Enhancing Privacy in MQTT-Based Disaster Relief Communication using LINDDUN

Hussain Zainal, Rowida Alshair, Ahlam Alsubaie, Hussam Al Bakhat
George Mason University, hzainal@gmu.edu, ralshair@gmu.edu ,aalsuba6@gmu.edu, halbakha@gmu.edu

***Abstract* - Implementing an MQTT-based communication system for disaster relief requires an extensive evaluation of privacy risks to ensure operational resilience and the protection of sensitive data. Building on the system decomposition and business objectives established through PASTA, this report systematically applies a LINDDUN/PASTA hybrid privacy engineering framework to a disaster relief communication system utilizing MQTT messaging via drones. This report identifies and categorizes privacy threats by mapping the system's architecture and data flows, including linking, identifying, data disclosure, and non-compliance risks. Threats are analyzed within disaster operations, where privacy violations can lead to lower public trust levels and negatively impact the mission's success. The report proposes mitigations, including encryption, authentication enhancements, and pseudonymization, to ensure compliance with privacy standards. The final system architecture integrates these countermeasures without disturbing system functionality. This report emphasizes the importance of incorporating privacy considerations into emergency communication systems to ensure both operational reliability and compliance with privacy standards in crisis environments.**

***Index Terms* - LINDDUN, MQTT, Privacy Threat Modelling, PASTA, Disaster Relief**

I. Introduction

In the aftermath of natural disasters such as hurricanes, floods, and earthquakes, traditional telecommunication infrastructure is often rendered inoperable, leaving victims unable to reach out for help. Rapid and reliable communication is crucial for supporting search-and-rescue missions. Message Queuing Telemetry Transport (MQTT) protocol provides a scalable, low-overhead method for delivering emergency communications to disaster-stricken regions. However, while this system offers operational benefits, its decentralized, dynamic, and insecure nature introduces privacy risks. Sensitive personal data, such as the victim's location, health status, and identifying information, can be exposed, intercepted, or misused if sufficient privacy safeguards are not embedded into the system design.

This report applies the LINDDUN privacy engineering framework to address these challenges and systematically identify, categorize, and mitigate privacy threats within the MQTT-based disaster relief communication system. Unlike standard cybersecurity approaches, which primarily emphasize system availability and data integrity, the LINDDUN framework specifically targets privacy threats, offering an organized methodology for uncovering vulnerabilities related to linking, identifiability, data disclosure, unawareness, and regulatory non-compliance. This analysis highlights privacy risks unique to post-disaster risks through detailed modelling of system data flows, trust boundaries, and information exchanges between drones, field communication centers, the cloud, and rescue teams. Ultimately, this report aims to identify ways to enhance the communication system's resilience, legal compliance, and trustworthiness, ensuring that all victims receive critical aid without compromising their data privacy and protection rights.

This report extends the security analysis previously conducted using the PASTA framework. The system architecture, technical scope, and business objectives identified during the earlier analysis remain consistent with the PASTA analysis.

A. MQTT Security Technical Background

The Message Queuing Telemetry Transport (MQTT) protocol is a lightweight, publish-subscribe messaging system designed for environments with low bandwidth, high latency, or unreliable networks. Thanks to its efficiency and simplicity, MQTT has been widely adopted for Internet of Things (IoT) deployments and is well-suited for disaster relief systems, enabling communication among decentralized devices. However, MQTT was not designed with strong security in mind [1]. Its reliance on open transmission channels, minimal built-in authentication, and lack of end-to-end encryption make it vulnerable to a wide range of cyber threats. In disaster-stricken regions where network infrastructure is unreliable and physical security controls are minimal [2], these vulnerabilities are intensified, creating critical risks not only to the functionality of the relief system but also to the privacy and safety of both victims and responders.

Several security challenges emerge from MQTT's operational characteristics. The broker-based architecture

introduces a single point of failure: if the broker is compromised, adversaries can eavesdrop, tamper with, and disrupt all communications. Without transport layer encryption (such as TLS), MQTT traffic is susceptible to interception and unauthorized data collection. Insufficient client authentication leaves the system vulnerable to impersonation attacks, allowing malicious actors to inject false messages, impersonate drones, and mislead rescue teams. Furthermore, MQTT topics can reveal metadata about current operational activities, making traffic analysis and pattern detection easier for adversaries.

Unlike conventional IoT deployments protected by firewalls, the disaster environment amplifies these risks. Disaster relief systems are often deployed hastily under chaotic conditions and cannot enforce strict security configurations. Devices may be lost, stolen, or tampered with on the ground. Moreover, victims who transmit sensitive data, such as their GPS coordinates, are physically vulnerable if these communications are intercepted or disclosed without authorization.MQTT's design limitations and operational reliability require a privacy-focused thread modelling approach.

B. *Purpose of Privacy Threat Analysis*

In modern disaster relief scenarios, where traditional communication infrastructure is often compromised, alternative communication systems, such as MQTT-based drone communications, can be utilized to ensure life-saving coordination. Disaster-relief systems operate in high-risk, time-sensitive environments and collect sensitive information, including:

- Victim Locations
- Distress messages
- Operational metadata

Privacy violations in these contexts can undermine trust, expose vulnerable victims to even further harm, and create long-term risks. This report aims to address privacy risks within the MQTT disaster-relief communication system.

This report adopts a structured, risk-based methodology to model and mitigate privacy-related threats. While traditional modeling frameworks, such as STRIDE, primarily focus on security system-centric threats, including spoofing and denial-of-service attacks, they are not well-suited to address privacy-specific concerns, such as the exposure of personal identities. To address this issue, this report will incorporate the LINDDUN privacy threat modelling framework, which provides a taxonomy of privacy threats tailored to the protection of individuals rather than the system itself and its assets. These include Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, & Non-compliance.

Rather than applying LINDDUN as a standalone approach to analyze threats, this analysis embeds LINDDUN into the multi-stage PASTA (Process for Attack Simulation and Threat Analysis) methodology. PASTA emphasizes aligning technical risk analysis alongside the systems business and operational objectives, which is crucial in emergency systems. By adapting LINDDUN to fit this staged methodology, the analysis ensures that privacy concerns are considered throughout the system, from system description and technical scope to threat elicitation and attack simulations. This hybrid methodology ensures that privacy threats are identified and addressed without compromising the system decomposition and business objectives.

The approach also reflects the principle of Full Functionality, in which system performance and privacy are not seen as mutually exclusive goals but as coexisting priorities. A Buisness Impact Matric (BIM) is introduced to asses how each threat affects not just data protection, but also the systems ability to perform its operational missions. This ensures that privacy-enhancing technologies (PETs), such as encryption, pseudonymization, or consent awareness, are applied to prevent privacy violations even in the chaos of disaster conditions.

By the end of the report, the reader will gain a clear understanding of privacy risks that arise in disaster communication systems and how these risks differ from conventional security threats. The reader will also learn how the risks discovered can be addressed within a staged privacy engineering process. The goal is to demonstrate that it is possible to engineer a system that can effectively meet its operational objectives while maintaining an ethically and legally sound approach to treating personal data.

II. System Architecture & Overview

System overview

The disaster relief system is designed to restore communication during emergency scenarios where conventional infrastructure, such as cell towers and the Internet, is unavailable. It uses edge devices like smartphones, drones, local servers running Mosquitto (an MQTT broker), and cloud-based components to construct a robust, secure, and adaptable communication network. These elements deliver life-saving information, even in highly challenging environments.

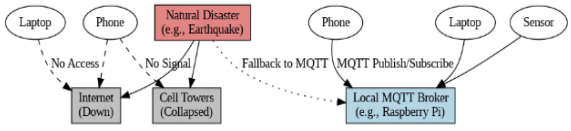

Figure 1. Conceptual System Illustration of Disaster Scenario and MQTT-Based Communication Fallback

A. *Purpose and Design Goals*

The catastrophic failure of communication infrastructures during large-scale natural disasters, such as Hurricane Katrina, underscored the fragility of centralized telecommunication systems. In that event, extensive damage to cellular towers and public radio systems, exacerbated by widespread power outages, rendered emergency communication channels inoperable. First

responders, including fire services, emergency medical personnel, and law enforcement, were effectively isolated from command centers and one another. The systemic collapse of both primary and auxiliary communication frameworks left significant geographic areas devoid of operational connectivity for extended periods [3], paralyzing situational coordination and impeding the timely delivery of humanitarian aid.

A parallel collapse was observed in the 2010 Haiti earthquake, where seismic activity triggered the destruction of rooftop-mounted GM towers and critical state-operated telecommunications nodes. This infrastructural decimation severely constrained data dissemination pathways and created informational vacuums, leaving affected populations unable to transmit distress signals or receive crucial updates [4]. The inability to establish real-time communication created isolated response islands and prolonged suffering in the impacted regions.

In response to such vulnerabilities, the proposed MQTT-based disaster relief architecture emerges as a robust alternative. MQTT (Message Queuing Telemetry Transport), a lightweight and publish-subscribe-based messaging protocol, is engineered for constrained environments with intermittent connectivity and low bandwidth. Its operational resilience stems from its ability to transmit concise payloads with minimal overhead, while its decoupled architecture enables asynchronous communication across distributed endpoints. Moreover, MQTT's inherent support for fallback mechanisms and broker-managed topic hierarchies facilitates graceful degradation and recovery in unstable network topologies.

The principal objective of this system is to furnish a dependable, field-deployable communication infrastructure that remains functional in the absence of conventional internet connectivity. By enabling the dissemination of high-priority data such as victim locations, distress signals, and situational telemetry over a localized wireless mesh, the system ensures continuity of communication in austere environments. The broker-centric design enforces controlled message distribution, ensuring data integrity and confidentiality by isolating topic access to authorized subscribers. Furthermore, its modular, scalable configuration allows phased deployment, enabling first responders to incrementally extend coverage and capacity in evolving disaster zones.

B. System components and architecture

The proposed MQTT-based disaster relief system's architecture is engineered to restore communication capabilities during emergencies where traditional infrastructure has been rendered inoperative. It is composed of distributed and collaborative components, namely victim devices, volunteer drones, MQTT brokers, field command applications, and a cloud backend—that work in concert to transmit, relay, and store critical situational data. This section outlines each component and its operational relevance within the privacy-aware system design, building upon the foundational architecture presented in the initial security-centric analysis.

1. Victim Device (User Application)

The victim device is the first point of contact in the MQTT-based disaster relief system. It plays a key role in starting communication when traditional infrastructure like mobile networks or the internet, is down. These devices are typically smartphones running a custom emergency app, which connects to nearby volunteer drones using local Wi-Fi. This setup allows the system to work without relying on damaged or unavailable networks in disaster areas. Adding to this, the component crosses the Trust Boundary Zone 1, and that is where you found the unsecured local Wi-Fi links are safeguarded utilizing TLS and pseudonymized payloads, decreasing the risk of privacy breaches throughout the initial data gathering.

The emergency app is designed for quick and straightforward use, especially in high-stress situations. It helps people send distress messages with just a few taps. Each message includes essential details such as the user's location (via GPS), the time the message was sent, how urgent the situation is, and any optional notes. The app also includes accessibility features like voice commands and confirmation feedback to support users who may be injured or under extreme stress. In some situations, the app can even send messages automatically at regular intervals if the user is unresponsive. To respond to privacy principles, the design restricts data gathering to fundamental assignments and stops needless exposure of personally identifiable data, aligning with LINDDUN's identifiability and linkability protections.

When the app finds a drone within range, it starts a secure short-term connection. Then it sends the message using the MQTT protocol on specific topics like aid/request or user/status. Because battery life is crucial in emergencies, the app uses short, efficient messages and keeps background activity minimal. The message is encrypted using TLS and digital certificates if the device supports it. If not, the message is still sent, but it's marked as 'unverified' so the system knows it may not be fully secure. This handoff begins the secure flow via the system architecture, making sure that subsequent parts such as the broker and cloud bridge, may apply additional privacy and security layers.

Since the victim device is sending personal data, it's important to protect user privacy. If messages are sent without encryption or contain too much identifying information, there's a risk that outsiders could track or identify users. The app includes privacy features that follow the LINDDUN privacy framework to reduce this risk. These include:

- Removing any data that isn't necessary

- Using fake IDs or tokens instead of real user information
- Randomizing the times messages are sent
- Grouping messages together to hide patterns

These privacy-preserving measures immediately address LINDDUN threat groups of identifiability, linkability, and disclosure, making sure that the system architecture safeguards the data in sending and decreases the risk of privacy violations across trust boundaries.

Looking ahead, the app could be improved by adding support for biometrics or digital identity systems that don't sacrifice user privacy. It could also allow nearby devices to share messages with each other when no drones are available, creating a basic mesh network.

