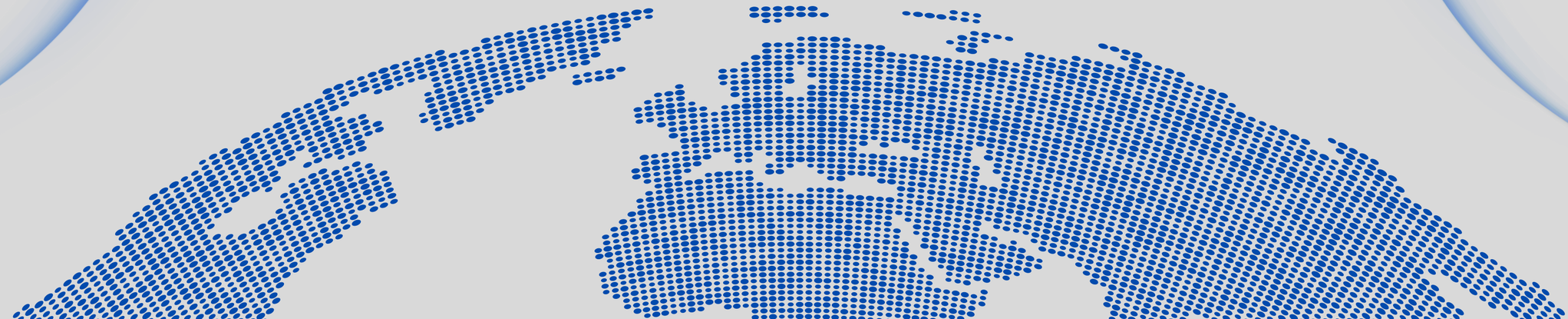
PROJECT GOUP #7

# FIELD-SENSITIVE ADAPTIVE ENCRYPTION FOR DIGITAL TWIN SYSTEMS

Presented by: Boyang Wang, Vaidehi Gohil



# INTRODUCTION

GROUP #7

- Digital Twin (DT) technology provides real-time monitoring and optimization in IoT systems.
- Security of DT data streams is critical since compromised data leads to incorrect predictions.
- Traditional encryption methods are often too heavy for resource-constrained IoT devices.
- There is a need for lightweight, adaptive, and fine-grained security mechanisms.

# PROBLEM STATEMENT

GROUP #7

Existing encryption schemes impose high computational and latency overheads.

Today ' s approach rely on static policies.


Sensitive and Non-Sensitive data are treated equally.

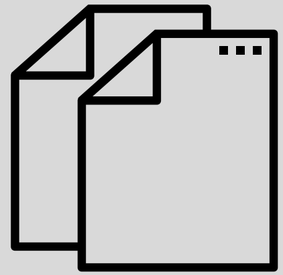
Digital-twin environment prone to multilayer threats

