IoT Security Capstone

Experiment Results, Insights & Recommendations

Tung Thanh Nguyen

01

The Threat: Unprotected IoT Pipelines

What happens when MQTT messages travel without protection?

Eavesdrop

Attackers can read unencrypted MQTT traffic in real time.
This exposes device data and system activity, enabling further attacks.

Inject Fake Data

Attackers can publish fake messages as trusted devices.
This can trigger false alerts or hide real system issues.

Replay Attack

Attackers resend old valid messages to the system.
This can mask real problems and delay detection.

Without encryption, authentication, and validation, attackers can see, send, and manipulate data freely, putting system operations at risk.

02

Defense Architecture: Four Layers of Protection

Each layer catches what the previous one can't.

Defense 1

mTLS Authentication

Verifies device identity using certificates

→ blocks unauthorized access.

Defense 2

HMAC Verification

Ensures messages are authentic and not modified

→ stops fake data injection.

Defense 3

Timestamp Validation

Rejects stale messages outside a time window

→ stops delayed replay attacks.

Defense 4

Sequence Counter

Tracks message order and rejects duplicates

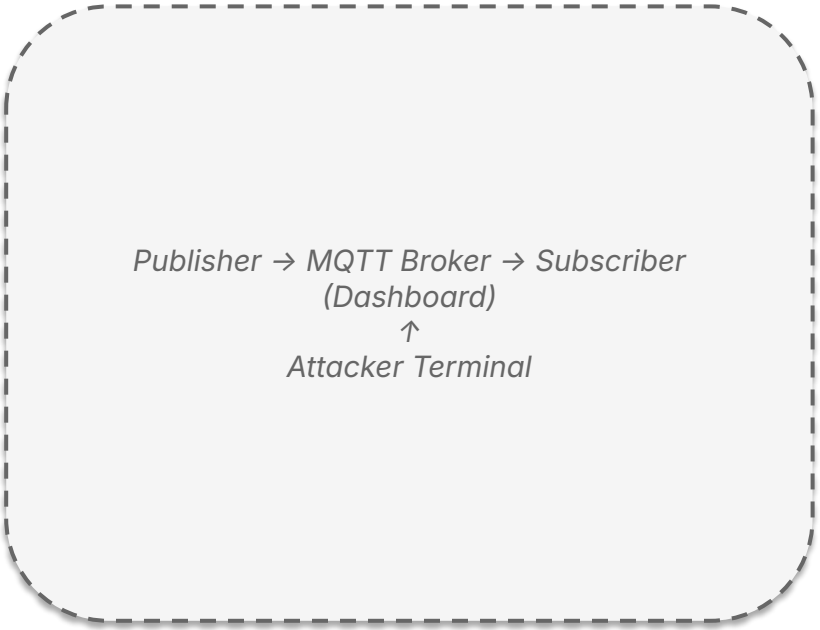
→ stops fast replay attacks.

Each layer protects against different attacks.
Removing one creates a gap attackers can exploit.

03

Experiment Setup: Three-Phase Attack Simulator

A controlled test against the live pipeline to verify every defense works.



Setup Process

- Started Mosquitto broker locally
- Ran publisher to send sensor data
- Ran subscriber as dashboard
- Used attacker terminal (mosquitto_sub / publish)
- Monitored traffic and system behavior

04

Attack Results: Every Attack Blocked

Which defense caught each attack phase — and why it works.