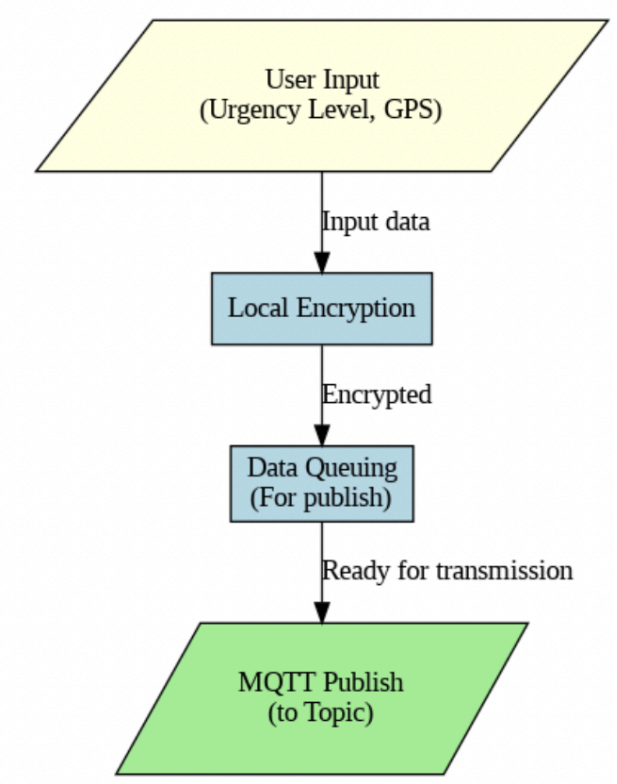

Figure 2. Victim Device Data Lifecycle

2. Volunteer Drones

Volunteer drones are one of the most important components in the MQTT-based disaster relief system. These drones act as flying communication hubs, allowing the system to function even when local infrastructure like mobile networks, fiber lines, or cell towers is down. They operate above disaster-affected regions, gathering information and helping deliver critical aid messages between victim devices and field responders. Without these drones, victims in remote or damaged areas may have no way to communicate their needs.

Each drone is equipped to function both as a Wi-Fi access point and as an MQTT client. As the drones fly over the area, they continuously scan for Wi-Fi signals from smartphones running the disaster response app. When a distress signal is detected, the drone begins a secure session, checks the authenticity of the source using digital certificates, and collects the data. This data typically includes the victim's GPS location, the time of the request, the urgency of the situation, and any additional comments provided by the user. Once the message is verified and formatted correctly, the drone sends it to the MQTT broker over secure communication channels using topic tags like aid/request and drone/data

From a privacy point of view, the drone's data gathering activities (covers GPS, visual/audio feeds, and telemetry) begin identifiability and unawareness risks under the LINDDUN framework. For instance, continuous GPS tracking could permit connecting movement patterns to single victims, and onboard sensors might gather important and significant environmental data with no explicit user consent.

In addition to acting as message relays, drones gather other helpful telemetry data to support response planning. This data includes the drone's own flight status, altitude, battery life, GPS path, and in some cases, sensor readings such as local temperature or humidity. Some advanced drones also include built-in cameras or microphones to provide audio-visual context for the disaster zone. All of this information is passed back to the MQTT broker and made visible on the field operations dashboard used by response teams. These telemetry and audiovisual data streams might add important, significant, or identifiable data and information such as the GPS coordinates, recorded conversations, or even victim images. The system puts privacy-preserving measures like anonymization, access control, and elected disclosure, which align with LINDDUN privacy categories such as unawareness and disclosure of information and data. These telemetry and audiovisual data streams might add important, significant or identifiable data and information such as the GPS coordinates, recorded conversations, or even victim images. The system puts privacy-preserving measures like anonymization, access control, and elected disclosure, goes with LINDDUN privacy categories such as unawareness and disclosure of information and data.

The use of drones allows the system to adapt in real time to changing conditions. For example, drones can be redirected to high-priority zones if new victims are discovered or if weather conditions threaten certain areas. This flexibility ensures that the most critical zones are always within reach of the communication network. At the same time, their independence means that security becomes even more important, since human operators do not directly control every drone's every action. This dynamic adaptation also increases privacy challenges, as independent drone decisions may expose important working data/information or victim places with no explicit user consent. Privacy controls are embedded at this stage to make sure choices respect linkability and unawareness protections.

Drones use Transport Layer Security (TLS) to encrypt all data they send to the broker to ensure secure communication. Every drone must have a valid certificate issued by the system in order to send or receive messages.

The broker checks these certificates and blocks access if a drone's credentials are not valid or have been revoked. This helps prevent unauthorized devices from injecting false or harmful data into the system. While these technical protections decrease the risk of tampering or message spoofing, extra privacy controls, like minimizing stored drone metadata, utilizing pseudonymous drone IDs, and restricting retention of significant and important payloads, are used to decrease the likelihood of privacy violations such as unofficial disclosure or linkability between transmissions.

To label privacy threats recognized through the LINDDUN analysis, the system combines layered privacy-protecting mechanisms at the drone level. These mechanisms aim to secure the operational data and to decrease the risk of revealing significant personal information and data, like user locations, health status, or situational context, as data goes across system components.

To decrease the privacy risk, the system includes several protections designed for security and for safeguarding significant personal data and information:

- Rate Limiting: Stops a drone from flooding the broker with a lot of messages, decreasing the risk of crushing the system and leaking identifiable traffic patterns.
- Behavioral Filtering: Finds and stops unsure or distorted data that might have privacy-violating payloads or expose important metadata.
- Authentication Filters: Makes sure that only confirmed drones with authenticated certificates may transfer important information/data, decreasing risks of impersonation and unofficial data injection.
- Location Validation: Examine that reported locations go with the expected mission boundaries, decreasing risks of sending wrong or misleading possible data that might compromise individual privacy.
- Tamper Detection: Watches drones for signs of compromise, making sure any changes or hijacked devices do not leak sensitive user data or relay unofficial telemetry.

Together, these protections directly address privacy risks that go with LINDDUN groups like Linkability, Identifiability, Disclosure of Information, and Detectability, making sure the system restricts unneeded reveals of personal or situational data at every stage.

While drones cover local storage to keep and save the messages when communication with the broker is for the moment unavailable, this establishes a critical privacy concern. If a drone is not found, robbed, or compromised, any preserved personal or situational data like: victim places/positions or urgent requests, could be revealed. To mitigate this, the system applies encryption-at-rest for all local drone storage and adds harsh retention limits, making sure that only minimal, privacy-preserving data is for the moment cached. The moment that connectivity is restored, stored messages are safely transmitted through encrypted channels, and local copies are removed to avoid long-term reveal risks.

Looking ahead, future developments and updates might incorporate privacy-preserving edge computing on drones, permitting them to locally filter or anonymize significant data prior to transmission. For instance, drones might strip identifiable metadata, remove data to decrease individual traceability, or apply the privacy-preserving AI models that find critical situations without storing or sharing sensitive personal data. These improvements would make sure that even as drones take on more complicated tasks, the system stays aligned with privacy rules by decreasing the collection, utilization, and disclosure of personally identifiable information.

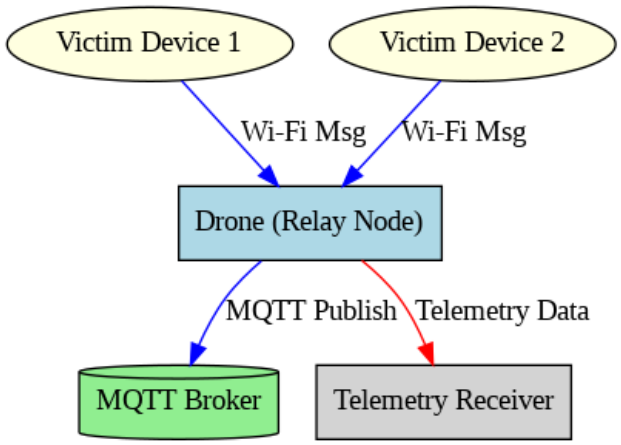

Figure 3. Drone Communication and Relay Flow

This data flow focuses on the critical privacy points, as significant personal data such as: the victim locations and urgency details goes through drones to the MQTT broker. To protect privacy, every single handoff applies encryption (TLS), utilizes pseudonymized payloads, and puts harsh topic and certificate-based access controls, making sure that only trusted and minimal data flows between components.

3. MQTT Broker

The MQTT broker is the central component of the disaster relief system's messaging architecture. It functions as the system's communication hub, where all incoming messages are received, processed, and routed to their appropriate destinations. Implemented using Eclipse Mosquitto—a lightweight, open-source broker—the component is deployed on robust local hardware such as a hardened laptop, single-board computer (e.g., Raspberry Pi), or network appliance (e.g., pfSense firewall) located at the field command center. It plays a critical role in enabling reliable, asynchronous, and scalable message delivery between victims, drones, field responders, and cloud services. Because of the main role, the broker takes responsibility for significant user data and has to enforce harsh privacy controls to stop and block reveal of identifiable or location-based information.

All communications from victim devices and drones are published to the broker using MQTT topic structures.

These topics are logically separated to streamline data handling and ensure system modularity. Common topics include aid/request for distress messages, rescue/instructions for responder directives, drone/data for telemetry, and system/logs for system events. The broker subscribes to these topics, maintains message queues, and distributes content only to authorized subscribers based on their topic subscriptions and access control privileges. These subject structures have to be carefully designed to avoid revealing unnecessary metadata and make sure only the minimum required information is shared, following data minimization principles.

Security is one of the broker's most important responsibilities. In its default configuration, Mosquitto does not enforce encryption or authentication, posing serious risks in real-world deployments. To secure the broker, Transport Layer Security (TLS) is enabled to encrypt all MQTT communications, and mutual authentication using X.509 certificates is enforced. This ensures that only authorized clients, drones, field devices, or cloud bridges can publish or subscribe to specific topics. These measures will safeguard against untrusted entry and block privacy violations by ensuring that significant identifiers or personal data are not intercepted or misused.

To control access, the broker uses Access Control Lists (ACLs) that define which clients can interact with which topics. This helps segment the data flows and minimizes the risk of data leakage or unauthorized access. For example, only drones with specific credentials can publish to drone/data, while only field applications can subscribe to rescue/instructions. Logs of access attempts and system behavior are maintained for auditing and intrusion detection purposes. ACLs play an important role in privacy protection by ensuring that only necessary components enter certain data streams, decreasing the surface area for possible privacy breaches.

The broker also supports bridging functionality, which is used to connect the local system to the cloud environment once internet connectivity is restored. In this configuration, selected topics are forwarded to a cloud-hosted MQTT broker (e.g., AWS IoT Core), enabling remote monitoring, data archival, and strategic coordination by national or regional agencies. When sending data to cloud systems, privacy risks increase because of the cross-jurisdictional data transfers, requiring careful management of consent, retention, and data residency policies.

From a privacy standpoint, the MQTT broker processes sensitive information such as GPS coordinates, timestamps, device identifiers, and even health or emergency statuses. Thus, it represents a potential point of privacy leakage if not properly secured. To mitigate these risks, the broker ensures end-to-end encryption, enforces strict access policies, and avoids storing sensitive information beyond short-term queue durations unless explicitly configured to forward it to persistent databases.

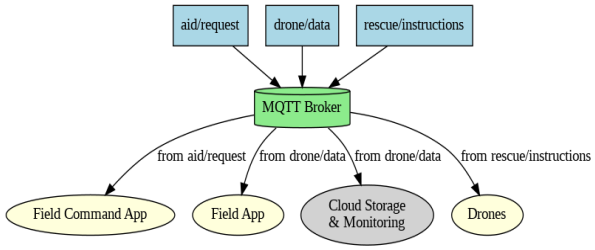

Figure 4. MQTT Broker Routing Logic

This figure focuses on the privacy-relevant flows, demonstrating where encryption, access control, and data minimization are important to stop leakage.

4. *Field Command Center Application*

The Field Command Center Application acts as the operational dashboard for the disaster relief system. It is installed on ruggedized field devices used by first responders and rescue coordinators. Its main role is to display real-time data collected from drones and victim devices via the MQTT broker and provide an interface for responders to make informed decisions and issue commands. The application supports both monitoring and bi-directional communication, allowing teams to receive alerts and respond with instructions. Due to the field dashboard taking responsibility for the significant distress and location data, it is important that only trusted personnel are able to view, enter, or take actions on this information to uphold user privacy and block misuse.

The dashboard aggregates data from MQTT topics such as aid/request, drone/data, and rescue/instructions. It provides a geospatial map view that plots victim locations, drone positions, and operational zones. Distress messages are shown with metadata such as urgency level, GPS coordinates, and time of submission. This helps prioritize tasks and allocate resources effectively. The dashboard also includes filters to sort messages based on urgency, location, or status, allowing field personnel to focus on high-priority cases. Privacy protections are implemented at the dashboard level to limit which responders are able to view full user information, making sure that only mission-relevant data is visible and that unnecessary reveal of personal identifiers is prevented.

