Securing Privacy in MQTT-based Systems

#### **1. Comparison Table (Before vs. After PETs)**

| **Metric** | **Baseline (No PETs)** | **Enhanced (With PETs)** |
| --- | --- | --- |
| **Message Structure** | "John Doe: SOS at Lat: 10, Long: 20" | "#3847: SOS: Sector A3" (XOR-encrypted) |
| **Identifiability Risk** | High (real names) | Low (random IDs) |
| **Linkability Risk** | High (exact locations) | Medium (generalized sectors) |
| **Encryption** | None | XOR (basic) |
| **Latency Overhead** | 5 ms per message | 7 ms per message (+2 ms) |

#### **2. Effectiveness of PETs**

* **Pseudonymization**:
  + *Effectiveness*: High (hides identities).
  + *Overhead*: Minimal (random ID generation).
* **Data Minimization**:
  + *Effectiveness*: Medium (reduces precision but sectors are guessable).
  + *Overhead*: None.
* **XOR Encryption**:
  + *Effectiveness*: Low (easily breakable, but demonstrates the concept).
  + *Overhead*: +2 ms latency.

#### **3. Trade-Offs**

| **PET** | **Pros** | **Cons** |
| --- | --- | --- |
| Pseudonymization | Anonymizes victims | Requires ID management |
| Data Minimization | Reduces data exposure | Less precise for rescuers |
| XOR Encryption | Obscures payloads | Not cryptographically secure |

#### **4. Reflection on System Changes**

* **Behavior**: Victims now communicate anonymously, but rescuers see less precise data.
* **Design**: Added encryption steps increase code complexity.
* **Usability**: Users must trust the system to map IDs to real people (C2-side mapping needed).

#### **5. Privacy Threat Analysis (LINDDUN Framework)**

A diagram of a diagram

AI-generated content may be incorrect.

#### **1. Linkability**

* **Threat**: Attackers can correlate multiple messages to the same victim.
  + *Baseline*: Messages contain exact locations, making it easy to link victims.
  + *Enhanced*: Random IDs + generalized sectors break linkability.

#### **2. Identifiability**

* **Threat**: Victims can be personally identified.
  + *Baseline*: Real names/locations exposed.
  + *Enhanced*: Pseudonyms (e.g., Victim #3847) hide identities.

#### **3. Non-Repudiation**

* **Threat**: Victims cannot deny sending messages.
  + *Baseline*: Plaintext messages are attributable.
  + *Enhanced*: XOR encryption (weak) provides minimal deniability.

#### **4. Detectability**

* **Threat**: Attackers can detect communication.
  + *Baseline*: MQTT topics (victim/sos) are visible.
  + *Enhanced*: Topics renamed (victim/sos\_secure), but still detectable.

#### **5. Disclosure of Information**

* **Threat**: Sensitive data leaks.
  + *Baseline*: Locations/names sent in plaintext.
  + *Enhanced*: Data minimized + encrypted (XOR).

#### **6. Unawareness**

* **Threat**: Victims don’t know their data is exposed.
  + *Baseline*: No privacy warnings.
  + *Enhanced*: Code comments explain protections (improvement needed).

#### **7. Non-Compliance**

* **Threat**: Violates GDPR/other regulations.
  + *Baseline*: High risk (exposes PII).
  + *Enhanced*: Reduced risk (pseudonymization).