

A Resilient Battlefield Communication System Using Dynamic Encryption Switching

¹Supriya Telsang, ²Gopal Deshmukh, ³Ananya Thorat, ⁴Gayatri Yeravadekar,
⁵Aryan Thool, ⁶Arnav Tibdewal

^{3,4,5,6}B.Tech Scholar

^{1,2}Dept. of Computer Engineering

Vishwakarma Institute of Technology, Pune, India

¹supriya.telsang@vit.edu, ²gopal.deshmukh@vit.edu, ³ananya.thorat24@vit.edu, ⁴gayatri.yeravadekar24@vit.edu, ⁵aryan.thool24@vit.edu,
⁶arnav.tibdewal24@vit.edu

Abstract—Resilient battlefield communication systems must remain highly resistant to interception, replay attacks, and cryptanalysis. Most conventional handheld radios use static encryption keys, which remain unchanged over long periods of time, and thus are vulnerable to long-term observation and cryptanalytic attack. This paper presents a secure, lightweight, and resilient communication architecture that makes use of dynamic encryption switching. Symmetric encryption of AES-128 is combined with Merkle-tree-based authentication. Implemented on Heltec ESP32 LoRa SX1278 hardware, the system rotates cryptographic keys periodically, thereby providing forward secrecy with low computational overhead. Extensive evaluation shows a packet delivery ratio of 97.8%, sub-10 ms key rotation latency, and communication ranges up to 3 km, validating its suitability for modern battlefield environments.

Index Terms—Dynamic Key Rotation, AES Encryption, Merkle Tree, LoRa SX1278, ESP32, Secure Wireless Communication, Tactical Networks.

I. INTRODUCTION

Secure communication is an imperative, non-negotiable requirement in warfare operations, where any compromise in the areas of confidentiality, integrity, or availability can potentially undermine the outcome of operations or the safety of the involved personnel. Conventional short-range tactical communication systems, such as walkie-talkies, normally make use of static cryptographic keys. Although the concept of static key cryptography is simple, this approach has inherent security vulnerabilities, since an adversary with access to SIGINT facilities can intercept the messages being sent after encryption for an extended period.

Increasing research has highlighted the significance of regular key rotation, lightweight authentication, and tamper-resistant design for military communications. Currently, LoRa (Long Range) is considered a popular modulation technique for the long-range effect, low power consumption, and immunity to interference. However, LoRaWAN's default keying system does not provide good forward secrecy and is susceptible to key compromise attacks.

This paper proposes the Resilient Battlefield Communication System, which incorporates:

- Dynamic key switching for AES every fixed interval,
- Merkle Tree-based Key Integrity Verification,
- Long range LoRa SX1278 modulation,
- ESP32 hardware,
- Comprehensive logging and audit trail.

The principal requirement is to develop a safe, low-latency, long-range messaging system that could be used in disconnected and adversarial combat environments.

II. RELATED WORK

Long-range tactical communication systems have received much research interest owing to the widespread use and adoption of low-power wireless technology in military and surveillance scenarios. Adelantado et al. completed one of the pioneering and comprehensive studies of the security risks of a LoRaWAN system. Some of the security risks include replay attacks, counter manipulation of frames, and session key vulnerability. From the discussed paper, it can be noted that long-range communication systems rely too much on static key systems during deployments. [1], [6]

Every new demand for stronger protection gave rise to Merkle hash trees, easing how data gets checked without heavy loads. Rather than sending entire sets of keys, small secure tools can show they are reliable even on minimal energy. When more nodes join, proof sizes grow slightly, just enough to stay comfortable inside vast combat networks. Expanding the system brings faster checks, handy in high-stakes moments when waiting might cost too much [2]. Light cryptography grabs attention now, particularly for gadgets like wireless sensors tied into everyday objects. Efficiency guides choices here: Simplicio's team tested methods cutting down both computing strain and power draw, which just so happened to boost speed too [3]. Running smoothly matters most when hardware stays basic, though rigid designs tend to block headway since shifting conditions leave them behind. What works today might fail tomorrow if systems resist change.