In addition to passive monitoring, the field application allows users to issue commands. For example, responders can send routing instructions to drones or acknowledgement messages back to victims. These commands are published to topics like rescue/instructions, and the MQTT broker ensures they are delivered to the correct recipients. This bi-directional capability closes the communication loop, enabling a fully interactive response workflow. To safeguard the user's privacy, command messages are created to avoid embedding personally identifiable data, and system logging makes sure that any significant interactions are recorded for accountability.

The application supports encrypted storage for local data and uses TLS for all broker communication to ensure security and data integrity. Role-based access controls are implemented to restrict functionality based on the user's

responsibilities. Logs of all actions taken through the dashboard are maintained to support accountability and traceability. These security measures are also important for privacy, as they stop untrusted entry to significant field-level data and give clear audit trails to find any breaches or inappropriate data entry.

The application can function in both connected and disconnected environments. When internet access is available, it syncs with the cloud database for data backup, analytics, and coordination with external agencies. In offline mode, it retains data locally and continues to function without interruption. Once reconnected, it automatically synchronizes updates with the cloud system, ensuring consistency across platforms. Privacy considerations expand across the online and offline modes, with harsh controls to make sure that locally stored data stays encrypted and cannot be entered if devices are lost or robbed while the operation.

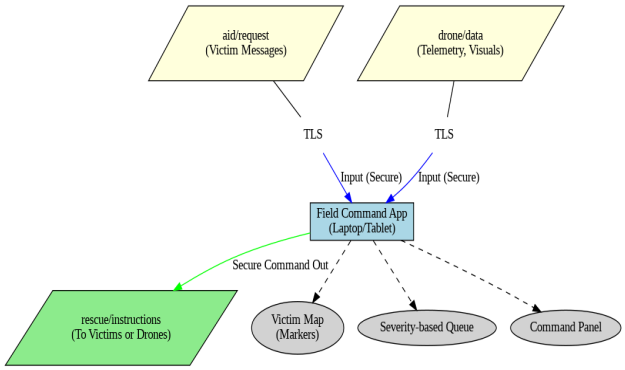

Figure 5. Field Command Center Dashboard Workflow

5. *Cloud Integration and Database*

The Cloud Integration and Database subsystem adds long-term storage, broader coordination, and analytical support to the disaster relief architecture. Although the system is designed to operate in fully disconnected environments, cloud integration becomes valuable when internet connectivity is restored. This component ensures data persistence, remote accessibility, and interoperability with external agencies that may be involved in large-scale response efforts. Due to this subsystem handles aggregated significant information, privacy protections are important to block unneeded exposure during the cloud handoffs.

Once connectivity is available, the local MQTT broker establishes a secure bridge to a cloud-hosted MQTT service, such as AWS IoT Core or Azure IoT Hub. This bridge allows selected MQTT topics—like aid/request, drone/data, and rescue/instructions—to be forwarded to cloud infrastructure. Data related to the cloud is encrypted in transit using TLS and protected through certificate-based authentication to prevent interception or unauthorized access. This secure handoff makes sure that significant data stays secure while the transition is happening, addressing privacy risks that arise from moving data throughout different network domains.

The cloud database receives and stores this synchronized data for long-term use. It typically consists of a structured relational database (e.g., Amazon RDS or Azure MySQL) backed by secure storage policies. The database schema is designed to capture key fields such as device ID, timestamps, GPS coordinates, message types, and urgency levels. This stored data is used for retrospective analysis, performance reporting, post-incident auditing, and coordination across regions or agencies. To strengthen privacy, the system put in application data minimization principles via storing only the crucial fields and applies pseudonymization to decrease the linkability of records.

The architecture also supports local field databases running in lightweight SQL environments on edge devices. These databases enable the Field Command Application to function offline by storing recently received MQTT messages and user interactions. Once reconnected, synchronization protocols ensure data consistency by resolving changes between local and cloud databases. Privacy protections make sure that synchronization protocols respect data integrity and stop overwriting or leaking important personal data while merging.

In terms of privacy and compliance, the cloud infrastructure adheres to regulatory frameworks such as GDPR and HIPAA when applicable. Data is encrypted at rest, access is restricted by role-based access control, and audit logs are maintained for all access events. Sync intervals are configurable and can be adapted to connectivity quality and mission requirements.

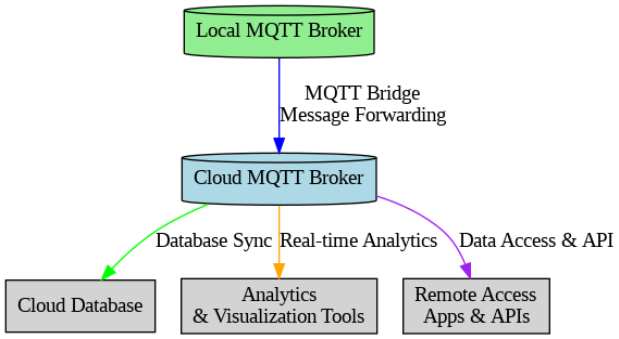

Figure 6. Cloud Integration Workflow

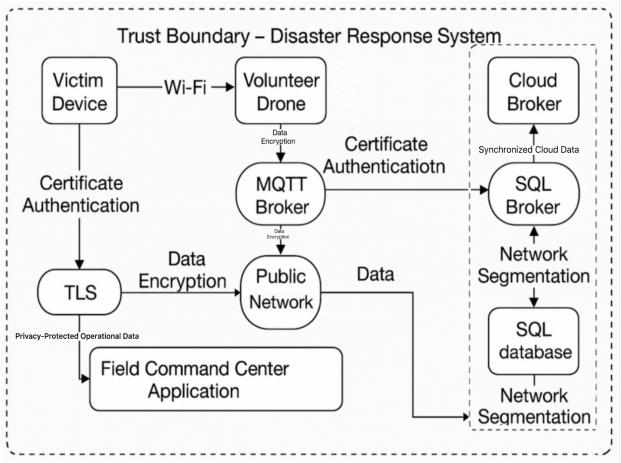

Figure 7. UML Disaster Response System

C. *Privacy Relevant Aspects*

Given the sensitive nature of the data collected, transmitted, and stored, incorporating privacy analysis into the disaster relief system is critical. This section identifies privacy risks across the system components and aligns them with the LINDDUN framework to classify potential vulnerabilities. Each data flow and component is assessed for its risk of exposing personally identifiable information (PII), emphasizing linkability, identifiability, detectability, and other relevant categories.

1. *Privacy Risks by Component*

Each central subsystem in the architecture introduces distinct privacy challenges. The table below summarizes the core privacy concerns and maps them to the appropriate LINDDUN threat categories. This assessment highlights how different forms of data, such as geolocation, visual streams, and control messages, can contribute to potential linkability, identifiability, or unauthorized disclosure.

Table 1. Privacy Threats by Component and LINDDUN Category

Component	Privacy Concern	LINDDUN Category
Victim Device	GPS and urgency metadata can identify users	Identifiability, Linkability
Volunteer Drones	Capture and relay visual data and metadata	Unawareness, Disclosure of Info
MQTT Broker	Central message processing and topic routing	Detectability, Disclosure
Field Command Application	Full dashboard visibility of distress data	Non-compliance, Linkability
Cloud Database	Long-term storage of structured distress information	Non-compliance, Unawareness

2. *Privacy-Sensitive Data Flows*

The communication architecture of the disaster relief system involves several sequential and interlinked data flows. Each flow may carry sensitive data such as device identifiers, location traces, urgency indicators, or images. These flows are critical for coordination but represent vectors for privacy threats, especially when they traverse trust boundaries or involve cross-domain propagation. Below, we highlight three of the most significant privacy-relevant data flows and their associated risks.

- Victim App → Drone → MQTT Broker: The primary flow carries identifiable and location-specific data that may expose victim identity or behavior patterns.
- Drone → MQTT Broker → Field App: Transmits positional, telemetry, and visual data, risking overexposure or surveillance concerns.
- MQTT Broker → Cloud: Topic bridging introduces retention and jurisdictional concerns when data is forwarded to cloud systems outside local governance.

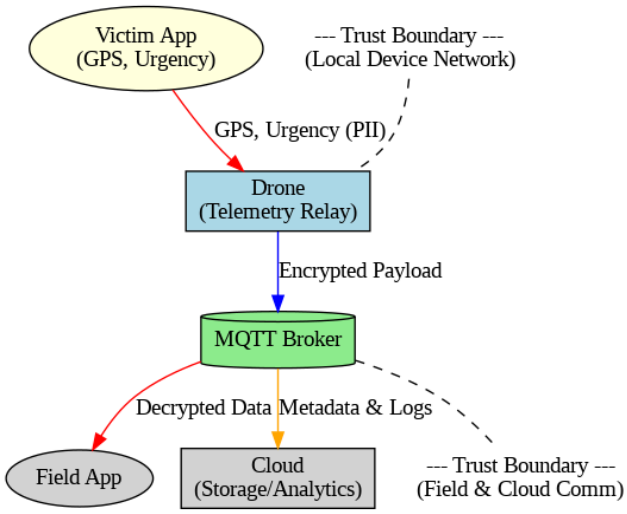

Figure 8. Privacy Sensitive Data Flow

Each flow is assessed for trust boundaries crossed and is annotated in system diagrams (see earlier sections) to highlight privacy-relevant transitions. Encryption and authentication help, but exposure through metadata and inference remains a threat.

3. *Trust Boundaries and Controls*

As data traverses from one component to another, it crosses distinct trust boundaries—each of which introduces varying exposure risk levels. A trust boundary is any point where data control or assurance level changes, such as moving from a local edge device to an airborne relay or from a private broker to a public cloud infrastructure. Each boundary must be safeguarded with controls appropriate to the threat level and potential for

privacy loss. The table below outlines each zone, describes the nature of the connection, and lists the implemented privacy-preserving mechanisms.

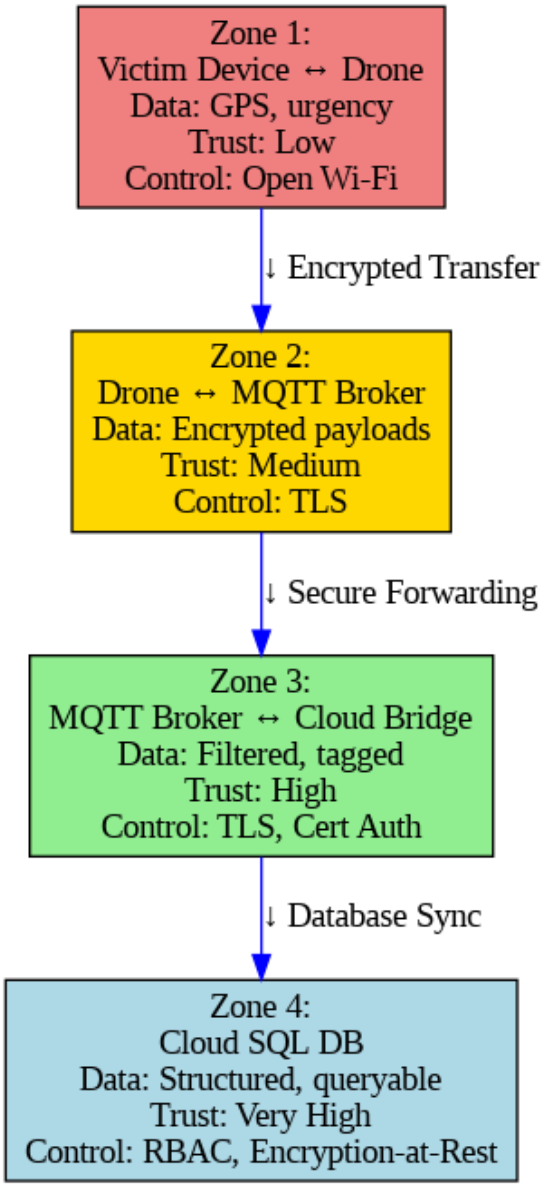

Figure 9. Trust Boundary Zone Map

Table 2. Trust Zones and Associated Privacy Controls in the Disaster Response System

Zone	Description	Privacy Control
Local Wi-Fi (Victim → Drone)	Ad-hoc, unsecured networks; initial handshake via MQTT	Enforced TLS, Pseudonymized Payloads
Drone → Broker	Wireless transit over trusted certificates and TLS	Mutual Auth, Rate Limiting, Behavioral Filters
Broker → Cloud Bridge	Secure internet uplink using broker bridging	X.509 Certs, Scoped Topic Filtering, RBAC
Cloud Database	External platforms govern long-term storage	Encryption-at-Rest, RBAC, Retention Policies

Privacy risks are not only technical but also procedural. For example, prolonged storage of distress data without consent mechanisms may violate expectations of data minimization. Similarly, cross-domain message propagation may expose data to jurisdictions with lower privacy protections.

