CSE7101- Capstone Project

IotBased Secure Microgrid Monitoring System with Advanced Intrusion Detection

Batch Number: CCS_40

Student Name: Jason Paul

Roll No: 20221CCS0004

Github

Under the Guidance of,

Dr. Ruhin Kouser Professor
School of Computer Science and Engineering
Presidency University

Introduction

- **The Challenge:**

• Microgrids are increasingly targeted by cyberattacks and operational faults. Traditional monitoring depends on manual inspection and basic logging, which is slow, reactive, and unable to detect sophisticated attacks in real time.

- **Current Limitations:**

•Most existing IoT-based microgrid systems rely only on sensor readings without securing communication channels or detecting network-level threats such as replay, injection, DoS, spoofing, and MITM attacks.

- **Our Solution:**

•A **Secure IoT-Based Microgrid Monitoring Framework**with integrated Intrusion Detection System (IDS).

- **Key Innovation:**

•We fuse **two critical data streams**to enhance microgrid security:

- **1. Environmental Sensor Data:**
- Temperature, Humidity (DHT11) and Ambient Light (LDR) for environment-aware m on ito r in g.
- **2. Network BehaviourData:**

•MQTT message frequency, payload patterns, timestamp analysis, and device identity verification processed through a Flask-based IDS.

• **Objective:**

- To achieve **high intrusion detection accuracy (86.3%)**, secure communication using **MQTT-TLS**, and real-time monitoring through a live dashboard—offering a low-cost, scalable defense system for modern microgrids.

Problem Statement and

- Traditionalmicrogridmonitoringmethodsareslow,manual,andlack real-time cyber-attack detection, making them unreliable for modern distributed energy systems.
- **Current Limitation:**
- Most existing IoT-based microgrid systems rely only on raw sensor readings (temperature, humidity, light).
They ignore **network-level behavior**, where most cyberattacks actually oc cur.
- **The"BlindSpot":**
- Environmentalsensordataalonedoes**not**revealsecuritythreats.
- Network anomalies—like sudden message floods, timestamp mismatches, or spoofed device IDs—are invisible without IDS.
- **Example:**

A replay attack can resend old "normal" sensor data, fooling systems that rely only on environmental readings.
Without timestamp validation + anomaly detection, such attacks go completely undetected.
- **OurGoal:**
- To build a system that *"thinks like an operator and a security analyst"*—monitoring both **environmental conditions** AND **network be hav io,** ensuring reliable and secure microgrid operation.

Proposed System

Layers Involved:

Sensor Layer → DHT11 (Temp, Humidity), LDR (L ight)

- Communication Layer → MQTT over TLS (Port 8883)
- Processing Layer → Flask Backend
- Security Layer → Intrusion Detection System
- Presentation Layer → Real-time Dashboard
- Storage Layer → SQLite (logs)
- End-to-End Flow:

ESP8266 → MQTT-TLS → HiveMQ→ Flask IDS → Dashboard

ESP8266 NodeMCU

Wi-Fi, low power, ideal for IoT

DHT11 Sensor

Temp & humidity monitoring

LDR Sensor

Light-level detection

Power Supply

5V USB

Arduino IDE(ESP firmware)