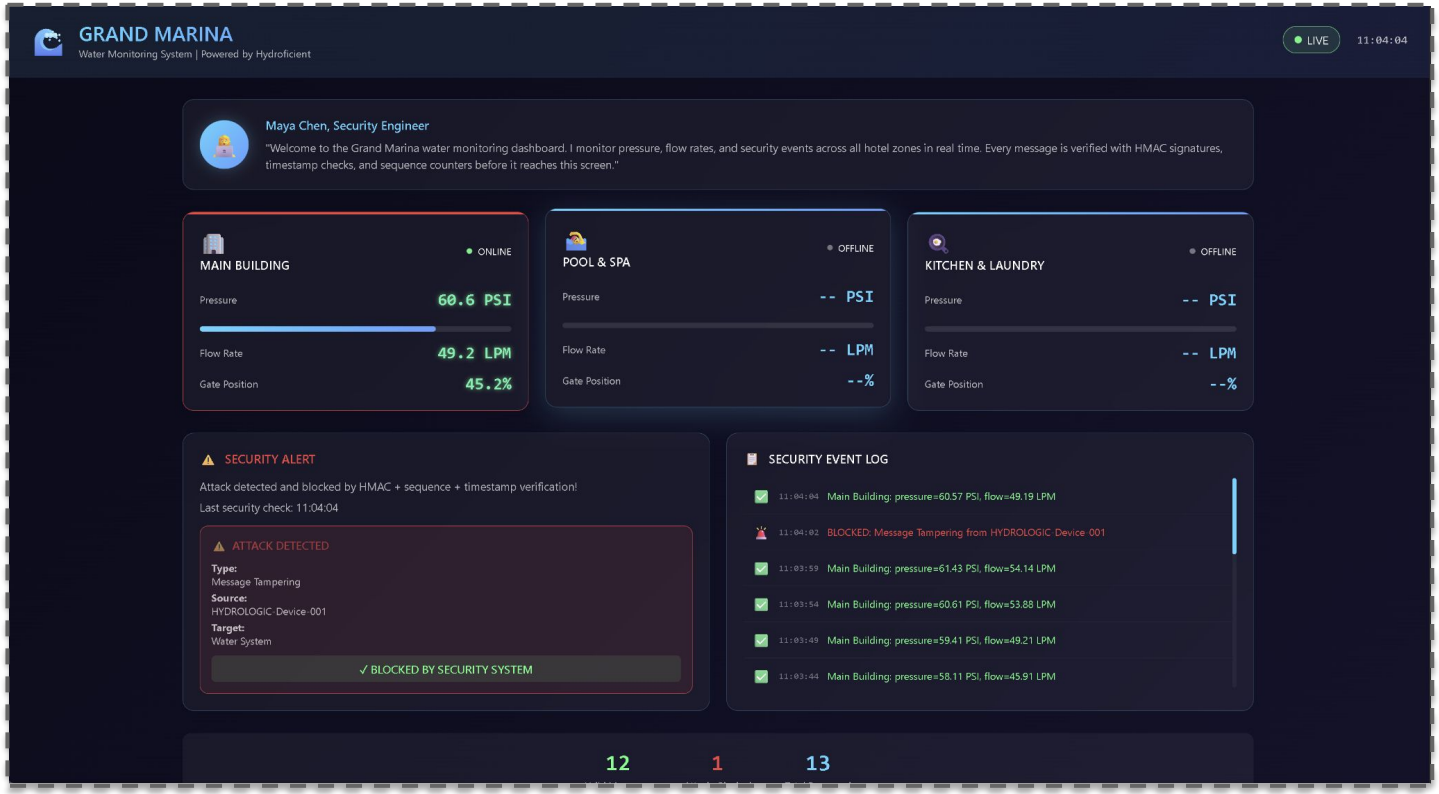
Attack Phase	What the Attacker Tried	Defense That Caught It	Why It Works
Phase 1: Eavesdrop	Subscribed to all topics to read data	mTLS	Attacker can listen but cannot modify or act
Phase 2: Inject	Send fake message with invalid HMAC	HMAC Verification	Attacker cannot generate valid signature without shared secret
Phase 3: Replay	Re-sent a captured valid message	Sequence Counter / Timestamp	Duplicate or stale messages are detected and rejected

✅ **Result: 0 attacks succeeded | 100% blocked**

05

Dashboard: Attack Detected

Red alerts, shaking zone cards — every attack caught in real time.