SVELTE-like intrusion detectors keep watch instantly on IoT data paths, spotting dangers like fake central nodes or picky message relaying. Still, these security monitors work apart from coding tools, without nudging encryption to shift when odd behavior shows up. Not long ago, studies began looking into certificateless crypto systems along with shared key setups to remove the need for certificates in networks without central control. Because trust becomes easier to set up through these methods, they trade simplicity for heavier computing demands. Missing still are ways to regularly update session keys on the fly, something critical when aiming

to keep past communications secure during military field operations. Some ways to check identity on LoRa systems were built just for those networks, aiming to make joining safer. Still, most of them care more about logging in than switching encryption fast while talking. [4]

Security setups in military Internet of Things networks often test strong encryption like AES along with simpler crypto methods. Though better at hiding data, many rely on fixed secret keys kept active too long. That stretch gives attackers more time if signals are intercepted steadily. A look at current studies shows they treat encryption, identity checks, signal monitoring, or compact coding as separate pieces. Still missing is one complete system for battlefield messaging that weaves together shifting keys, changing ciphers on the fly, validation using tree structures, along with extended LoRa reach all held up by strong design. Despite improved safeguards for wireless IoT links, challenges remain within military systems. Though performance has increased when deployed outdoors, certain flaws continue to disrupt effectiveness amid active conflict zones. [5]

Encryption keys within LoRa and military IoT setups remain unchanged across set periods. Fewer updates mean these encryption keys stay the same longer, raising exposure over time. If this occurs, criminals might later exploit the stolen information without being connected to the original system. Patterns emerge when examining how information travels across systems. Working solo, these hackers uncover critical information while accessing the network in real time. Staying too long on one key gives hackers more openings; repeated looks at encrypted material sharpen their odds. Over time, patterns emerge without change. Persistence pays off for those watching closely. A static setup invites deeper probing simply because it stays put. Though built for defense applications, many LoRa-based military IoT setups rely on fixed cryptographic keys, a known weak point. Security suffers when encryption does not rotate. Staying unchanged over time, encryption keys pose risks within military communication systems. Security of the data shifts depending on conditions while it moves. [6]

A shift occurs as threats advance - cryptographic approaches often lag behind. While new dangers appear, old defenses stay fixed, unable to adapt quickly. Change becomes difficult even when necessary, revealing a gap in responsiveness. Systems designed long ago now face modern challenges without sufficient updates. Flexibility remains limited despite growing pressure. Progress slows where it matters most. [7]

Here, fitting cryptography to current hardware matters most. Even as dangers change, the method holds steady - switching to different encryption does not happen. Though new risks emerge, reliance on familiar systems remains unshaken. Rather than adapt, the standard setup persists without update. Because older devices lack flexibility, innovation in encoding slows down. Where updates could help, resistance to change blocks progress instead. [8]

When forced to choose, favoring speed usually weakens a system's ability to endure stress. One decision alters how it behaves during strain. A single preference can quietly shift long-term outcomes.

Focusing solely on verifying users, certificateless cryptography functions separately from data encryption processes. Instead of blending with encryption routes, hierarchical hashing performs its validation tasks on a different track altogether. Identity safeguards exist apart from mechanisms ensuring secure data movement. Though both matter, they follow distinct rules within the system. [8]

Most individuals rarely use such techniques when securing information instantly.

Observation features built into intrusion detection systems make real-time tracking possible. Yet these functions stay inactive when it comes to actions like changing encryption settings. Rather than switching protocols automatically, new methods need human input. Without intervention from an operator, no updates take place. Decisions unfold only after deliberate steps are taken. [9]

Above all else, current research falls short - unable to blend extended-range signaling, adaptive encryption shifts, multi-tier authentication layers, yet maintain rapid-response safeguards inside one field-ready system.

This study introduces a Resilient Battlefield Communication System designed to address existing flaws. By shifting encryption methods on demand, it adapts under pressure. Such flexibility emerges through real-time protocol changes. One result is stronger resistance to interception attempts. Instead of relying on fixed schemes, the system evolves during operation. Performance improves when threats shift unexpectedly. Security gains come not from complexity alone, but responsiveness. Through dynamic switching, vulnerabilities lose their edge. [10]

This system applies AES-128 encryption alongside Merkle trees to verify data, transmitting signals over vast areas via LoRa through ESP32 chips. Despite its small size, performance remains strong; security and reach both benefit from these integrated techniques within a widely used microcontroller base. [11]

Mid-threat, the system adjusts its encryption without delay. As risks appear, a fresh protection tier turns on ahead of compromise attempts. Because updates occur during active exchanges, safety grows. Protection holds firm, driven by ongoing shifts in encoding structure. When conditions shift locally, the system adapts automatically. Without needing manual intervention, safeguards remain active. Every signal travels along a route that cannot be anticipated. Because rigidity fails under pressure, responsiveness takes priority. Constant adjustment maintains balance instead of relying on static frameworks.