Python 3.10

Flask Framework

paho-mqtt clientfor MQTT

Socket.IOfor real-time updates

SQLitefor logs

HiveMQ Cloudfor secure MQTT broker

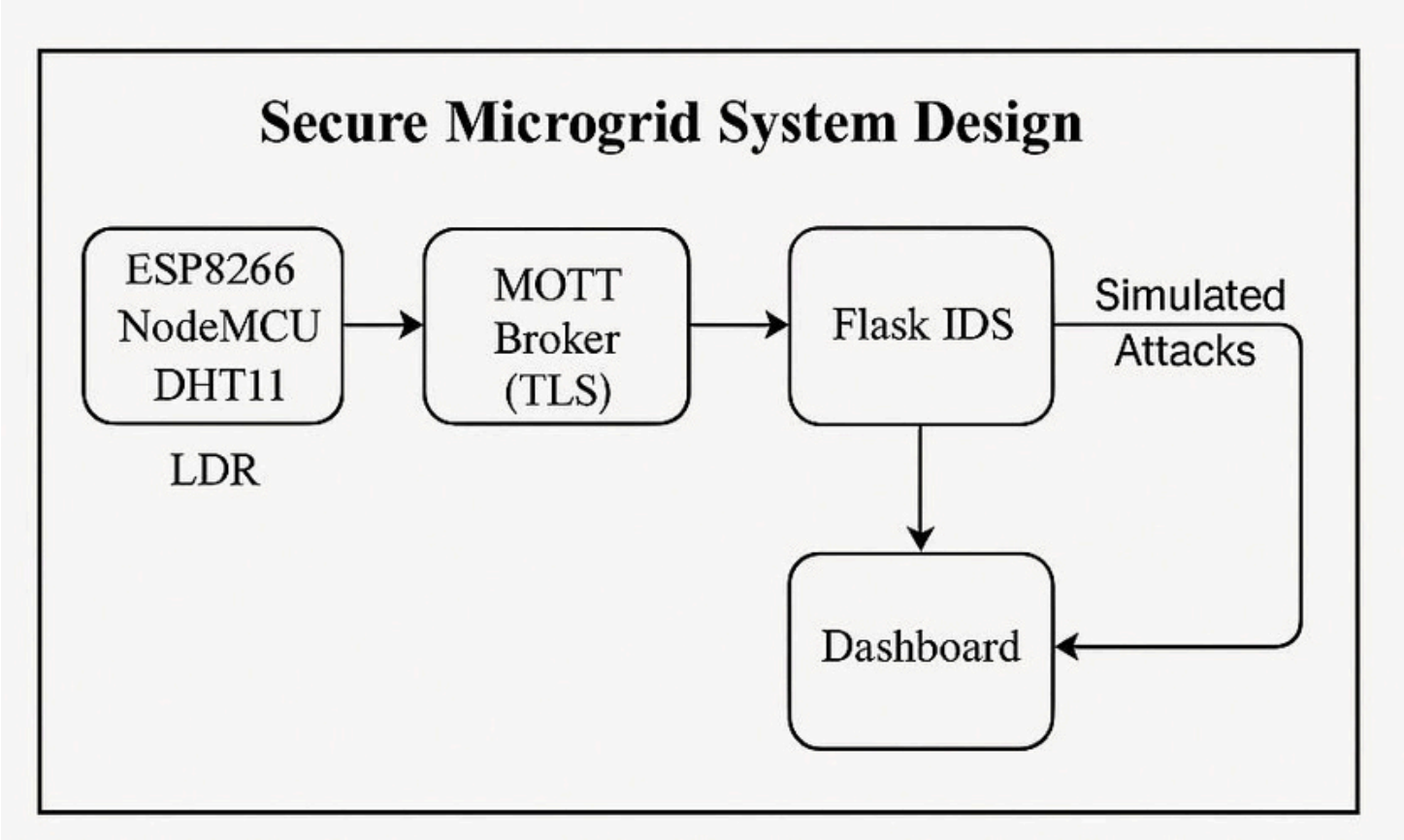
System Architecture

•Sensors readtemp,humidity,light

- ESP8266 preprocesses + sends JSON
- MQTT publishes securely (TLS 1.2)
- Flask backend subscribes + parses pack ets

•IDS detects anomalies and s po ofi ng

•Dashboard displays alerts and live data



IDS Model

- **Techniques Used:**
- Threshold rules
- Payload anomaly checks
- Message frequency analysis
- Device-ID authentication
- Replay detection using timestamp mismatch
- **Performance:**
- Accuracy: **86.3%**
- Precision: **85.2%**
- Recall: **86.7%**
- F1-Score: **85.9%**

Results: Sensor and IDS Performance

- DHT11 temp range: 28°C → 32°C
- Humidity: 57% → 63%
- LDR response: < 150 ms
- Stable 10-sec sampling
- No packet loss during readings
- **Conclusion:**Sensors reliable for microgrid environments
- True Positives: 104
- False Positives: 18
- False Negatives: 16
- True Negatives: 282
- **Detection Rate perAttack:**
- Replay → 92%
- Injection → 88%
- DoS Flood → 100%
- Spoofing → 81%
- MITM → 78%
- Brute-force → 100%
- Topic Hijack → 84%
- Tampering → 86%