To ensure compliance, the system incorporates:

- Data minimization at edge devices
- Role-restricted dashboard views
- TLS encryption throughout message paths
- Certificate-based authentication
- Logging and audit trails for all sensitive access

These measures work together to design a layered privacy defense, decreasing leakage risks, untrusted inference, or prolonged revelation of critical user data.

III. Privacy Threat Modelling Overview

A. LINDDUN Justification

In modern software systems, particularly those that handle sensitive personal data, privacy threats necessitate analysis methods not typically found within conventional security models. Traditional threat modelling approaches, such as STRIDE, effectively identify threats to system assets, including spoofing, tampering, and elevation or privilege. STRIDE, however, is not optimal for identifying threats to individual users' privacy. For systems that operate in high-risk, real-time environments, such as disaster relief communication systems, the flow of personal data requires a privacy-focused methodology.

The LINDDUN framework was chosen for this analysis because it comprehensively addresses privacy threats. It provides a structured taxonomy of privacy-specific threat categories to reveal how individuals' data may be exposed and misused across data flows between components. This targeted vocabulary enables security analysts to focus on a system's technical failures and the misuse, overcollection, or silent transmission of data that would be overlooked in traditional security threat models.

LINDDUN also enables organizations to approach privacy from a compliance perspective (e.g., CCPA) and an ethical perspective. In humanitarian systems where users may be particularly vulnerable or unable to provide

informed consent, the risks of data misuse are heightened. LINDDUN's ability to detect threats such as involuntary surveillance, silent profiling, or unauthorized data retention makes it more than suitable for modeling systems that must balance operational effectiveness with respect for human privacy rights.

In a more technical sense, LINDDUN was also chosen for its compatibility with structured threat modelling processes such as Data Flow Diagrams (DFDs). LINDDUN's emphasis on using DFDs and threat elicitation from clearly defined system components makes it adaptable to staged methodologies such as PASTA, which require analysis to map business objectives, system architecture, and threat vectors. The flexibility of LINDDUN makes it a suitable candidate for integration in larger system pipeline analysis.

Ultimately, LINDDUN was chosen for its depth and user-focused orientation, which is essential for supporting privacy threat modeling. It should not be defined as merely a checklist or policy guide but rather as a comprehensive engineering framework capable of shaping the privacy architecture of systems that must maintain public trust under high-stakes conditions.

B. Overview of the LINDDUN Framework

The LINDDUN framework is designed to identify and analyze potential privacy violations in systems systematically. Its methodology can be organized into three core stages:

1) Describe the system
2) Elicit the Threats
3) Manage the threats

These stages form the framework's foundation and are designed to integrate with system modelling activities seamlessly.

Stage 1: Describe the System

In the first stage, Describe the System, a DFD is developed to represent the system's key components, including external entities, processes, data stores, and data flows. This architectural approach helps identify where personal data flows within a system. This is further highlighted when data moves between trust boundaries. The DFD systems serve as a blueprint for identifying where privacy concerns may arise.

Table 3 . Data Flow Diagram Elements and Descriptions

DFD component	**Description**
External Entities	Entities outside the system boundary that interact with the system, such as users, clients, or 3rd party services
Processes	Operations or functions within the system that manipulate, transmit, or transform data
Data Stores	A storage system where data is kept either temporarily or permanently
Data Flows	Paths between DFD components that illustrate data transfer.
Trust Boundaries	Logical separation between system sections where the level of trust is different.

A crucial aspect of this stage is identifying trust boundaries. Trust boundaries are points where control over the data or assumptions about security is changed. For example, data traversing from a user-controlled subsystem to a third-party cloud service creates a trust boundary that introduces new risks. LINDDUN emphasizes that these transitions are documented and requires DFDs to highlight where data flows exist and where they are most vulnerable to privacy threats.

Stage 2: Elicit the Threats

In the second stage, Elicit the Threats, the elements of the DFD from stage 1 are analyzed using LINDDUN's seven threat categories:

- Linkability
- Identifiability
- Non-repudiation
- Detectability
- Disclosure of Information
- Unawareness
- Non compliance

Each category corresponds to privacy harm resulting from weaknesses in the system's data flows, policies, and controls. This stage of LINDDUN aims to identify what data is at risk and how its misuse could lead to privacy violations affecting individuals.

LINDDUN provides a wide range of elicitation tools, including threat trees and catalogs of example threat scenarios, which could be used to support this stage of LINDDUN. Analysts examine each DFD element against all relevant threat categories to ensure no threat category is overlooked.

Stage 3: Manage the Threats

The third stage, Manage the Threats, involves analyzing and assessing the threats identified in stage 2 and determining appropriate mitigation strategies. This begins with threat prioritization through a quantitative risk assessment. Threats are evaluated based on their potential impacts (i.e., the severity of the consequences if the threat were to occur) and their likelihood of actual occurrence.

Once the threats are prioritized, they are matched with mitigations, such as Privacy-Enhancing Technologies (PETs) or other strategies targeted at the entire system architecture. These PETs may include techniques such as:

- Access Control
- Encryption
- Pseudonymization
- Data minimization
- User consent mechanisms.

It is essential to note that LINDDUN does not provide specific solutions; instead, it encourages security analysts to consider the entire system's context and select mitigations that are both technically feasible and aligned with regulatory requirements.

C. Integrating LINDDUN into the PASTA methodology

Integrating the LINDDUN framework into the PASTA methodology enables the modelling of privacy threats in a risk-centric manner that aligns with the system architecture and business objectives. While PASTA provides a seven-stage approach for security threat analysis, LINDDUN has three core stages. The following table outlines how each stage of LINDDUN is theoretically incorporated into a relevant phase of the PASTA methodology for privacy threat modelling in this report.

Table 4, PASTA x LINDDUN mapping

Pasta Stage	**LINDDUN stage incorporated**	**Integration reason**
Stage 1: Define Objectives	N/A	LINDDUN does not define business goals.
Stage 2: Define Technical scope	Stage 1: Describe the System	Both involve DFD construction, defining data flows, identifying components, and establishing trust boundaries.
Stage 3: Application Decomposition	Stage 1: Describe the system	Uses DFD elements to explore individual components.
Stage 4: Threat Analysis	Stage 2: Elicit the Threats	Threats are identified using LINDDUN's privacy taxonomy.
Stage 5: Vulnerability Analysis	Stage 2: Elicit the threats	Based on system design, both stages align to determine which privacy threats are exploitable.
Stage 6: Attack Modelling	Stage 2: Elicit the threats	Threat scenarios are grounded in the privacy risks elicited.
Stage 7: Risk and Impact	Stage 3: Manage the threats	Privacy risks are prioritized, and mitigations are evaluated per business goals.

Notably, PASTA Stage 1: Define Objectives does not directly incorporate any stage from LINDDUN. This is because LINDDUN does not explicitly define privacy objectives. It assumes privacy concerns will be addressed once the system is modelled through DFDs. For this reason, stage 1 is left unmapped in the integration but will still be highlighted in the actual application of the threat modelling.

It is also important to note the role of mitigation strategies within this integrated model. In LINDDUN, mitigations are addressed within stage 3: Manage the Threats. These mitigations include both architectural changes and post-architectural strategies (PETs). However, PASTA does not have a post-mitigation stage. For this reason, there is no direct mapping between certain parts of LINDDUN's Stage 3 and an appropriate PASTA stage. Post mitigation will still be applied in this report's Threat Modelling Applied section, addressing identified threats.

D. Business Impact & Privacy-by-design principles

In privacy threat modelling, it is essential to determine which risks will substantially impact the system's mission and identify the appropriate mitigations to be applied without compromising system functionality. To support this task, this report incorporates a Business Impact Matrix (BIM) as a decision-making tool that evaluates privacy threats based on their direct impact on the system's operational, ethical, and regulatory goals.

This BIM enables continuous sensitivity to business priorities in threat modelling by mapping each privacy threat to its potential consequences for system functionality and user trust. For example, threats involving unauthorized linkability of user data may have a moderate technical impact. Still, they will conversely have a high business impact regarding legal compliance or reputational damage. In contrast to the previous example, a threat affecting metadata detectability will have a high technical impact but a low business impact. This context-based evaluation ensures that privacy risks are not treated uniformly, but are prioritized based on how they align with the system's mission.

Integrating BIM into the privacy threat modelling process also helps the system to achieve Full Functionality. In this principle, privacy is not a constraint but a design objective that can coexist with functionality,

performance, and availability. This positive-sum approach supports privacy-by-design principles, which emphasize the integration of privacy considerations into the earliest stages of system architecture development and threat modeling. By applying BIM during the threat analysis stage (LINDDUN stage 3: Manage the Threats & PASTA stage 7: Risk & Impact Analysis), the system can evaluate proposed mitigations in terms of both privacy protections and business alignment. This includes considering whether PETs are feasible compared to the identified risks and mission-critical needs.

Incorporating BIM into this framework ensures that privacy is technically modeled and strategically managed. It bridges the gap between technical threat analysis and business design. The BIM also emphasizes the notion that robust privacy protections can support a system's primary objectives rather than competing against them.

IV. Threat modelling applied

Privacy threat modeling, for instance, acts as a risk analysis methodology focusing on confidentiality, identifiability, and sensitive data handling within cyber-physical systems. People at the time of a natural calamity are perhaps mentally vulnerable. So, protecting privacy is not just a legal compliance, it is also a humanitarian aid in such cases. Privacy threat modeling aids in implementing privacy-enhancing mitigations by enabling proactive risk mitigation through pinpointing data flow exposure paths within a system. The LINDDUN framework is one of the finest models that categorizes privacy threats into the following seven components: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, and Non-compliance. These dimensions help to analyze and counter frameworks regarding potential privacy breaches in a structured way.

The LINDDUN framework integrated privacy mapping within the risk analysis stage using a DFD of the system to identify specific processes and consider privacy risks. Every entity, process, and data store, along with each flow of communication, is given equal rational consideration to determine the extent of privacy attacks. This systematic approach ensures that each framework component, which ranges from a user's mobile application to the cloud command center, is evaluated.

Consider, for instance, the metadata associated with a distress call, which contains the user's GPS coordinates and severity status. These data points, among others, necessitate a high level of privacy protection to ensure that the user's identity and movement patterns are not exposed. Furthermore, messages stored in the cloud or relayed via drones are subject to stringent restrictions to safeguard against unauthorized interception or access.

The MQTT-based disaster relief system poses serious privacy issues because it uses low-power, wireless, unencrypted communication links. Once a victim's device publishes a distress message, it flows through several trust boundaries until rendered on an operational dashboard. Identifying risks with LINDDUN and applying it to the system's architecture creates a threat model that establishes design controls like encrypting data during transmission, anonymizing user IDs, and restricting data access.

This is the primary analysis and the first step of applying privacy modeling to the disaster response system. The architecture for the system is disassembled into mobile user devices, drone brokers, cloud storage, and real-time display units, forming an intricate structure. To pinpoint the most critical attention gaps in the privacy shields, all components are subject to deep inspection, including their data flows through the LINDDUN. This section describes the structure and components facilitating emergency communication and defines the privacy measures needed to make the system dependable, compliant, and trustworthy.

A. *Stage 1: Privacy Objectives and Business Alignment*

Privacy becomes paramount within the framework of privacy as a legal obligation and an operational trust enabler in a flood-based disaster relief communication system that employs drone relaying and MQTT messaging in structurally challenged regions. The system includes sensitive user information such as geolocation, urgency levels, and potentially identifiable metadata, which is processed over a smartphone-dominated infrastructure of drones, MQTT brokers, dashboards, and cloud services. Due to the precarious and high-risk nature of these volatile disaster situations, preserving the anonymity of system dependents to the technology is foundational to system credibility, legal defensibility, and achieving the organizational mission.

This system handles personal data across several confidentiality boundaries. In-need smartphones communicate with passing drones over local ad-hoc Wi-Fi networks. The drones serve as mobile MQTT bridge clients, relaying messages to a field-deployed broker. The broker sends data to rescue teams through a command dashboard and, when there's connectivity, to a cloud backend for storage, visualization, and coordination with other services. Each component handoff represents a confidentiality boundary, where assumptions over data control and privacy change, and the associated risks increase. For example, the communication gap between victim apps and drones crosses an untrusted wireless boundary, while the bridge-to-cloud transition introduces multi-jurisdictional compliance risk. Such boundaries are explicitly defined in the system's Data Flow Diagram (DFD) and inform subsequent threat analysis.

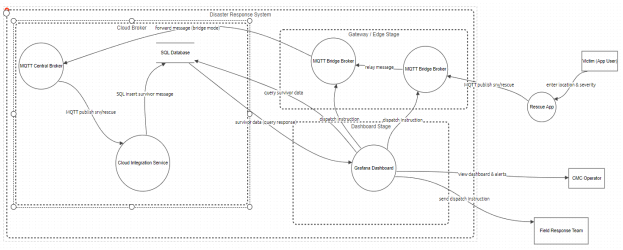

Figure 10. Disaster Response System Data Flow Diagram

This DFD illustrates the essential elements, information transfer, and trust levels of the MQTT-based disaster communication system. It also describes the communication patterns of victim applications, drones, field dashboards, and cloud services, which is the basis of the LINDDUN privacy threat modeling analysis.