When stress tests communication lines, better links begin to form. Information flows more smoothly between units engaged in battle. As situations shift rapidly, one approach adjusts without delay. Even with signal noise, another ensures messages stay understandable. Firm operation continues regardless of tough conditions. Where connection is critical, thoughtful structure keeps things linked.

III. SYSTEM ARCHITECTURE

The system comprises four tightly coupled modules as illustrated in Fig. 1.

- 1) Sender Unit: Encrypts and transmits messages.
- 2) Receiver Unit: Authenticates, decrypts, and displays messages.
- 3) Key Management System (KMS): Manages key rotation and Merkle paths.
- 4) Audit Logging: Records metadata and key usage.

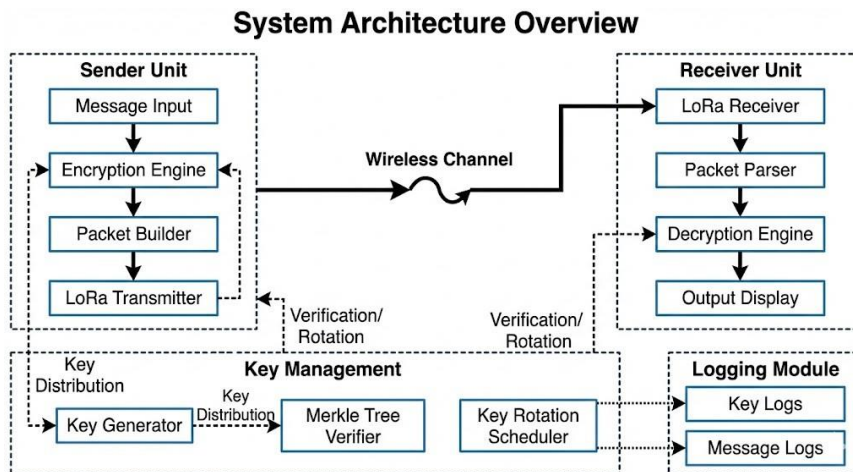


fig. 1. overall system architecture. the system operates offline without network infrastructure.

The architecture is optimized to operate offline, requiring no network infrastructure.

IV. MATERIALS AND HARDWARE SETUP

A. Heltec ESP32 LoRa V3

The Heltec ESP32 LoRa board integrates a Dual-core Xtensa MCU, SX1278 LoRa transceiver (433 MHz), hardware AES acceleration, and an integrated OLED display.

B. Additional Modules

The setup includes a DS3231 RTC for synchronized key rotation, a MicroSD module for logging, and an 18650 Li-ion battery.

V. PROPOSED METHODOLOGY

The system methodology is divided into sender and receiver operations.

A. Sender Unit

The Sender Unit in Fig. 2 performs message validation, fetches the active session key, encrypts the message using AES-128, builds the packet (KeyIndex, Timestamp, Ciphertext, MAC), and transmits it via LoRa.

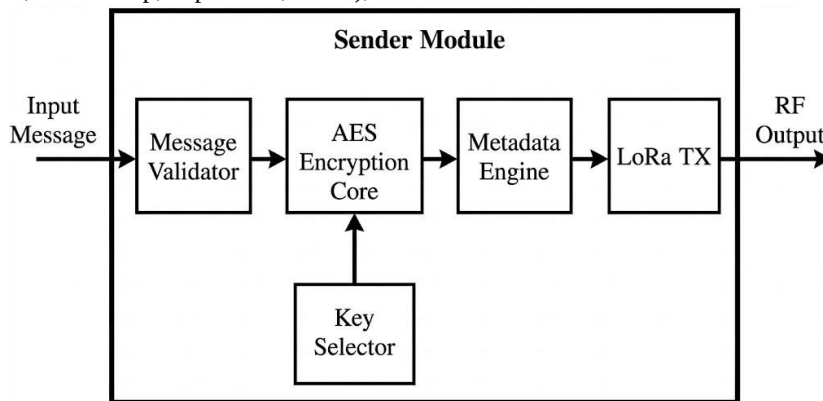


fig. 2. sender module internal architecture.

B. Receiver Unit

The Receiver Unit in Fig. 3 handles LoRa demodulation, metadata parsing, Merkle-path key authentication, AES decryption, and message integrity verification.