06

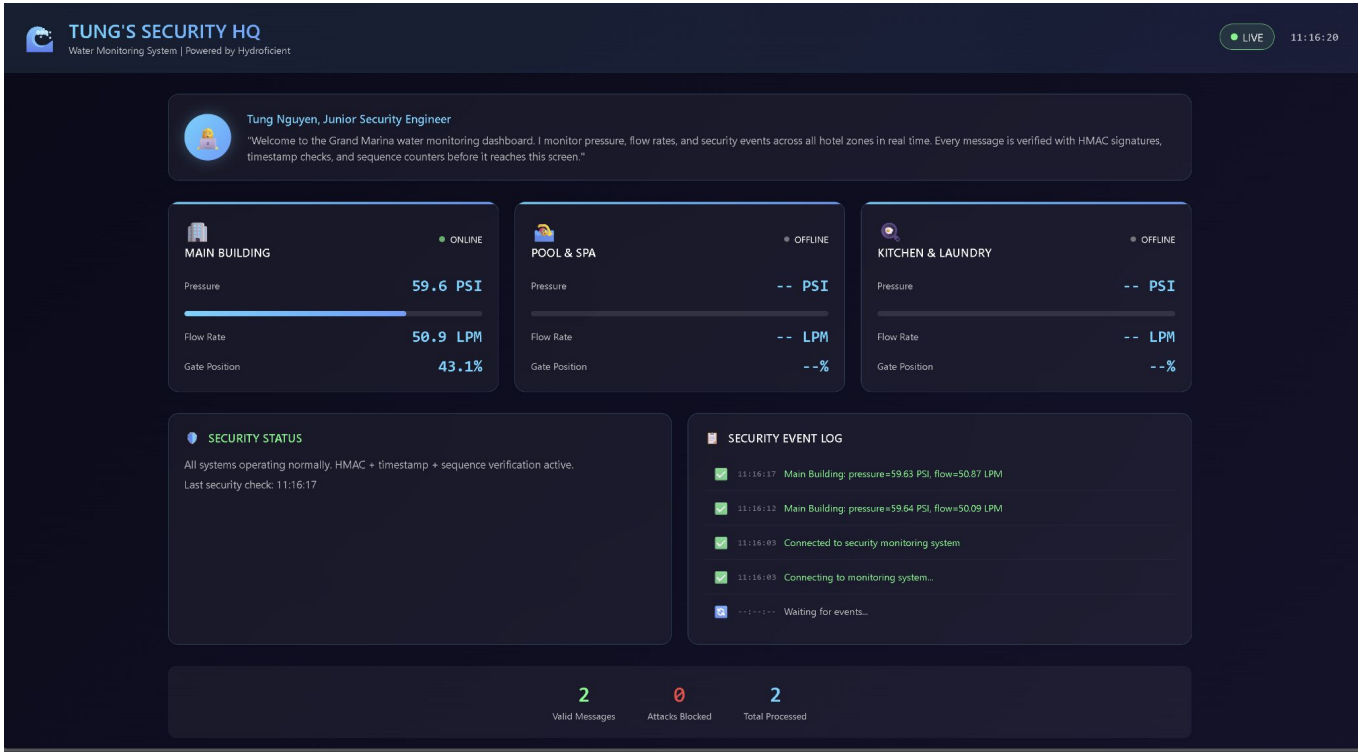
Stats: Attacks Blocked

The numbers tell the story — every attack rejected, every valid message accepted.

07

Custom Dashboard: Making It Mine

Personalized branding, AI-generated color theme, custom alert rules.



08

AI-Powered Anomaly Detection

Teaching the dashboard to catch what rules can’t — using machine learning.

Green

Normal

System operating within historical "baseline" parameters.

Orange

AI Flagged

Anomaly Detected. Data is mathematically "isolated" from normal patterns, even if it hasn't hit a hard limit yet.

Red

Blocked

Immediate cutoff triggered due to high-confidence threat detection.

