SOEN 422
Embedded Systems

Section MM

Computer Science and Software Engineering (CSSE)
Fall 2025

Presented to:
Dr. Hakim Mellah

Authored by:
Massimo Caruso (40263285)

Due: Friday, November 14, 2025

1. Part 1

1.1 Problem

University labs and research facilities house high-value, sensitive assets that require protection beyond standard key-and-lock systems. These assets are vulnerable to unauthorized entry, physical tampering, and data integrity breaches. A robust "Smart Campus" solution is needed that provides sophisticated, real-time security monitoring while operating on resource-constrained embedded devices, necessitating a highly memory-efficient and resilient communication architecture.

1.2 Proposed Solution

The proposed system is a Secure LoRa-Based Asset Monitoring System that provides multi-layered physical and network security. The core of the system is an embedded device utilizing its built-in LoRa radio for a lightweight, proprietary network link, eliminating the need for heavy, resource-intensive TCP/IP stacks.

1.2.1 Sensing (Dual-Mode Security):

Room Trespassing: An Infrared (IR) sensor detects general unauthorized motion within the lab.

Asset Tampering (Forced Entry): A Servo Motor acts as a physical lock on a mock-up asset cabinet. A Potentiometer is mechanically linked to the door, serving as a high-precision position sensor. If the door is physically forced against the servo lock, the position change is immediately registered as a high-priority tamper event.

1.2.2 Lightweight & Secure Communication:

Network Stack: The system uses the LoRa radio for low-power, long-range communication to a central gateway, avoiding the memory overhead of a full TCP/IP/TLS stack.

Confidentiality: Application-Layer AES-128 Encryption is performed on the data payload before transmission, ensuring data secrecy across the wireless link.

Integrity & Authentication: A Hash-based Message Authentication Code (HMAC) is appended to every LoRa packet. The receiving gateway verifies the HMAC, ensuring the message originated from an authorized device and has not been tampered with.

1.2.3 Secure Disarming Protocol (Two-Factor Authentication)

The system utilizes a Bluetooth Module for local disarming by authorized personnel.

To enhance security, a Challenge-Response (2FA) protocol is implemented: The device issues a random Challenge Code (via Bluetooth), and the user must enter a corresponding Response Key (obtained via the Cloud Dashboard) to successfully disarm the system.

1.2.4 Resilience and Forensics

A MicroSD Card acts as a secure Black Box Log. All high-priority events (tamper, alarms, power cycles) are written to the card immediately, ensuring an unalterable forensic record even if the network is unavailable.

The software employs a Watchdog Timer (WDT) to automatically reset the device in case of software failure, maximizing system reliability and availability.