# PROPOSED SOLUTION

GROUP #7

## Selective Protection

## Field Sensitive Encryption



## Adaptive selector

# PROJECT WORKFLOW

GROUP #7

**STEP 1** Literature review on Digital Twin security and selective encryption

**STEP 2** Define threat model and identify critical vs. non-critical fields

**STEP 3** Design field-sensitive adaptive encryption framework

**STEP 4** Build simulation environment and implement baseline schemes

**STEP 5** Implement our adaptive encryption approach

**STEP 6** Run experiments and collect metrics (latency, CPU, memory, security)

**STEP 7** Analyze results and compare with baselines

**STEP 8** Prepare final report and presentation

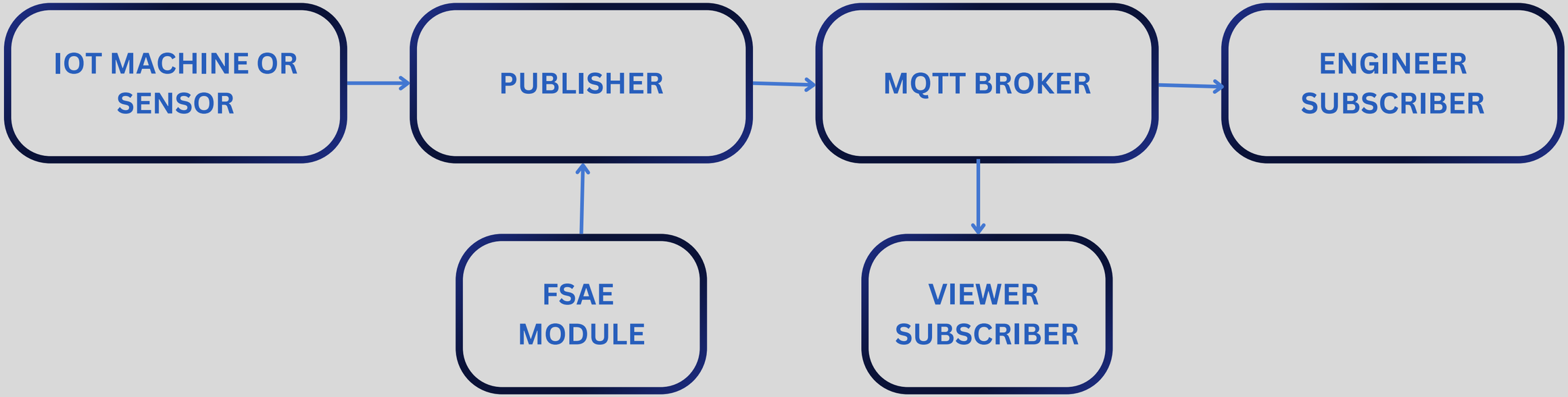
# DESIGN GOAL

GROUP #7

- Provide strong per-field confidentiality and integrity using AES-256-GCM for sensitive fields.
- Make encryption context-aware, adapting to network risk, user role and event state at runtime.
- Keep the system real-time friendly, adding sub-millisecond latency with no loss in throughput.
- Enforce least-privilege views, so different subscribers see only the data they're allowed to see.
- Remain easy to integrate, as a drop-in component for existing JSON/MQTT digital-twin pipelines.