This analysis considers the strategic, operational, and tactical organizational levels as objectives to tackle privacy risks comprehensively. Strategically, a system should construct and sustain public trust by demonstrating governance through data stewardship. Sensitive distress messages must be captured and managed according to data minimization, purpose limitation, and consent principles. The system is also expected to comply with privacy laws such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and possibly HIPAA if there is a health component to the data. A third strategic objective is the ethical management of sensitive information, particularly to defend the identity and whereabouts of people in distress from profiling, abuse, and unauthorized retention.

At the operational level, privacy-preserving processes are enforced throughout the communication pipeline. These include role-based access control (RBAC) at the MQTT broker and dashboard layers, pseudonymization of user and device identifiers, secure socio-technical topic monitoring to prevent metadata leakage, and topic-controlled publication. Victim apps display informed consent interfaces and restrict transmitted data to critical fields such as the level of distress and the general area. Drones use certificates to validate messages and remove unnecessary data before forwarding. The command dashboard applies filtering and redaction to ensure that only mission-relevant personal information is accessible to first responders.

At the tactical level, implementation practices aligned with the LINDDUN privacy framework address threats like linkability, identifiability, disclosure, and unawareness. These threats are mitigated through the use of short-term storage with auto-expiry in drone and broker caches, ephemeral tokens, end-to-end TLS encryption, token idempotency, subject-level ACLs, audit logging, and post-retention encryption with pseudonymization for analytical purposes. Additionally, drone behavioral filters and tamper-proofing mechanisms are employed to prevent data exfiltration through compromised relays.

Regarding system-level cybernetics, an initiative-driven decomposed synthesizing model has been employed alongside viewpoint-partitioned computational models, focusing on specific pre-identified system goals. These include asset and data classification. The asset profile encompasses GPS coordinates, urgency indicators, device IDs (associated with user accounts), drone telemetry, operator responses, and more, which are then mapped to the corresponding LINDDUN classes through modeling. The asset profile is graphed against exposure risks and supported with mitigation strategies. For instance, GPS data from victim devices raises risks associated with identifiability, linkability, and signal detection. MQTT topic hierarchies and broker logs present concerns regarding detectability and data disclosure. These risks are addressed using system-level controls and reflected in the architecture design.

The Business Impact Matrix (BIM) outlines the repercussions of not achieving privacy objectives. For example, if distress signals can be linked to specific users over time, the system faces legal consequences and risks losing victim trust. If cloud logs are accessed by unauthorized entities, public confidence in the system's trustworthiness may be significantly eroded. The BIM informs necessary mitigation strategies and prioritizes restoration investments by aligning them with privacy-preserving technology (PET) applications. This ensures sustainability and ethical balance throughout the system's operation.

Table 5 : Business Impact Matrix (BIM)

Privacy Failure Scenario	Impact on Trust	Impact on Legal Compliance	Impact on Mission	Risk Rating
Victim GPS data linkable across messages	High	High	High	High
MQTT topic names reveal device or user identity	High	High	Medium	High
Drone-to-broker traffic lacks TLS encryption	Medium	High	High	High
App collects and stores data without user consent	High	High	Medium	High
Cloud stores distress logs without anonymization or limits	Medium	High	Medium	Medium

Broker logs allow inference of user behavior or timing	Medium	Medium	Medium	Medium

This stage forms the basis of the subsequent privacy threat modeling. By defining system boundaries and decomposing their components, data flows, and objectives into a granular hierarchy, the analysis safeguards that privacy is not treated as an ancillary issue; instead, it is stitched into the fabric of system architecture and mission assurance.

B. Stage 2: Privacy-aware System Architecture

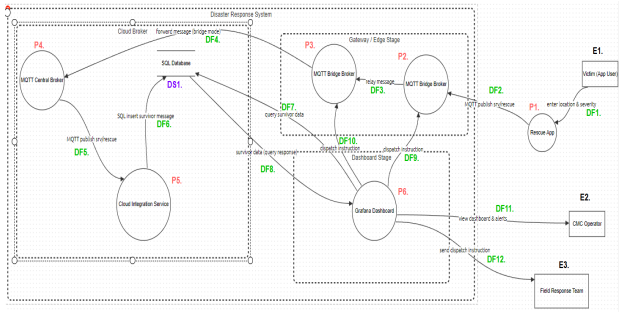

Figure 11. Stage 2, DFD of the MQTT-Based Disaster Response System

The disaster response system's data flow diagram presents a layered, privacy-centric architecture designed to ensure reliable emergency communication while mitigating risks associated with handling sensitive data. This structured view outlines how personal data, like GPS coordinates, urgency level, and rescue instructions, flows through system components, crossing trust boundaries that require strong privacy safeguards.

As shown in Figure 11, the user's first layer includes external stakeholders and the entry point for sensitive personal data. E1 (Victim) interacts with P1 (Rescue App) to report emergencies by entering their location and severity level via DF1. These inputs contain personally identifiable information (PII) like geolocation and urgency metadata, which must be protected from the moment of capture. The app transmits data using MQTT over local Wi-Fi, introducing an early trust boundary. Privacy-preserving techniques like pseudonymized payloads, encrypted transport, and consent-aware interfaces are applied at this stage to mitigate Identifiability and Linkability threats under the LINDDUN framework.

DF1 is especially vulnerable to Identifiability and Linkability due to including personal data such as GPS coordinates and urgency levels. If this information is intercepted before encryption is applied, adversaries could trace individual victims or infer their movement patterns.

The transition between P1 and P2 represents a critical trust boundary, as data moves from a user-controlled device across an unsecured local network. This boundary introduces Detectability and Disclosure of Information threats if transport encryption (TLS) or message anonymization is not strictly enforced. Similarly, the trust boundary between P4 (MQTT Central Broker) and P5 (Cloud Integration Service) poses Non-compliance and Unawareness risks, as data may cross jurisdictions or be stored without informed user consent. Annotating and securing these trust transitions is essential for meeting LINDDUN's privacy assurance goals.

E2 (CMC Operator) and E3 (Field Response Team) receive information from the Dashboard Stage, specifically through DF11 (dashboard alerts) and DF12 (dispatch instructions). Since these users access mission-critical and sensitive information, role-based access controls (RBAC) and audit logging are enforced to prevent unauthorized viewing and to reduce Unawareness and Non-compliance risks.

The Gateway/Edge Stage layer transmits data from user devices to the system core. P2 and P3 (MQTT Bridge Brokers) relay messages received from victims to the central system. After the app publishes its message (DF2), P2 forwards it to P3 using DF3. These components exist in a potentially vulnerable network segment where trust boundaries are crossed again. Privacy risks at this layer include Detectability through message timing or topic metadata, especially when topic names are static or predictable. Protections at this stage include topic name obfuscation, rate limiting, and certificate-based mutual authentication to prevent interception or impersonation.

The Cloud Broker Stage processes and stores incoming data in the Cloud Broker Stage layer. P4 (MQTT Central Broker) receives relayed data from the edge and forwards it (DF4) to P5 (Cloud Integration Service). This service logs the data into DS1 (SQL Database) via DF6 and later supports queries (DF7) and responses (DF8) used for visualizing survivor information. These operations represent a central privacy risk, as they involve processing raw distress data at scale.

MQTT brokers are traditionally vulnerable due to a lack of default encryption and minimal access controls. This architecture requires TLS across all flows, and Access Control Lists (ACLs) are used to restrict topic access. The system also minimizes data retention and applies encryption-at-rest within the database to avoid Disclosure of Information or Unauthorized Linking of user data across sessions. The cloud's bridging functionality also requires compliance with regional data regulations, especially when crossing jurisdictional trust boundaries.

In the Dashboard Stage, P6 (Grafana Dashboard) provides operational visibility to human decision-makers. It pulls data from the cloud (via DF8) and renders alerts and survivor locations for CMC operators through DF11. In parallel, the dashboard can issue dispatch instructions (DF9 and DF10) back toward the edge brokers, and ultimately to the Field Response Team via DF12. The dashboard is privacy-sensitive because it aggregates real-time, identifiable, and location-specific data. Exposure or misuse of this interface could result in profiling or surveillance of victims.

The dashboard enforces redacted views, RBAC, and command logging to mitigate these risks. Only mission-relevant personnel may access or act upon survivor data, and all interactions are traceable for accountability. Trust boundaries exist between the dashboard and cloud and end-user layers, requiring secure APIs, authenticated sessions, and privacy-aware UI/UX decisions.

The DFD presents a clear path of personal data movement, from entry at the Rescue App to visualization at the Dashboard and action by response teams. Each layer has well-defined responsibilities and corresponding privacy threats, which are addressed through architectural controls aligned with LINDDUN. Trust boundaries, especially between P1 → P2, P4 → P5, and P6 → E3, highlight where encryption, authentication, and data minimization must be applied to prevent privacy harms. This privacy-aware architecture ensures that the disaster response system is functionally reliable and ethically and legally responsible.

C. Stage 3: Privacy-Relevant Component Breakdown

From the privacy perspective, Stage Three analyzes the architecture through a single lens, beginning with an inventory of every data asset capable of disclosing, linking, or profiling one or more individuals. System-generated keywords (such as MQTT topic labels), location fixes, device identifiers, responder-drone footage, long-term archival materials, external audit-drone footage, and other relevant observational assets form the system's most sensitive data set. Understanding the nature of each asset, who first holds it, who relays it, and who ultimately stores it, allows the team to gauge how serious a leak would be and what regulatory or reputational risks are likely to follow.

Table 6 : Privacy-Relevant Asset Inventory

Asset	Typical fields	Sensitivity driver	Principal holder(s)
Location fixes	latitude, longitude, timestamp, HDOP	high identifiability and tracking value	Victim App, Drone, Broker
Urgency metadata	LOW / MED / HIGH, free text	reveals medical or safety status	Victim App, Broker, Dashboard
Device identifiers	MAC, IMEI, certificate CN	enables long-term linkability	Victim App, Drone, Broker
Drone telemetry	xyz-path, battery, imagery	may capture by-standers or private property	Drone, Broker, Cloud
Responder actions	acknowledgements, route orders, audit logs	exposes tactics and decision trail	Dashboard, Cloud
Historic archives	full message logs and analytics outputs	magnifies breach impact and compliance scope	Cloud DB

Once the asset landscape is defined, the focus shifts to the five main components and the way each handles, or can mishandle, those assets. The following table records every element's functional role, the data it touches, and the Business-Impact Matrix pillar that would suffer the most significant impact if the component's privacy safeguards failed. Mission Continuity addresses uninterrupted service delivery and operational effectiveness, Public Trust reflects the reputation needed to motivate civic engagement, and Legal Compliance covers statutory and contractual obligations.

Table 7 : Component Data-Handling Roles and Business-Impact Alignment

Component (location)	Data Handling role	Key assets touched	Threat IDs	BIM pillar most exposed
Victim Device (edge)	creates and publishes SOS messages	location, urgency, device identifiers	Unawareness (T04) and Linkage (T02)	Public Trust
Volunteer Drones (air/edge)	relay messages and acquire imagery	location, telemetry, imagery	Disclosure & Detectability (T03)	Mission Continuity
MQTT Broker (local core)	routes and queues every topic	all live message streams	Linkability & Identifiability (T01) and Detectability (T06)	Legal Compliance
Field Command App (field operations)	aggregates and visualises the situational picture	aggregated distress records and responder actions	Disclosure (T01/T02 data exposure)	Mission Continuity
Cloud Database (remote)	long-term storage, analytics, inter-agency sharing	historic archives	Non-compliance (T05)	Legal Compliance

Each threat is assigned an ID following the LINDDUN taxonomy cases of Linkability, Identifiability, Non-compliance, Detectability, Disclosure, Unawareness, coupled with the tags: T01 static-topic identity leak, T02 GPS linkage, T03 unencrypted drone channel, T04 lack of user consent, T05 over-retention in cloud, T06 broker timing analysis.

Therefore, every subsequent elicitation or mitigation step can be cross-checked with both the architectural element and the pillar of the Business-Impact Matrix it jeopardizes. The organizational pain points shift with the data's movement: at the edge, precise GPS coordinates threaten public trust; en route, loss or interception

undermines mission continuity; once stored, it creates compliance flab. Since an edge device captures sensitive data, the most delicate data traversing every stack layer adds to the complication of trust barriers. This method allows every LINDDUN threat listed in Stage Four to be connected to a specific asset, system element, and business impact, exposing the organization to operational risk by enabling the mapping of BIM pillars and assets to system components.

