System

- Amazon Linux 2 (AWS-managed)
- Compatible with Python 3.x runtime-compatible

6 3.2 Programming Language

- **Python Version:** Python 3.9 or above

7 3.3 Python Libraries and Dependencies

cryptography

Python library of secure cryptographic operations.

Provides primitives for encryption, hashing, digital signatures, and key exchange.

pycryptodome

Python cryptographic library Low-level control self-contained Python Cryptographic library.

It supports symmetric/asymmetric ciphers, hashes, MACs, and random number generation.

psutil

A system and process resources monitoring cross-platform library.

Used to retrieve CPU, memory, disk, network, and process statistics.

flask

A framework and web application created to develop REST APIs and web applications, which are lightweight.

Provides routing, request handling, and extensibility with minimal overhead.

multiprocessing

A typical Python package for parallel execution using multiple processes.

Bypasses the GIL to achieve real CPU-bound parallelism.

threading

A Python standard module that can be used to run multiple threads.

The most appropriate in I/O-bound activities in a single process.

numpy

Python numerical library A central scientific computing library.

Provides multi-dimensional arrays and optimized mathematical functions.

time

A built-in Python module for time-related operations.

Used for delays, timestamps, and performance measurement.

os

An operating system communication module in Python.

Provides file handling, environment variables, and process-related utilities.

8 3.4 Cryptographic Algorithms Used

- **Lightweight Algorithms:** ASCON, ChaCha20, DES
- **Cloud-Side Algorithms:** AES-GCM, ChaCha20
- **Purpose:** Secure encryption with reduced computational overhead for IoT devices

9 4. AWS Services Used

10 4.1 AWS Cloud9

- Development and testing environment
- Used for:
 - Writing and debugging encryption modules
 - Running IoT client-side simulators
 - Measuring resource utilization

11 4.2 AWS Elastic Beanstalk

- Implementation and hosting of Flask-based cloud application
- Manages:
 - EC2 provisioning
 - Application runtime
 - Scaling and environment configuration

12 4.3 AWS EC2

- Backend processing layer
- Handles:
 - Parallel encryption and decryption
 - Performance metric logging
 - API request handling

13 5. Implementation Flow Configuration

1. IoT simulator encrypts plaintext using a lightweight cipher.
2. Encrypted data is sent to cloud API endpoint.
3. Cloud service re-encrypts information with a more powerful algorithm.
4. Parallel processing is applied for encryption tasks.
5. Decryption requests are handled and validated.
6. Measures are recorded and kept to be analysed.

AWS Deployment :

AWS Cloud9

aws Search [Alt+S] United States (N. Virginia) Account ID: 2022-6103-8261 voclabs/user3524650=x23337818@student.ncirLie

AWS Cloud9 > Environments > x23337818-cloud9

x23337818-cloud9

Delete Open in Cloud9

Details

Name
x23337818-cloud9

Description
-

Environment type
EC2 instance

Owner ARN
arn:aws:sts::202261038261:assumed-role/voclabs/user3524650=x23337818@student.ncirLie

Number of members
1

Status
Ready

Lifecycle status
Created

Edit

EC2 instance Network settings Tags

EC2 instance

ARN
arn:aws:cloud9:us-east-1:202261038261:environment:550394d1d1084e5eb7303c7c7571c405

Platform
Amazon Linux 2023

Instance type
t3.medium (4 GiB RAM + 2 vCPU)

Storage
EBS only

Manage EC2 instance

File Edit Find View Go Run Tools Window Support Preview Run Share

Go to Anything (Ctrl-P)

cloud9-thesis-x23

- templates
- app.py
- ascon_chacha.py
- des_ascon.py
- profile
- README.md
- requirements.txt

```

35 from flask import Flask, render_template, request, jsonify
36 from ascon_chacha import chacha_ascon_encrypt_decrypt
37 from des_ascon import des_ascon_encrypt_decrypt
38
39 application = Flask(__name__)
40
41 app = application
42
43 @app.route("/")
44 def index():
45     return render_template("index.html")
46
47
48 @app.route("/run_chacha_ascon", methods=["POST"])
49 def run_chacha_ascon():
50     text = request.form.get("plaintext", "")
51     data = text.encode() if text else b"Temperature=26.8;Humidity=49%;Device-Sensor=22" * 1000
52     result = chacha_ascon_encrypt_decrypt(data)
53     return jsonify(result)
54
55
56 @app.route("/run_des_ascon", methods=["POST"])
57 def run_des_ascon():
58     text = request.form.get("plaintext", "")
59     data = text.encode() if text else b"Temperature=29.5;Humidity=53%;Device-Sensor=12" * 1000
60     result = des_ascon_encrypt_decrypt(data)
61     return jsonify(result)