Results: System Performance

END-TO-END
LATENCY: **3.5 SEC**

DASHBOARD
REFRESH RATE: **1 SEC**

MQTT DELIVERY:
99. 4%

UPTIME: **99%**

ALERT DISPLAY
DELAY: **< 0.8 SEC**

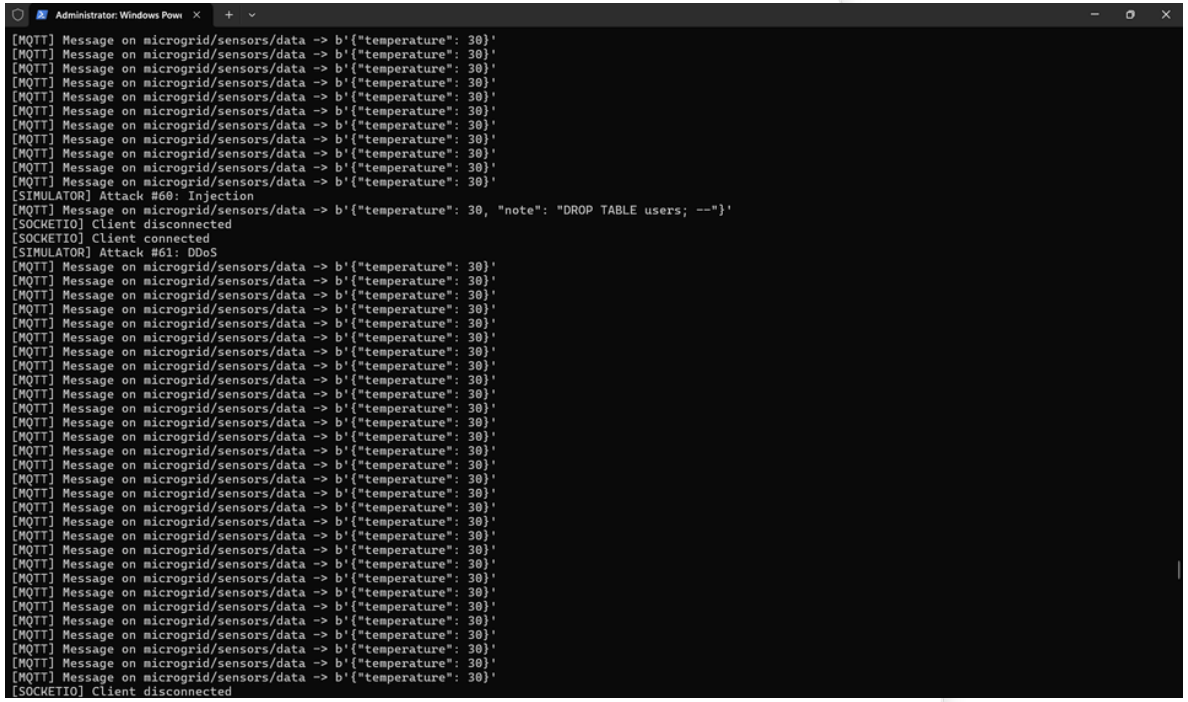
OVERALL
RELIABILITY: **HIGH**

Limitations and Future Enh anc eme nts

- Only DHT11 + LDR used (no electrical parameters)
- Attacks simulated artificially
- Only one ESP8266 node tested
- Rule-based IDS → miss advanced attacks
- No SCADA/EMS integration yet

- **FutureEnhancements**
- Add voltage & current sensors LSTM / GRU-
- based IDS for advanced detection Multi-node
- distributed IDS LoRaWAN/5G deployment
- TinyMLmodels on-device Blockchain-based log
- integrity SCADA + EMS integration
-
-

Results


Administrator: Windows Pow
[MQTT] Message on microgrid/sensors/data -> b'{"temperature": 30}'
[SIMULATOR] Attack #60: Injection
[MQTT] Message on microgrid/sensors/data -> b'{"temperature": 30, "note": "DROP TABLE users; --"}'
[SOCKETIO] Client disconnected
[SOCKETIO] Client connected
[SIMULATOR] Attack #61: DDoS
[SOCKETIO] Client disconnected


Microgrid Secure Monitoring Dashboard
Session: 1766
System Stats
Total packets analysed: 1204
Total threats blocked: 2212
Average detection time: 0.28 ms ms
Current Risk Score
100.00
Live Sensor Values
Temperature: 30.00 °C
Humidity: 50.00 %
Light: 500
Recent Alerts
Time Type Severity Message
2025-12-18 16:04:35 timing_attack MEDIUM Timing: rhythmic pattern (σ=0.002)
2025-12-18 16:04:35 ddos CRITICAL DDoS Attack: 28 req/5s
2025-12-18 16:04:35 replay HIGH Replay: Duplicate message
2025-12-18 16:04:35 timing_attack MEDIUM Timing: rhythmic pattern (σ=0.001)
2025-12-18 16:04:35 ddos CRITICAL DDoS Attack: 29 req/5s
2025-12-18 16:04:35 replay HIGH Replay: Duplicate message
2025-12-18 16:04:35 timing_attack MEDIUM Timing: rhythmic pattern (σ=0.001)
2025-12-18 16:04:35 ddos CRITICAL DDoS Attack: 30 req/5s
2025-12-18 16:04:35 replay HIGH Replay: Duplicate message
2025-12-18 16:04:35 timing_attack MEDIUM Timing: rhythmic pattern (σ=0.001)
Alert Log

Conclusion

- Built a secure, low-cost microgrid monitor
- MQTT-TLS ensured safe communication
- IDS achieved **86.3%**accuracy
- Dashboard showed real-time alerts effectively
- System proved reliable, fast, and ready for e xp an si on
- Supports modern microgrid safety requirements