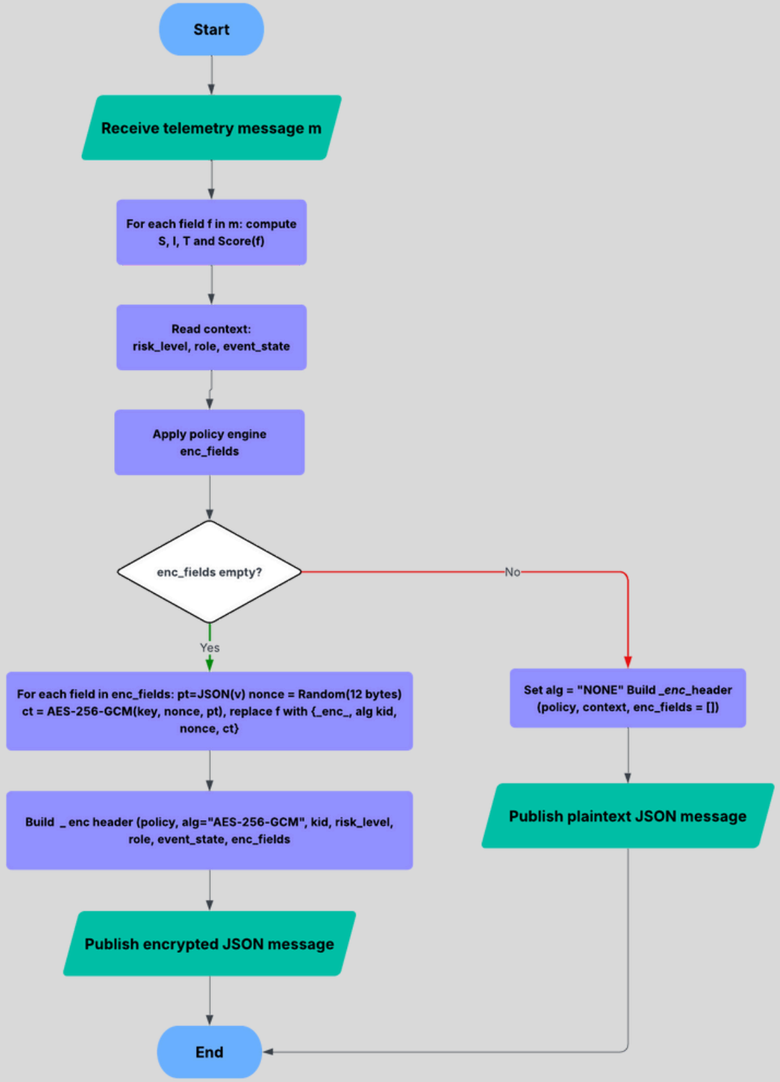
# BLOCK DIAGRAM

GROUP #7



# ALGORITHM FLOWCHART

GROUP #7



# IMPLEMENTATION AND SETUP

GROUP #7

publisher.py - generates telemetry, calls DFSE, publishes via MQTT

policy.py - S - I - T config + context rules

subscriber_engineer.py - role-based views

dashboard.py - simple console

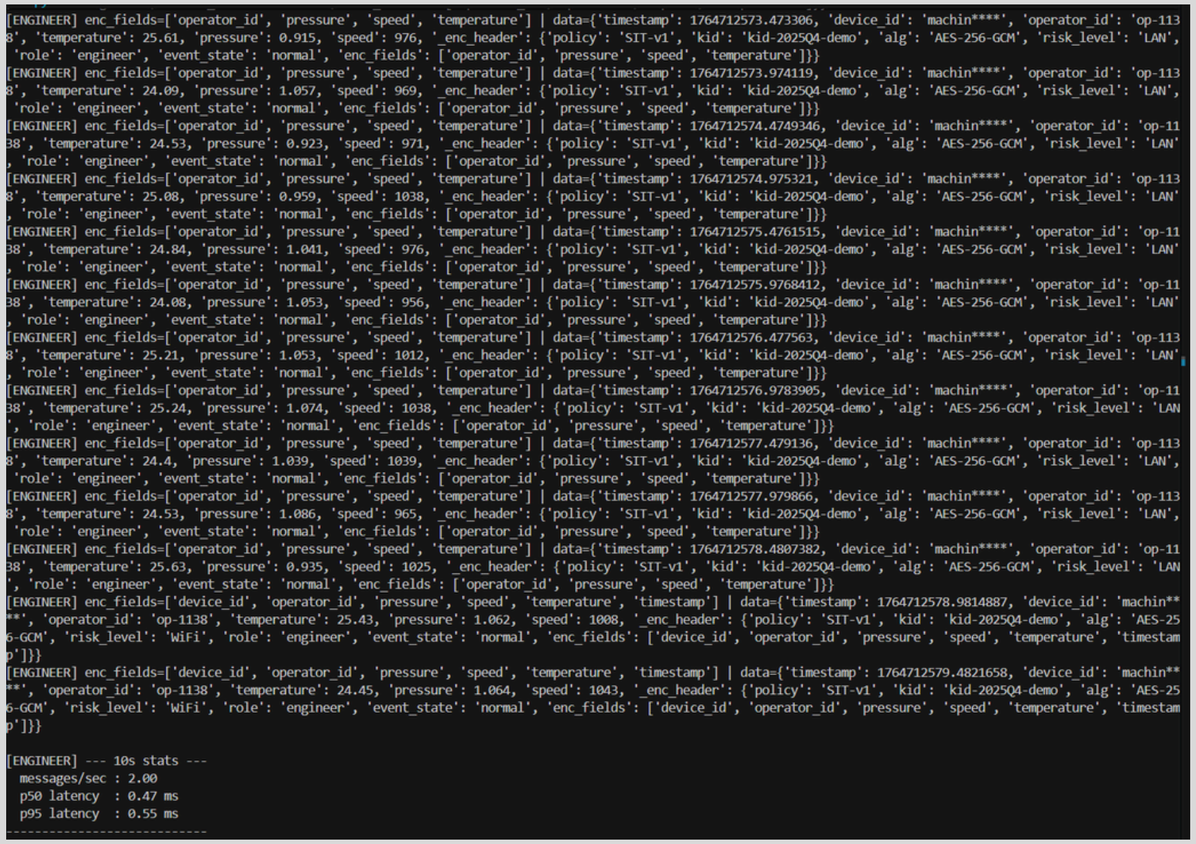
# EVALUTION METHODOLOGY

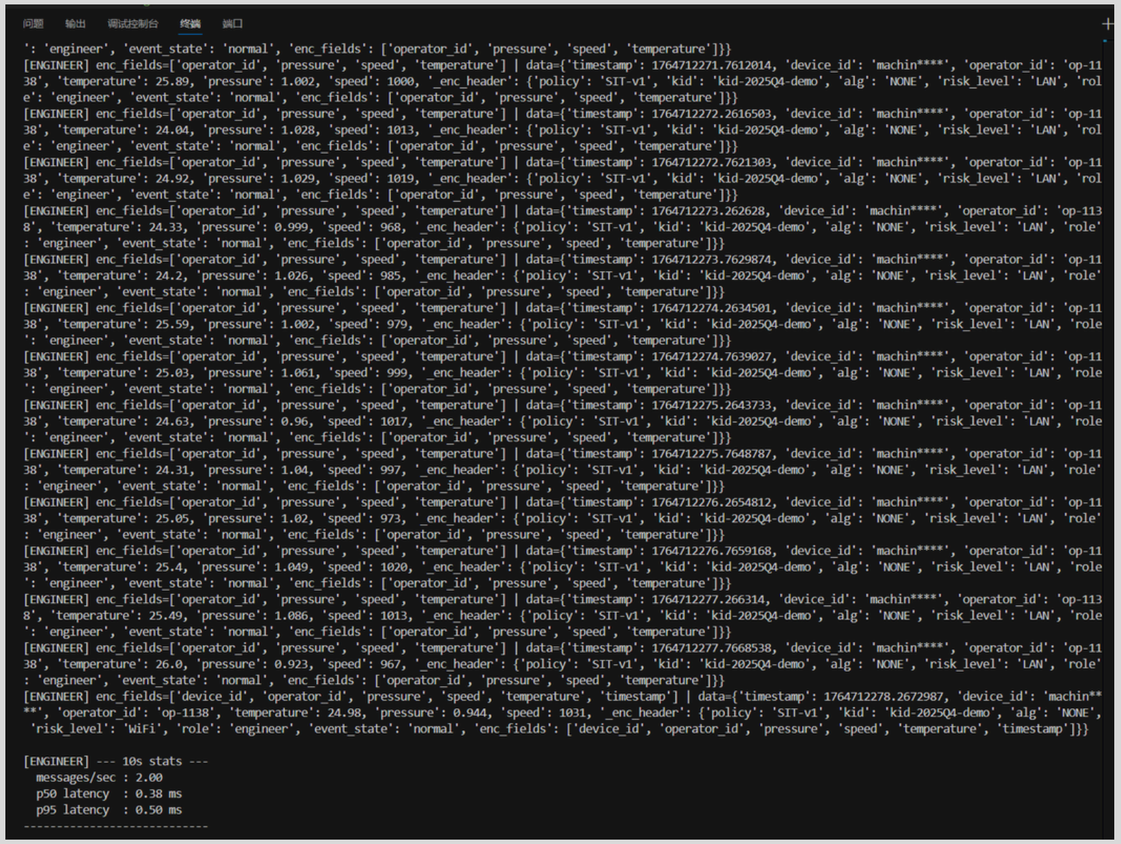
GROUP #7

- Compare two modes: crypto_off (no encryption, alg = NONE) vs crypto_on (DFSE with AES-256-GCM on selected fields).
- Generate telemetry at a fixed rate (2 messages/sec) and run each mode for a 10-second window.
- Measure and log p50 latency, p95 latency, and messages/sec in the subscriber; stats are printed at the bottom of the terminal every 10 seconds (as shown in screenshots).
- Use these logs to quantify the extra latency and throughput impact introduced by DFSE.