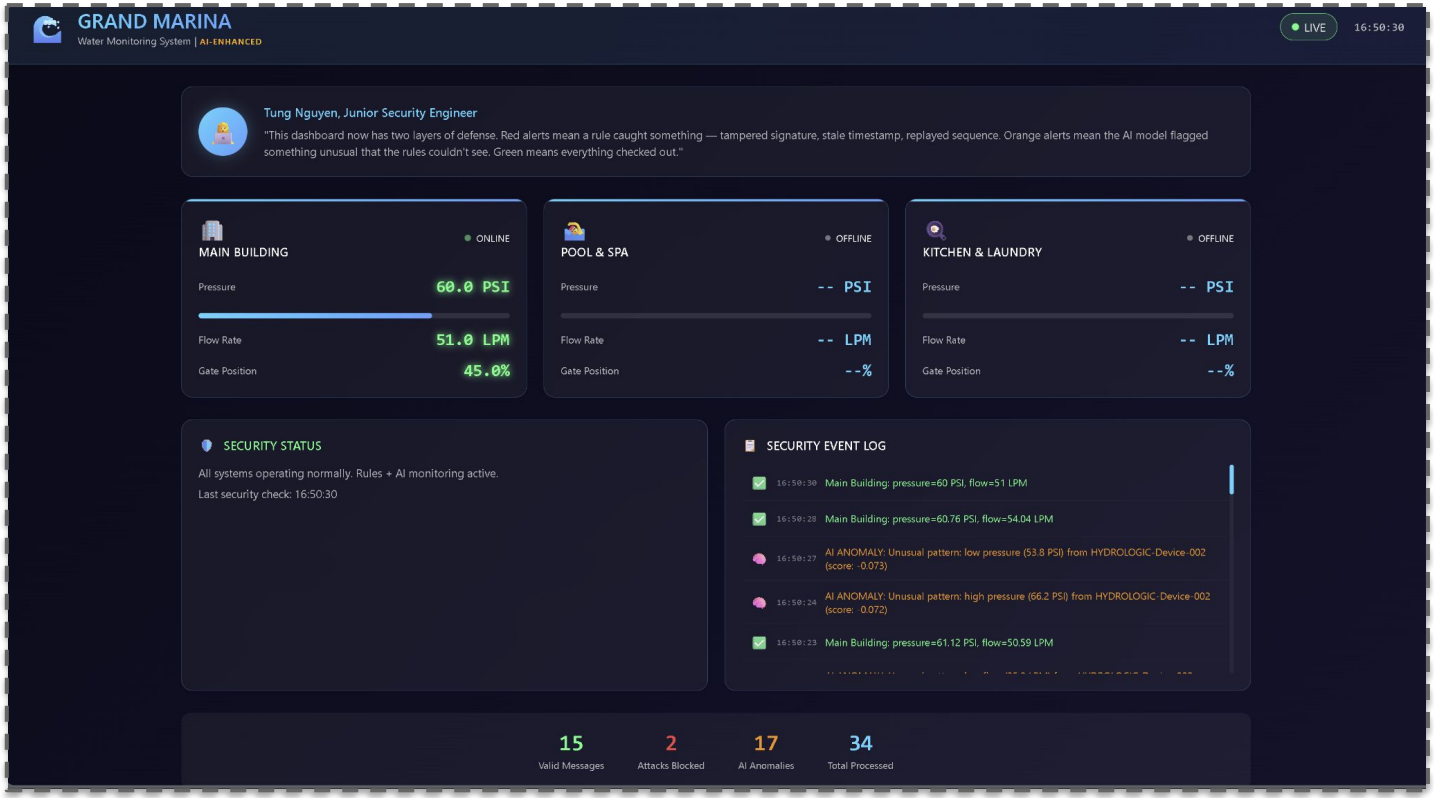
Model Used: Isolation Forest | Precision: 0.74 | Recall: 0.78 | F1: 0.76

Gradual Sensor Drift: Unlike rule-based "ceilings," the AI identifies slow, upward trends over several hours, spotting potential failures long before they hit a danger threshold.
Abnormal Combinations: The model flags "impossible" pairings—like high flow while a valve is 0% open—that individual rule checks would miss, signaling a bypass or sensor compromise.
"Near-Miss" Detection: The AI identifies erratic patterns that stay "just under" the alarm limit, allowing for proactive maintenance before a full system shutdown occurs.

09

AI Dashboard: All Three Layers Working

Rules and AI working together — green, orange, and red in real time.



Key Insights

What this experiment revealed about IoT security.

1

No single defense is enough

mTLS stops outsiders but not compromised insiders. HMAC stops forgeries but not replays. You need all layers working together.

2

Replay Attacks Are Subtle

Even valid messages can be malicious if reused. Without sequence and timestamp checks, they would bypass security.

3

Visibility Matters

The dashboard made attacks immediately visible. Without monitoring, attacks could go unnoticed.

4

IoT is Insecure by Default

Without added protections, MQTT allows anyone to read, send, and manipulate data freely.

Recommendations for Grand Marina

What should happen next to secure the IoT infrastructure at scale.

1. ## Enforce Strong Authentication

   Use mTLS for all devices and regularly rotate certificates to prevent unauthorized access.

2. ## Implement Message Validation

   Require HMAC, timestamps, and sequence counters for all device communications.

3. ## Deploy Access Controls (ACLs)

   Restrict which devices can publish/subscribe to specific topics to limit attack impact.

4. ## Enable Monitoring & Alerts

   Deploy real-time dashboards and logging to detect and respond to attacks quickly.

Questions?