```

46.1 Python Spaces: 4

bash -ip-172.31.82.42.ec x Immediate x app.py - Running x app.py - Stopped x

Stop Command: app.py Runner: Python 3 CWD ENV

* Debug mode: on
 WARNING: This is a development server. Do not use it in a production deployment. Use a production HTTP server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:8000
 * Running on http://172.31.82.42:8000
 Press CTRL+C to quit

AWS Elastic Beanstalk

The screenshot shows the AWS Elastic Beanstalk console. The left sidebar contains navigation links for Elastic Beanstalk, Applications, Environments, and Change history. The main content area displays the details for environment X23337818-eb-env. The environment overview section shows the health status as 'No Data', the environment ID as 'e-mdmypyq5msf', the application name as 'x23337818-eb', and the domain as 'X23337818-eb-env.eba-sswestvl.us-east-1.elasticbeanstalk.com'. The platform section shows the platform as 'Python 3.11 running on 64bit Amazon Linux 2023/4.7.5', the running version as 'x23337818-eb-version-2', and the platform state as 'Supported'. The events section shows a list of events, including a transition from 'Info' to 'No Data' and a transition from 'No Data' to 'Info'.

Environment overview

Health: No Data

Environment ID: e-mdmypyq5msf

Domain: X23337818-eb-env.eba-sswestvl.us-east-1.elasticbeanstalk.com

Application name: x23337818-eb

Platform

Platform: Python 3.11 running on 64bit Amazon Linux 2023/4.7.5

Running version: x23337818-eb-version-2

Platform state: Supported

Events (31)

Time	Type	Details
November 7, 2025 11:07:42 (UTC+5:30)	INFO	Environment health has transitioned from Info to No Data. Application update completed 36 seconds ago and took 50 seconds. None of the instances are sending data.
November 7, 2025 11:06:42 (UTC+5:30)	INFO	Environment health has transitioned from No Data to Info. Application update in progress (duration: 36 seconds). None of the instances are sending data.

Output:

The screenshot shows the Hybrid Encryption Dashboard. The dashboard has a dark blue background with white text. The title 'Hybrid Encryption Dashboard' is prominently displayed at the top. Below the title, there is a description: 'Encrypt and decrypt data using parallel ChaCha20-Ascon and DES-Ascon hybrid algorithms. Monitor encryption metrics in real-time with this interactive dashboard.' The dashboard is divided into two main sections: 'Input Data' and 'Encryption Results'. The 'Input Data' section has a text input field labeled 'Enter Plaintext to Encrypt' containing the text 'Temperature=26.8;Humidity=49%;Device=Sensor-22'. Below the input field is a button labeled 'Run ChaCha20-Ascon'. The 'Encryption Results' section has a message that says 'No results yet. Select an encryption algorithm above to see metrics and results here.'

Hybrid Encryption Dashboard

Encrypt and decrypt data using parallel ChaCha20-Ascon and DES-Ascon hybrid algorithms.
Monitor encryption metrics in real-time with this interactive dashboard.