2. Part 2

2.1 Functional Architecture and Connectivity

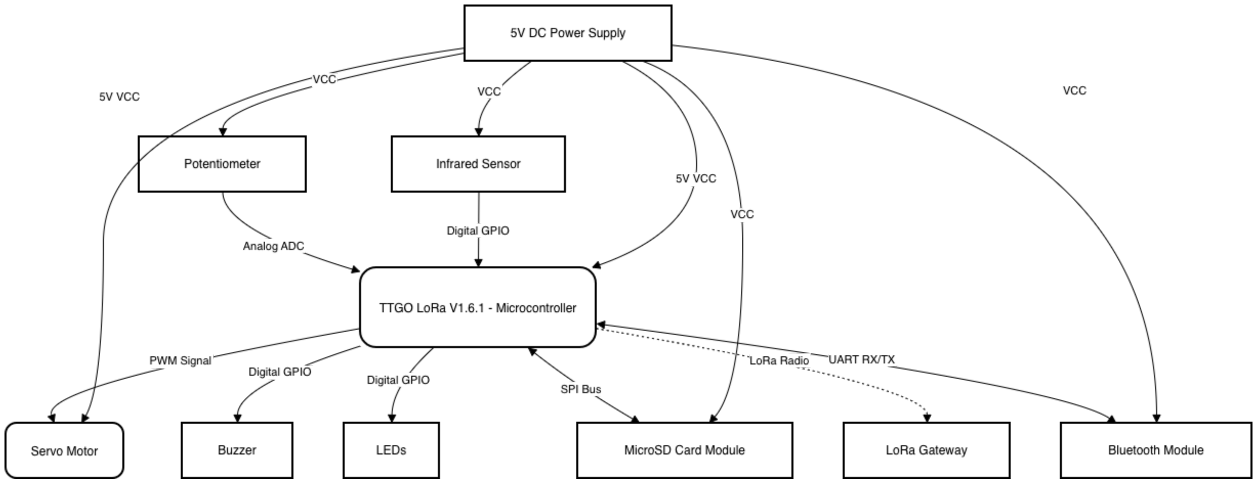

Figure 1: Functional Block Diagram

The system is architected around the **TTGO LoRa V1.6.1** microcontroller, which serves as the central processing unit. As shown in Figure 1: Functional Block Diagram, the system is divided into three logical blocks: Sensory Inputs, Security Actuation, and Secure Communication.

- **Input Processing:** Analog data from the potentiometer is read via the ADC to determine physical door state, while the IR sensor triggers immediate interrupts via Digital GPIO.
- **Secure Logging:** To ensure non-repudiation, forensic data is transmitted over the SPI Bus to the MicroSD card before any network transmission occurs.
- **Communication:** The system utilizes UART (Serial) for local Bluetooth 2FA interactions and the internal LoRa radio for long-range encrypted telemetry.

Component	Direction	Signal Type	Connection Details	Functional Role
Infrared Sensor	Input → MCU	Digital (GPIO)	Sends logic HIGH on motion detection.	Triggers "Room Trespassing" event.
Potentiometer	Input → MCU	Analog (ADC)	0V–3.3V voltage divider reading.	Measures exact door angle for tamper detection.
Bluetooth Module	Bidirectional	UART (Serial)	RX/TX Pins (9600 baud).	Receives 2FA challenge/response for disarming.
MicroSD Card	Bidirectional	SPI Bus	MISO, MOSI, SCK, CS.	Writes encrypted logs; reads config if needed.
Servo Motor	MCU → Output	PWM	Pulse Width Modulation.	Rotates to physical lock/unlock positions.
Buzzer/LEDs	MCU → Output	Digital (GPIO)	Logic HIGH to activate.	Visual/Audio alerts for alarms or status.
LoRa Radio	Bidirectional	Internal SPI	Wired internally on TTGO board.	Transmits AES-encrypted packets to Gateway.

2.2 Hardware (Preliminary List)

Component	Quantity	Purpose
TTGO LoRa V1.6.1	1	Core processing, LoRa radio, Bluetooth.
Infrared sensor	1	Room motion detection.
Potentiometer	1	Asset tamper detection (door position).
Servo motor (Hitec HS-422)	1	Physical locking mechanism.
Buzzer	1	Audible alarm.
Bluetooth Module	1	Local wireless override interface.
MicroSD Card Module	1	Secure event logging (Black Box).
Red LED / Green LED	1 each	Visual status indicators.
Passive Components	1 set	Resistor Pack, breadboard, dupond cables.
Power Supply	1	DC 5V supply for stable operation.

2.3 Security and Resilience Parameters

The project is designed with the TTGO's memory constraints as a primary security consideration:

1. **Confidentiality (Memory-Optimized):** Achieved through Application-Layer AES-128 Encryption of all LoRa payloads, eliminating the need for a heavy MQTTS/TLS stack.
2. **Integrity & Authentication (Memory-Optimized):** Provided by appending a HMAC to every LoRa packet. This lightweight approach verifies the message source and prevents data tampering.
3. **Authentication:** Implemented via the Bluetooth Challenge-Response (2FA) protocol for user authorization before disarming.
4. **Availability & Reliability:** Ensured by using the software Watchdog Timer (WDT) to automatically reset the system and prevent memory-related failures (like heap overflow) from causing a security lapse.
5. **Non-Repudiation:** Guaranteed by the unalterable, local MicroSD card logging of all security events for forensic analysis.