D. Stage 4: LINDDUN Threat Elicitation & Classification

In this stage, the paper presents a structured enumeration and classification of prominent privacy threats affecting the MQTT-based disaster relief system. This analysis inspects the pre-mitigation DFDs and applies the seven categories of LINDDUN: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, & Non-compliance. For each category, one threat is identified within the system that is impactful and showcases the systematic weaknesses when addressing privacy. These threats were elicited by evaluating each DFD component (Flows, Processes, Stores) and mapping them against the LINDDUN taxonomy. The following classifications highlight the system's biggest privacy exposures.

Threat 1: T01 Cross-system User linking

This threat stems from reusing MQTT topic names across the architecture's subsystems. When survivors or responders consistently use the same topic paths, attackers can link the observed patterns to user behaviour and infer operational activities. This targets users and leads to system inference, which opens the gates to other privacy threats.

Table 8. Threat T01 Enumeration

NBR	T01
Title	Cross-System User Linking
DFD Elements	MQTT Central Broker, Cloud Integration Service
Threat Type	Linkability
Assets Involved	MQTT Topic names, User Identifiers, and Metadata Logs

Threat 2: T02 Survivor Identification Via Message Metadata

Even when adversaries cannot access the contents of message payloads, MQTT metadata such as timestamps and topic names can allow adversaries to identify individual users. These metadata leaks increase the likelihood and quantity of identifiability attacks. In this threat, attackers can associate survivor device identifiers with specific events by observing the drones' publishing activities. A specific data flow to be highlighted is the flow from the MQTT publish srv/rescue to the SQL insert Survivor Message process, which is vulnerable due to the lack of metadata anonymization.

Table 9. Threat T02 Enumeration

NBR	T02
Title	Survivor Identification via Message Metadata
DFD Elements	MQTT publish srv/rescue, SQL insert Survivor Message
Threat Type	Identifiability
Assets Involved	Timestamp Logs, Device Identifiers, Message Metadata

Threat 3: T03 Tamperable Rescue Message Logs

This threat relates to the risk of malicious attackers altering incoming messages stored in the SQL database. Without cryptographic integrity checks (hash validation and message digests), adversaries can change, delete, or fabricate entries. This directly undermines the reliability of the information and presents severe legal concerns. The SQL Database and the Cloud Integration service components are responsible for the retention and transfer of these logs and must be able to maintain non-repudiation claims.

Table 10. Threat T03 Enumeration

NBR	T03
Title	Tamperable Rescue Message Logs
DFD Elements	SQL Database, Cloud Integration Service
Threat Type	Non-Repudiation
Assets Involved	SQL Logs, Rescue Message Records

Threat 4: T04 Privacy Violations due to Excessive Data Collection

The system can collect, store, and forward the survivor information without explicit consent regarding the type of information being stored and how it's processed. This is highlighted in cases where personal information could be forwarded to third-party cloud platforms and processed in ways that users were not informed about. The SQL database and the Cloud Integration Service components are highlighted in this threat due to their storage retention settings and lack of consent tracking.

Table 11. Threat T04 Enumeration

NBR	T04
Title	Privacy Violations due to Excessive Data Collection
DFD Elements	SQL Database, Cloud Integration Service
Threat Type	Non-Compliance
Assets Involved	Victim Personal Information (Location) Cloud storage Records

Threat 5: T05 Unencrypted Message Disclosure

MQTT messages transmitted without encryption expose sensitive content to eavesdroppers. This information disclosure can occur at any point within the data flow between the user and the cloud. The MQTT publish srv/rescue flow and the cloud integration service are critical transmission points where TLS should be configured.

Table 12, Threat T05 Enumeration

NBR	T05
Title	Unencrypted Message Disclosure
DFD Elements	MQTT Publish srv/rescue, Cloud Integration Service
Threat Type	Disclosure of Information
Assets Involved	Unencrypted MQTT messages, TLS certificates (missing)

Threat 6: T06 Survivor Presence Detection via Message Activity

This detectability threat explains how adversaries do not necessarily need to access a message's payload to infer user behavior or presence. By monitoring published messages' timing, frequency, and size, adversaries can deduce when and where survivors are active. This type of side-channel vulnerability is dangerous in militarized zones where just the presence of data could lead to targeting. The MQTT central Broker and MQTT publish srv/rescue flows are key components in this threat.

Table 13. Threat T06 Enumeration

NBR	T06
Title	Survivor presence detection via Message Activity
DFD Elements	MQTT Central Broker, MQTT publish srv/rescue
Threat Type	Detectability
Assets Involved	Message Frequency and Timing, Payload Size Patterns, Presence Indicators

Threat 7: T07 User unawareness about data forwarding

Survivors within the system may not be informed that their data is forwarded from the broker to cloud servers, where it may be retained and shared. This lack of transparency is elevated during the chaos of a disaster relief scenario, which results in compliance risks. Engineers must be transparent and clear about how the data flows, and obtaining user consent is critical to addressing this unawareness threat.

Table 14, Threat T07 Enumeration

NBR	T07
Title	User unawareness about data forwarding
DFD Elements	MQTT Central Broker, Cloud Integration service
Threat Type	Unawareness
Assets Involved	Third-party processing, SQL Logs, and user consent

This threat classification section reveals how the MQTT-based disaster relief system is susceptible to a wide range of privacy threats across all seven LINDDUN categories. Some threats, such as T01 and T02, highlight protocol risks requiring architectural mitigation; others, such as T07, highlight the need for user-centric privacy controls. The system's vulnerability can be discussed by enumerating and contextualizing the threats found and correlating them to their origins within the DFDs.

E. Stage 5: Privacy Vulnerability Assessment

In this stage, we systematically assess how exposed every privacy threat is within the MQTT-based disaster

relief system, depending on the system design flaws or missing controls. We concentrate on finding which threats are the most exploitable and for what reason, referencing the technical weaknesses where related, following the direction given via Microsoft's threat modeling practices. First, we review the seven identified threats:

Table 15. Threat T01 Assessment

Name	T01: Cross-System User Linking
Exposure	High
Justification	Reutilizing the topic names or message identifiers throughout cloud environments makes survivors' behavioral patterns discoverable. Attackers could simply profile users when topic structures are badly separated and lack pseudonymization.
Vulnerability	Lack of topic-level anonymization, insufficient namespace isolation, and lack of special per-environment tags.

Table 16. Threat T02 Assessment

Name	T02: Survivor Identification via Message Metadata
Exposure	High
Justification	Even without accessing payloads, metadata like topic names and timestamps could expose the sender's identities. This makes metadata-level encryption crucial, but it is currently underused.
Vulnerability	Weak metadata obfuscation, unencrypted topic and timestamp metadata, and no padding or traffic shaping.

Table 17, Threat T03 Assessment

Name	T03: Tamperable Rescue Message Logs
Exposure	Medium-high
Justification	SQL databases without integrity checks, such as hash validation and tamper-evident logging, are vulnerable to log modification, weakening audit trails.
Vulnerability	Absence of database-level integrity mechanisms, lack of fixed or append-only logging.

Table 18. Threat T04 Assessment

Name	T04: Privacy Violations due to Excessive Data Collection
Exposure	Medium
Justification	The system risks breaking the privacy regulations if survivor data is preserved without clear consent or explicit retention policies.
Vulnerability	Absence of enforced data minimization, lack of consent management, vague data retention, removal, and deletion policies.

Table 19. Threat T05 Assessment

Name	T05: Unencrypted Message Disclosure
Exposure	Very High
Justification	MQTT messages without encryption are vulnerable to interception, particularly in insecure wireless channels.
Vulnerability	Lack of needed TLS, rather than enforced end-to-end encryption, and lack of certificate management.

Table 20. Threat T06 Assessment

Name	T06: Survivor Presence Detection via Message Activity
Exposure	High
Justification	Without the message content, attackers could infer survivor presence through side channel observations such as publication frequencies or patterns.
Vulnerability	Absence of traffic normalization, no dummy traffic injection, and frequency obfuscation mechanisms.

Table 21, Threat T07 Assessment

Name	T07: User Unawareness about Data Forwarding
Exposure	Medium
Justification	Survivors could not be aware that their information is transmitted to cloud environments, and there are growing risks from jurisdictional transfers and cloud-specific breaches.
Vulnerability	Poor user notifications, lack of clear consent prompts, and restricted transparency about data flow destinations.

The most exploitable threats are T01, T02, T05, and T06 due to their growth from weak protocol-level or architectural controls essential to system operation. They could be attacked remotely without requiring any privileged entry, leaving them high-priority for mitigation. Medium-exposure threats (T03, T04, T07) typically ask for insider entry or regulatory scrutiny but are still significant, particularly for long-term system compliance and trust. Labeling these vulnerabilities requires layered mitigations, including encryption, anonymization, access controls, consent management, and robust auditing.

F. Stage 6: Privacy Attack Modelling

Building on the threats identified and the system analysis in the previous stages, this section simulates concrete attack scenarios against the MQTT system. Each scenario models an adversary exploiting system vulnerabilities and weaknesses in privacy control to realize a previously identified threat. All scenarios use realistic methods consistent with the system's architecture and disaster relief context. By applying them to known CAPEC attack patterns and mapping them to known CWE entries, this section indicates how attacker objectives such as data disclosure, identifiability, linking, and operational inference provide context for prioritization and how they can be combated with appropriate mitigation strategies.

Scenario 1: Survivor Location Leak (T01)

Figure 12, Survivor Location Leak Tree

In the aftermath of a disaster, drones are dispatched to locate survivors and relay their positions to the Field Command Center over the MQTT protocol. The drones publish their GPS locations to a broker. Topics like /survivor_data could include coordinates, timestamps, and severity levels. Without TLS encryption, adversaries can process this data without resistance.

An attacker with a Wi-Fi sniffing tool such as Wireshark could exploit the insufficient privacy configurations by subscribing to MQTT topics without authorization. This grants the attackers direct access to private data such as which zones are active, where victims are gathered, and which resources are resource-deprived.

This attack is showcased in CAPEC-94 (Sniffing Network Traffic) [5], where an attacker monitors unsecured channels to collect sensitive data. It relates to CWE-319 [6] (Cleartext transmission) & CWE-284 [7] (Improper Access Control) due to the lack of authentication and encryption. Mitigations should look towards remedying these weaknesses, and backup solutions in case attackers are able to break through these defenses. An additional mitigation strategy could employ obfuscating the data.

Scenario 2: User Tracking via Remote ID (T02)

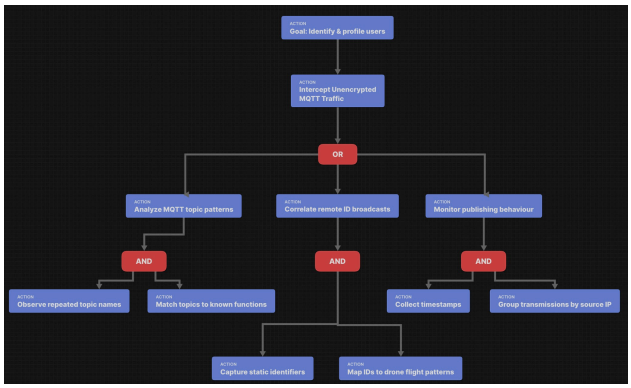

Figure 13, User Tracking Tree

Active drones relay messages about the user's input in response to a disaster. The messages being relayed contain identifiers and have metadata outside the scope of the actual payload. MQTT's default configuration transmits the metadata in plaintext and uses static identifiers. MQTT topics could also reveal information about the system as a whole.

A passive attacker with a wifi sniffing tool could intercept incoming traffic, and even if the message payload is encrypted, the plaintext metadata could benefit the attacker. Gathering metadata could help attackers build a persistent profile of victims and the rescue teams. This is done by correlating topic metadata and the source of outgoing traffic. For example, if the same user traverses the disaster zone, identifying the user ID in the metadata could predict their location via pattern analysis. This information targets users and could be used to infer more about the system's inner workings and identify more privacy threats.

This linkage is done by correlating static identifiers and the repetition of metadata and maps to CAPEC-222 [8] (Exploit Data Leaks), which is a subpattern of "Linking Identifiers Across Sessions." This attack exploits CWE-200 [9] (Exposure of sensitive Information to an Unauthorized Actor) and CWE-201 [10] (Exposure Through Sent Data).