# EVALUTION METHODOLOGY

GROUP #7

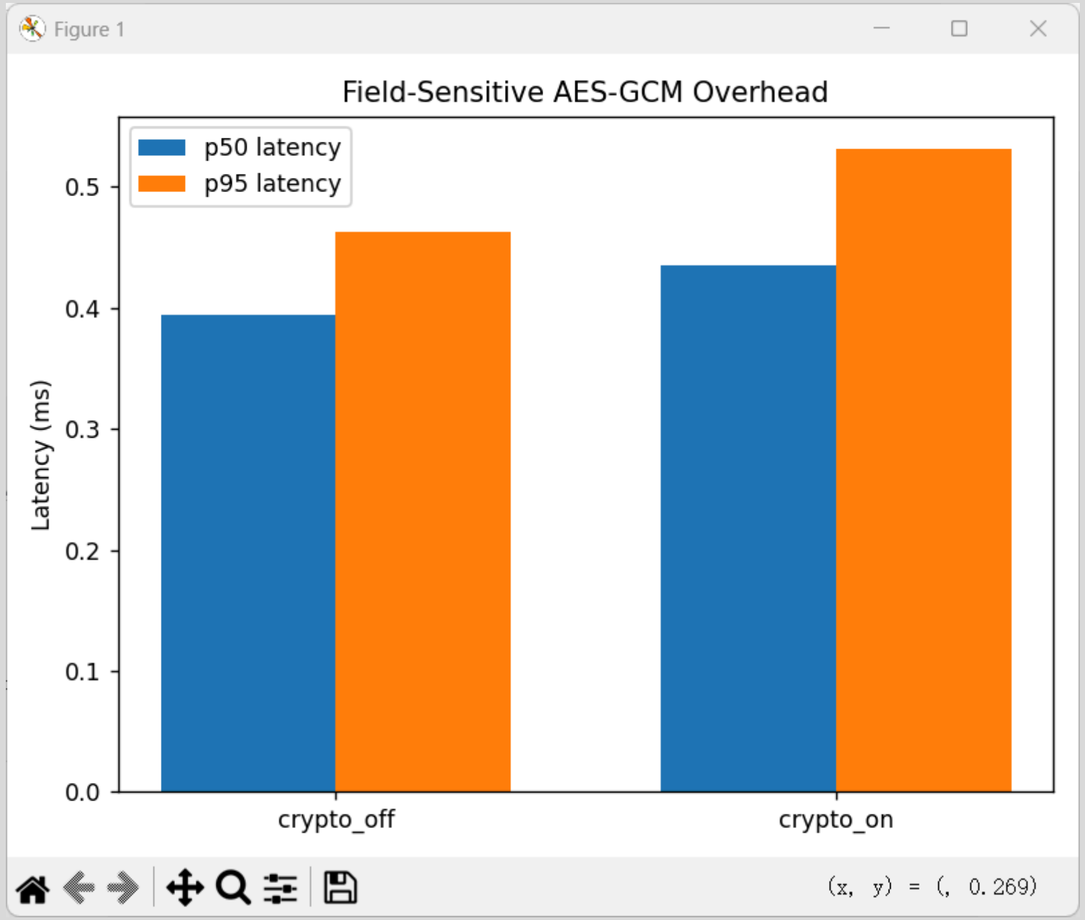


# RESULTS AND DISCUSSION

GROUP #7

- Latency impact is tiny
- Tail latency stays under control
- Throughput is unchanged
- Noise-level overhead
- Security vs performance trade-off is excellent
- FSE satisfies digital-twin timing constraints without requiring hardware acceleration or protocol changes.



# CONCLUSION

GROUP #7

- FSE adds context-aware, per-field AES-256-GCM on top of existing JSON/MQTT telemetry.
- Encryption decisions adapt to field risk + runtime context (network, role, event state).
- Measurements show sub-millisecond extra latency with no loss in message throughput.
- Role-based subscribers can perform partial decryption, enabling different views from the same encrypted stream.

# FUTURE WORK

GROUP #7

- Run hardware-in-the-loop experiments on real IoT gateways and industrial PLC/edge devices.
- Extend the policy engine with per-tenant / per-production-line rules and finer-grained masking.
- Integrate with central key management / HSM for key rotation and auditability.
- Explore higher message rates and multi-topic deployments to evaluate scalability in larger digital-twin systems.

# REFERENCES


[1] Jammula, Mounika, Venkata Mani Vakamulla, and Sai Krishna Kondoju. "Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system." Connection Science 34.1 (2022): 2431-2447.

[2] Sicari, Sabrina, et al. "Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware." International Journal of Information Security 20.5 (2021): 695-713.

[3] Perazzo, Pericle, et al. "Performance evaluation of attribute-based encryption on constrained IoT devices." Computer Communications 170 (2021): 151-163.

[4] Qureshi, Abdul Rehman, et al. "A survey on security enhancing Digital Twins: Models, applications and tools." Computer Communications (2025): 108158.

[5] Alcaraz, Cristina, and Javier Lopez. "Digital twin: A comprehensive survey of security threats." IEEE Communications Surveys & Tutorials 24.3 (2022): 1475-1503.

[6] Kaur, Kawalpreet, et al. "IoT CCTV Video Security Optimization Using Selective Encryption and Compression." International Journal of Advanced Computer Science & Applications 16.2 (2025).

# THANK YOU