Input Data

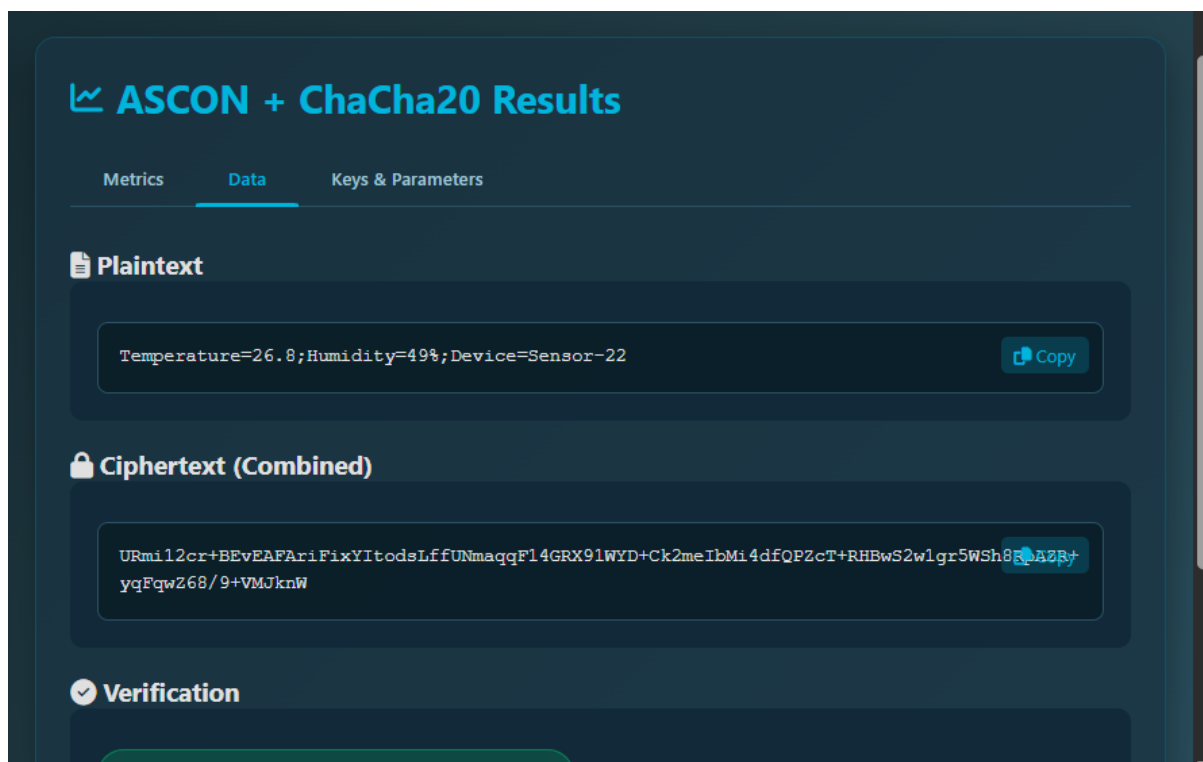
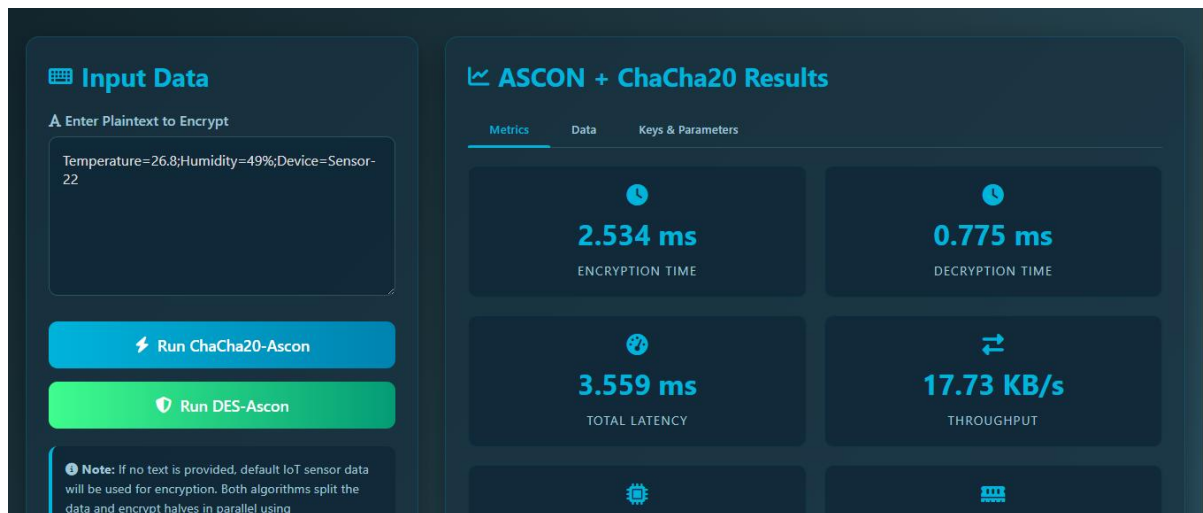
Enter Plaintext to Encrypt

Temperature=26.8;Humidity=49%;Device=Sensor-22

Run ChaCha20-Ascon

Encryption Results

No results yet. Select an encryption algorithm above to see metrics and results here.



References

- Dobraunig, C., Eichlseder, M., Mendel, F., & Schl  ffer, M. (2016). ASCON – A Family of Lightweight Authenticated Encryption Schemes. *Journal of Cryptology*, 34(1), 1–42. <https://ascon.iaik.tugraz.at/>
- Bernstein, D. J. (2008). ChaCha, a Variant of Salsa20. Workshop Record of SASC 2008 – The State of the Art of Stream Ciphers. <https://cr.yp.to/chacha.html>
- Dworkin, M. (2007). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM). NIST Special Publication 800-38D. <https://csrc.nist.gov/publications/detail/sp/800-38d/final>