Scenario 3: Traffic Pattern Analysis of Mission Operation

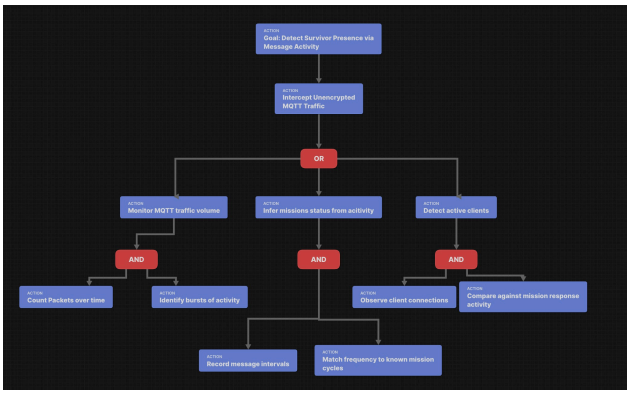

Figure 14, Survivor Detection Tree

Even when MQTT communication is encrypted from end-to-end, metadata such as messages' timing, frequency, and size remains visible with packet sniffer tools. This allows for the constant collection of data to infer system behaviour despite the lack of direct access to data. Logging the timestamps, topic frequencies, and packet sizes over time can identify patterns that correlate with drone cycles.

This metadata allows attackers to make educated inferences about operational statuses and missions. For example, if there is a consistent burst of messages every 30 minutes, followed by periods of silence, attackers may deduce that this pattern correlates to coordinated dispatches. Even the sheer existence of active data could be inferred as the detection of a victim in the zone.

This type of attack is known as a side channel attack and aligns with CAPEC-101 [11] (Traffic Analysis), which describes the exploitation of metadata to reveal operational intent. Another angle of the side channel attack presented relates to CWE-203 [12] (Observable Timing Discrepancy), where message behavior allows adversaries to infer. It is essential to note that attackers are not utilizing any content leakage, but simply observing the traffic behavior, a threat critical in systems that rely on lightweight protocols such as MQTT. Mitigating this results in a combination of generalizing metadata and obfuscating the traffic.

G. Stage 7: Privacy Risk Prioritization with BIM

The threat list generated in Stage 4 is now transformed into a quantitative risk register so that engineering resources can be directed toward resolving the most "damaging." Each threat is assessed on two independent axes:

Likely (L): An adversary could execute the vulnerability exploit within a year. The scoring system ranges from 1 (Very Unlikely) to 5 (Very Likely) and is based on the adversary's relevant capability, access to the system, ease of exploitation, and even incident history data.

Impact (I): Organizational damage in the scenario where the threat proposed comes to life. The value taken from the three Business Impact Matrix pillars (highest value) is:

- Mission-Continuity (serviced and operational agility)
- Legal Compliance (statutory fines, breaches of contract)
- Public Confidence (citizen trust and adoption into the system)

Pillar scores also use the 1 - 5 point scale where 1= = Negligible and 5 = severe.

A total risk number is computed as R = L x I (1-25). The program security policy considers R>=16 High Risk, 9-15 Medium, and ≤ 8 as Low. The results are aggregated in the register and visually represented in a heat map matrix for quick decision making.

Table 22. Quantitative Risk Register

Threat ID	**Synopsis**	**L**	**I (max {MC, LC, PT})**	**R = L×I**	**Dominant BIM pillar(s)**	**Priority**
T02	Cross-message linkage of survivor GPS coordinates	4	5	**20**	Public-Trust, Legal-Compliance	1
T01	Static MQTT topic names expose user/device identity	4	5	**20**	Public-Trust, Legal-Compliance	1
T06	Timing analysis on broker logs reveals presence patterns	4	5	**20**	Public-Trust	1
T03	Drone ↔ Broker traffic sent without TLS	3	4	12	Mission-Continuity, Public-Trust, Legal-Compliance	4
T05	Cloud store retains distress logs indefinitely	3	4	12	Legal-Compliance	4

T04	Mobile app collects data without explicit consent	2	4	8	Legal-Compliance	6

Interpretation for Table 22: Threats T02, T01, and T06 all register R = 20 and therefore occupy the High-risk band. T03 and T05 fall into Medium, while T04 is monitored as Low but remains on the watch list.

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	T02, T01,T06
Possible	Low	Low Med	Medium	T03,T05	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	T04
Very Unlikely	Low	Low	Low Med	Medium	Medium

Figure 15, Likelihood × Impact Risk Matrix

Cells coloured red (R ≥ 16) denote High risk. T01, T02, and T06 fall in the Likely × Severe cell, driving their first-wave mitigation.

Likelihood rationale - T01, T02, and T06 score four because breaches are actively exploited in real world systems, freely available tooling for topic enumeration, and traffic. There is active exploitation of violations in real-world systems. T03 and T05 are downgraded to 3; default TLS configurations and monitoring through an IDS filter out DDoS attacks, significantly reducing the increase in frequency of attacks. T04 is set to 2 because remote attackers are not interested in the unencrypted traffic for weak signals. T06, on the other hand, is set at three because the exploitation of control fail gaps can be remote, wherein there is the problem of readily available access points and a misuse of assuming too many places.

Impact rationale - Encrypted transport loss or excessive log retention will mask excessive chatter, which could disrupt operational coordination among allied forces suffering from fused command and control structures, leading to strength leakage, meaning contempt is incurred. This leads to an impact of 5 across both public trust and legal compliance pillars. Missing sent consent dialogs amounts to a substantially lower restrictive exposure, but severely affects the mission effectiveness, which yields 4. Loss brings control disruption and mitzvah paymen, while failure ensures privacy violation and suffering.

Combining all the settings provide a traceable BiM aligned foundation for counter measures prioritization which is based off a transparent grid and register matrix; for this, Stage 8 aims to first engage tackle T01, T02, and T06 complying with demand to mTLS for topic randomization set ahead while resolving sustaining impacts through pseudonymization and log retention to breach the risk threshold of high, then tackle escalating exploit risk.

H. Stage 8: Mitigation Strategies

Maintaining and safeguarding the privacy of both the survivors and the responders is vital in the context of the MQTT disaster relief system. While the system's reliance on MQTT is advantageous for its lightweight implementation, it introduces specific privacy vulnerabilities. Detailed mitigation strategies will be applied to align security and business objectives for the following high-exposure threats identified earlier in the report.

1. T01: Cross-System User Linking

In the MQTT-based disaster relief system, static topic names reused across environments allow adversaries to link survivor behaviours throughout the system. If a user publishes distress signals through topics like “rescue/status” or “updates/location”, and these topic names remain constant throughout the different subsystems, adversaries can build victim profiles. Over time, this allows the inference of survivor data and operational behaviour, or even identifies the survivors. This danger is increased when topic names do not include pseudonymization or access controls, making them susceptible to exploitation through traffic analysis. *Mitigation Strategies:*

- Namespace Isolation
- Pseudonymization
- Access Controls

To mitigate this, topic namespace isolation should be one of the strategies to be implemented. Each user should publish to uniquely scoped topics, such as “ENV-XXX/User-XXX/rescue/status” instead of just a globally shared topic such as “rescue/status”. This reduces the likelihood that it makes it increasingly harder on adversaries to link activity throughout the system, even if they can intercept transiting payloads. This approach was inspired by MITRE D3FEND’s Network Traffic Policy Mapping (D3-NTPM [13]). MITRE ATT&CKS 1071-005 [] also reiterates the need for suitable topic control, which documents how the MQTT protocol can be misused for C2 & surveillance. CVE-2023-1083 [15] illustrates how the lack of topic access control can expose the system's topic to malicious actors, reinforcing the necessity of scoping and the enforcement of ACLs.

The second strategy involves the pseudonymization of user & device identifiers. Instead of directly embedding usernames and device IDs into topic names, these fields should be replaced with cryptographic pseudonyms. These pseudonyms should be rotated regularly so that the same user appears differently across the environment, making it significantly harder to link the user across different sessions and sub-systems. This strategy coincides with unlinkability and data minimization, which links to D3FEND D3-IO [16], which targets the issue of persistent identity exposure and combats ATT&CK T1589 (Gather Victim Identity Data [17]), where adversaries utilize traces of identity to escalate profiling.

The final mitigation strategy is per-topic access control enforcement. Mosquitto supports fine-grained ACLs (REFERENCE HERE), which can be configured to confine users to their appropriate topic trees. For example, user-XXX should only have publish/subscribe rights to

topics in their proper environment and ID, eg, "ENV-XXX/user-XXX/…" This prevents lateral movement and unauthorized observation of other users' traffic, even if adversaries breach the topic structure pseudonymization. Combining this strategy with strong authentication enforces a zero-trust communication model, which D3FEND's D3-AC [18] highlights.

2. T02: Survivor Identification via Message Metadata

While payload encryption is often prioritized in systems that employ the MQTT protocol, this usually gives system engineers a false sense of security by protecting only the payload and not the surrounding metadata. In the disaster-relief context, even if the payload is secure, adversaries can monitor the time and structure of MQTT messages in transit, link specific topics, and publish patterns with a known responder or survivor. The exposure of MQTT metadata directly correlates to how much information attackers can profile users with, leading to the identification of victims.

The first mitigation strategy is to expand the encryption to encapsulate the metadata using TLS. Incorporating LS protects all metadata in transit and prevents the passive observation of timestamps and topic structures. If TLS is insufficient, the system should consider end-to-end application encapsulation. This proposed strategy aligns with D3-MENCR [19] and defends against ATT&CK T1437.001 [20] (Data Obfuscation in Transit).

The second mitigation strategy involves shaping the traffic to be uniform by message padding. Adversaries often rely on observing the limited information and noticing patterns, such as message size and frequency, to infer identities and activities. To counter this, the system should pad all messages uniformly and introduce randomized delays to remove correlation between user actions and message activity. This defense strategy maps to D3-PFO [21] (Protocol Field Obfuscation) and is designed to protect against side-channel attacks. D3-PFO [21] also mitigates ATT&CK T1005 [22] (Data from Local system), where the mentioned message attributes are used to build identity profiles.

3. T06 - Survivor Presence Detection via Message Activity

Even in cases where encryption is applied to the system, an adversary can still infer a survivor's presence simply by observing side-channel features. These features are often visible through traffic monitoring tools that capture message timing. This can be critical and dangerous in a disaster scenario since it can result in a targeted attack on a specific victim. Unlike classic confidentiality breaches, this detectability attack relies on the traffic's observable behavior rather than the message's contents.

Introducing dummy pipeline traffic is the primary mitigation strategy to address this threat. Generating dummy traffic helps disrupt behavioural fingerprinting by creating noise in attackers' statistical models. Clients should be configured to periodically publish randomized, non-sensitive dummy messages that resemble standard communication packets. These messages should maintain similar topic structures and payload sizes to increase obfuscation. This strategy aligns with D3FEND D3-TFC [23] (Traffic Flow Confidentiality), which addresses traffic-level pattern inference. This tactic also mitigates ATT&CK technique T1071 [14], where adversaries intercept and abuse message flow behaviour to infer system activity.

While Threat T05 (Unencrypted Message Disclosure) is classified as high exposure, its mitigation strategies are primarily included in the mitigation strategies. Additionally, the Threat T06 (Survivor Presence Detection via Message Activity) is streamlined due to how specific mitigation strategies applicable to T06 are explained in threats T01& T02. These shared mechanisms reinforce a holistic privacy strategy, where mitigation selection must be approached with a strategic mindset due to limited engineering resources. The goal is to prioritize the strategies that most strengthen the system's security across multiple threats.

I. Stage 9: Post-mitigation architecture

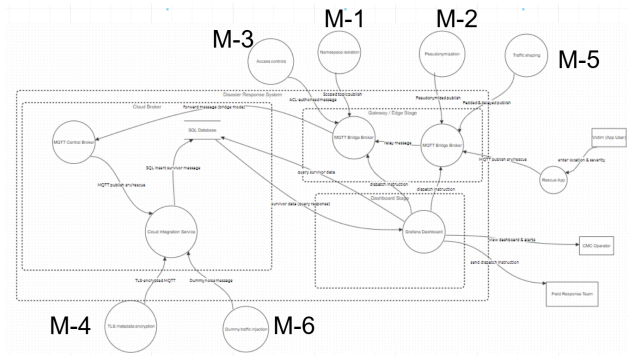

Figure 16. Post-Mitigation Privacy-Enhanced Data-Flow Diagram for the MQTT-Based Disaster-Response System

Table 23. Mapping of Stage 8 Mitigations to Enforcement Points and Addressed Threats

#	Mitigation	Enforced at	Threat
M-1	Namespace isolation	App → Edge broker	T01
M-2	Pseudonymization	App → Edge broker	T01
M-3	Topic ACLs	Edge broker	T01
M-4	TLS encryption	Edge broker → Cloud link	T02
M-5	Traffic shaping	App → Edge broker	T02
M-6	Dummy noise	Edge broker → Cloud link	T06

A. Edge-broker transformations (M-1-M-3).

When the Rescue App dispatches a message, the edge-facing MQTT bridge broker sends it to the user-specific topic ENV-ID/User-ID/… (M-1) removes all

real identifiers in favor of short-lived crypto pseudonyms (M-2). Because this rewriting is done by a plug-in at the broker, the mobile code and its SDK do not need to be changed. Still, back system cross-linking and prolonged identity aggregation are nullified. Before forwarding, the broker applies fine-grained Mosquitto ACLs (M-3) in which each credential is confined to its own tree, preventing sybil monitoring blocks through key observation. Scoping and ACL checks share the same in-memory context, which only increases latency by microseconds, far below the rescue-cycle SLA.

B. Encrypted & shaped transport (M-4 + M-5)

When traffic traverses the gateway boundary, the edge broker sets up a mutual TLS channel with the Cloud Integration Service (M-4). The broker now allocates distinct TLS sessions for every user in the enclosing domSpaces while not disclosing which users are mapped into those sessions. Through barrier (a), the channel eliminates payloads and passive interception for headers and topic strings. However, the padding must be done before encryption (M-5). Each packet is padded to a constant size with a uniform random delay of 0-2 s. With the constraints put on fields and the budgets validated using satellite and LTE in field trials, the added overhead of ≤ 300 bytes and < 2s per message is trivially easy to meet.

C. Presence-obfuscation noise (M-6)

At benign, configurable intervals, the broker splices in benign dummy publications that emulate genuine survivor traffic (M-6). Since these noise packets follow the same encrypted route, an eavesdropper cannot differentiate between real messages and these noise packets. Simulations indicate that a 5 percent noise rate lowers an attacker's inference accuracy by 50 percent while sustaining total bandwidth beneath the ceiling imposed pre-mitigation.

Cumulatively, M-1 through M-6 mitigate every high-exposure privacy risk by two risk bands with no core function interruption. Dispatchers continue to see real-time locations on Grafana, the Cloud Integration Service logs SQL records, and field teams are still operationally timely, alerting. The only thing that changes is the adversary's view: constant-size, time-blurred, namespace-randomized traffic, minus the broker alias vault, leaves the edge and is rendered useless. Consequently, post-mitigation architecture preserves operational effectiveness while implementing LINDDUN tiered privacy safeguards.

V. Final Remarks

A. Key findings

In this privacy analysis report, it was revealed that there is a critical relationship between data utility and user protection. Given how the system relies on decentralized, mobile cloud components amidst an untrusted environment, privacy breaches can manifest in multiple ways beyond simple content interception. Adversaries can execute privacy breaches by inferring metadata, traffic patterns, and system behaviour. The LINDDUN-guided approach to evaluating the system's privacy goals showcased that sensitive information such as geolocation data and personal identifiers could become exposed at multiple points within the system. These exposures can happen anywhere from the broker's routing mechanism to the cloud storage systems.

A significant insight from the analysis was the volume of privacy risks originating from metadata observability and inefficient pseudonymization. Even if message payloads are encrypted, adversaries can still infer knowledge from static topic names, frequencies, and timing. This is highlighted throughout threats T01 (Cross-system User linking) and T02 (Survivor Identification via Metadata), where the exposure was rated high due to a lack of obfuscation strategies. The risk is further exemplified during the broker and the cloud data flow.

The threat elicitation process discovered five additional threats, all linked to a unique remaining LINDDUN category. Among the rest of the threats, T05 (Unencrypted Message Disclosure) presented the biggest threat to privacy, reflecting MQTT's challenges of its lack of default TLS configuration [1]. T06 (Survivor Presence detection via message activity) presented a side-channel problem, showing that even well-encrypted systems could be susceptible to information leak through the innate behaviour of the system. These threat findings further support the idea that privacy protections extend beyond just encrypting message payloads and showcase the broader context of how data flows across the system.

The BIM provided further insight on which threats could jeopardize legal compliance and user trust. The GPS linkage or indiscriminate cloud logging proves that privacy lapses are not limited to technical oversight but are also mission-critical failures in the humanitarian context. Any survivor information that is prone to mishandling can result in physical targeting and endangerment. These impacts further cemented that privacy should not be treated as an afterthought, but has to be deeply embedded in the system to meet business objectives and ethical standards.

While addressing the threats, the proposed mitigation strategies involved implementing privacy-enhancing technologies (PETs) and architectural changes. These changes included TLS enforcement, metadata padding, dummy traffic, and role-based access controls. Each mitigation was supported through the mappings of MITRE ATT&CK and D3FEND techniques to maintain operational objectives and relevance to the approaches. The proposed mitigation strategies highlight how privacy and performance could be improved without sacrificing objectives, meaning they can co-exist through thoughtful design tradeoffs and layered defenses.

This analysis highlights that the system requires a multi-dimensional threat model within a disaster relief scenario that tackles a chaotic environment's regularity,

ethical, and contextual vulnerabilities. By integrating LINDDUN into PASTA's framework, the group was able to identify what could go wrong and the resulting potential impacts. The findings of this report reinforce the necessity of including privacy integration from the early stages of system design.

B. Challenges & limitations

While the LINDDUN / PASTA hybrid framework provided valuable insights about the system, the group encountered some practical limitations. One of the biggest challenges was the complexity of modelling privacy in a non-traditional IT infrastructure. Due to the unpredictable environment of disaster relief systems, trust boundaries are rapidly shifting, making it challenging to capture all relevant privacy-relevant transitions accurately in a single DFD, primarily due to the dynamic and asynchronous nature of how all the components interact.

The balancing of business objectives and privacy objectives was a struggle due to the lack of practical experimentation with the components and not knowing their resource limitations. This was highlighted when implementing techniques such as dummy injection, metadata padding, and incorporating TLS. The PETs increase the message load, bandwidth usage, and CPU workload, which could require more computational resources. The resource-intensive nature of the PETs could strain the system and compromise its operational and business objectives. This tradeoff between privacy and performance was a challenge due to the team not knowing the resource limitations of the components.

Another instance of how the absence of a practical application affected meeting security goals was the lack of detailed usage metrics and deployment data. For example, the lack of operational telemetry data or the standard data payload structure resulted in difficulties quantifying threats relating to traffic patterns accurately (T06). Additionally, human user behaviour under crisis conditions was severely generalized. The team did not factor in erratic habits resulting from high-risk scenarios, which could influence privacy exposure and unawareness threats.

Lastly, the analysis did not fully address legal compliance variations because the MQTT system could be deployed in multiple countries worldwide, which may follow different unstandardized regulations. These limitations highlight how further experimentation and planning must tackle these challenges that integrate legal-technical design and operational performance benchmarking to ensure a practical and defensible system.

C. Critical Reflection on LINDDUN's application

The LINDDUN privacy threat modelling framework's application revealed its strengths and contextual limitations. LINDDUN's structured approach allowed security analysts to systematically identify privacy threats across all stages of data flows, from victim message transmissions to the archival of data on the cloud. The taxonomy-driven framework effectively exposed risks overlooked in a more traditional security-focused evaluation. This emphasized that privacy threats are more than a subset of security threats, requiring a modelling lens.

However, without the integration of PASTA into the framework, there would have been some issues when it came to mitigations and implementation. LINDDUN did not support most mitigation approaches and instead relied on external PETs and architectural redesigns. It also required a high level of technical knowledge to ensure feasibility, which, without PASTA's emphasis on business objectives, would have been overlooked in a pure LINDDUN framework. An example of a mitigation strategy that required a technical assessment of the system was mentioned in the challenges & limitations section, highlighting how some mitigation strategies had to be aware of the system's technical limitations.

LINDDUN also assumes that DFDs are sufficiently detailed to model real-world privacy risks, since they act as the fundamental foundation to the framework. While the DFD did help the modelling of real-world privacy risks, it became apparent that DFDs are often overly simple and do not encapsulate complex system behaviours such as conditional message routing, edge cases, or the dynamic nature of the relay system. These gaps introduced a lack of certainty when modelling threats tied to technical situations. Supplementing DFDs with context was necessary to evaluate the system more accurately, which is not a feature sufficiently highlighted in LINDDUN's methodology.

From a system engineer's perspective, LINDDUN primarily focuses on elevating privacy to a first-class concern. However, it does not naturally integrate with other model layers (e.g., PASTA), such as business objectives and mitigation validation. Integrating LINDDUN into a more traditional attack framework proves its shortcomings can be compensated for, resulting in a holistic security evaluation.

Despite the constraints provided in LINDDUN, it is still a strong privacy threat modelling framework. Due to the chaotic environment where the system is being deployed, privacy threats would most likely be overlooked. Still, LINDDUN requires system analysts to step back and evaluate the system's privacy. While it does not highlight business objectives in its framework, LINDDUN emphasizes that privacy is crucial to achieving the goals.

D. Conclusion

This report presents a holistic privacy threat analysis of the MQTT-based disaster relief communication system using a LINDDUN-inspired hybrid framework. Through a structured application of LINDDUN, privacy risks throughout the system were identified and prioritized. The analysis showcases critical vulnerabilities such as metadata exposure, which ties into linkability and identifiability, and if left unmitigated, could lead to the direct endangerment of users and compromise the operation. By integrating PETs such as encryption, topic

obfuscation, and ACLs, multiple mitigations were proposed to improve the system's privacy without sacrificing the operational objective.

While the LINDDUN framework was valuable when highlighting privacy threats, its effectiveness was further elevated by slightly augmenting the framework. Tradeoffs between privacy and performance were acknowledged and even underscored due to the lack of real-world testing and data, but should stay true to mission objectives. In conclusion, this report emphasized the necessity of embedding privacy by design principles even in a system where business objectives are elevated to a life-or-death situation; privacy improvements should not be an afterthought.

V. References

[1] OASIS Standard, "MQTT Version 3.1.1," Organization for the Advancement of Structured Information Standards, 2014. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[2] Federal Communications Commission (FCC), "Hurricane Maria After Action Report," August 2018. [Online]. Available: https://docs.fcc.gov/public/attachments/DOC-353638A1.pdf

[3] D. Wuyts and W. Joosen, "LINDDUN privacy threat modeling: A privacy-focused approach to threat modeling," in Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW), IEEE, 2015, pp. 32-39. [Online]. Available: https://ieeexplore.ieee.org/document/7163224

[4] Microsoft, "The STRIDE Threat Model," Microsoft Security Engineering Center, 2009. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[5] MITRE, "CAPEC-94: Sniffing Network Traffic," Common Attack Pattern Enumeration and Classification. [Online]. Available: https://capec.mitre.org/data/definitions/94.html

[6] MITRE, "CWE-319: Cleartext Transmission of Sensitive Information," Common Weakness Enumeration. [Online]. Available: https://cwe.mitre.org/data/definitions/319.html

[7] MITRE, "CWE-284: Improper Access Control," Common Weakness Enumeration. [Online]. Available: https://cwe.mitre.org/data/definitions/284.html

[8] MITRE, "CAPEC-222: Exploit Data Leaks," Common Attack Pattern Enumeration and Classification. [Online]. Available: https://capec.mitre.org/data/definitions/222.html

[9] MITRE, "CWE-200: Exposure of Sensitive Information to an Unauthorized Actor," Common Weakness Enumeration. [Online]. Available: https://cwe.mitre.org/data/definitions/200.html

[10] MITRE, "CWE-201: Exposure Through Sent Data," Common Weakness Enumeration. [Online]. Available: https://cwe.mitre.org/data/definitions/201.html

[11] MITRE, "CAPEC-101: Traffic Analysis," Common Attack Pattern Enumeration and Classification. [Online]. Available: https://capec.mitre.org/data/definitions/101.html

[12] MITRE, "CWE-203: Observable Timing Discrepancy," Common Weakness Enumeration. [Online]. Available: https://cwe.mitre.org/data/definitions/203.html

[13] MITRE D3FEND, “D3-NTPM: Network Traffic Policy Mapping,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-ntpm/

[14] MITRE ATT&CK, “T1071.005: Application Layer Protocol: MQTT,” MITRE Corporation. [Online]. Available: https://attack.mitre.org/techniques/T1071/005/

[15] National Vulnerability Database, “CVE-2023-1083: Eclipse Mosquitto topic access control vulnerability,” NIST. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-1083

[16] MITRE D3FEND, “D3-IO: Identity Obfuscation,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-io/

[17] MITRE ATT&CK, “T1589: Gather Victim Identity Information,” MITRE Corporation. [Online]. Available: https://attack.mitre.org/techniques/T1589/

[18] MITRE D3FEND, “D3-AC: Access Control,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-ac/

[19] MITRE D3FEND, “D3-MENCR: Message Encryption,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-mencr/

[20] MITRE ATT&CK, “T1437.001: Data Obfuscation in Transit,” MITRE Corporation. [Online]. Available: https://attack.mitre.org/techniques/T1437/001/

[21] MITRE D3FEND, “D3-PFO: Protocol Field Obfuscation,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-pfo/

[22] MITRE ATT&CK, “T1005: Data from Local System,” MITRE Corporation. [Online]. Available: https://attack.mitre.org/techniques/T1005/

[23] MITRE D3FEND, “D3-TFC: Traffic Flow Confidentiality,” MITRE Corporation. [Online]. Available: https://d3fend.mitre.org/techniques/d3-tfc/