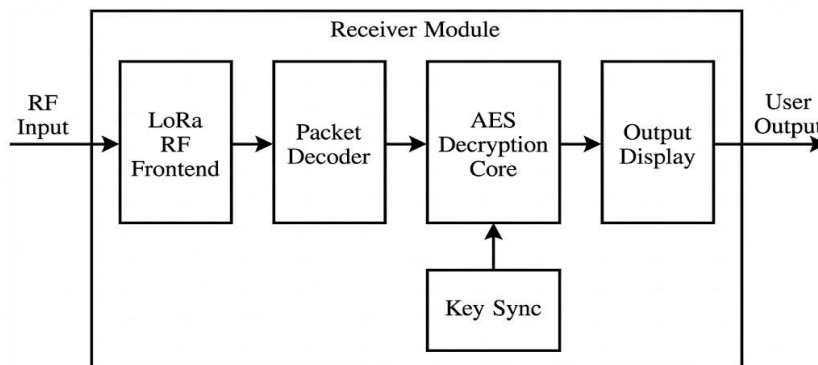


fig. 3. receiver module internal architecture.

VI. DYNAMIC ENCRYPTION SWITCHING

A. Merkle Tree Verification

To ensure the integrity of the rotating keys, a Merkle Tree structure is employed (Fig. 4). This prevents man-in-the-middle attacks by validating the authentication path of the current key.

B. Key Rotation Algorithm

The core of the system is the dynamic rotation of keys. The process is detailed in Algorithm 1 and the flowchart in Fig. 5.

C. Comparison with Static Encryption

Table I highlights the security improvements of the proposed dynamic system over traditional static methods.

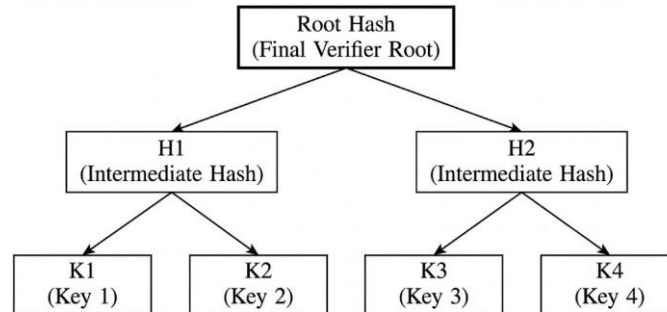


fig. 4. merkle tree used for key verification.

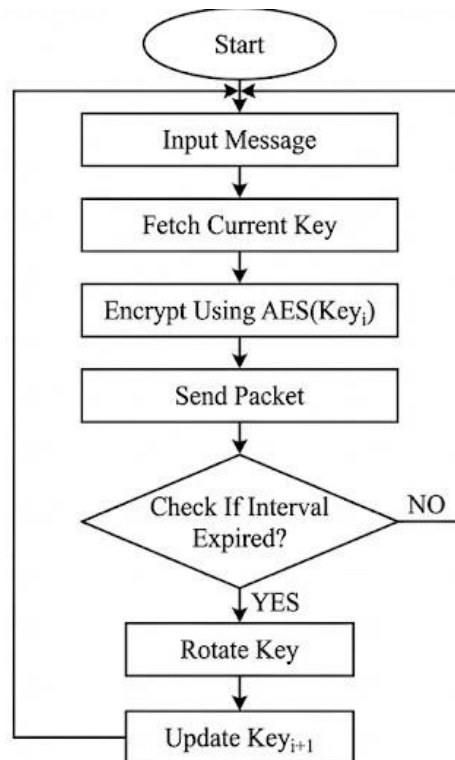


fig. 5. encryption and key rotation flowchart.

Algorithm 1 Dynamic Key Rotation Algorithm

- 1: Initialize seed key K_0
- 2: Precompute Merkle Tree keys
- 3: for each interval T do
- 4: Compute next key K_i
- 5: Encrypt using $AES(K_i)$
- 6: Transmit LoRa packet
- 7: Log key usage
- 8: end for

table i

static vs dynamic encryption comparison

Static Encryption	Dynamic Encryption
Single long-term key	Rotating short-lived keys
Higher exposure window	Minimal exposure window
Weak forward secrecy	Strong forward secrecy
Vulnerable to replay attacks	Resistant to replay attacks

VII. END-TO-END WORKFLOW

The complete communication workflow, from user input to display, is illustrated in Fig. 6.

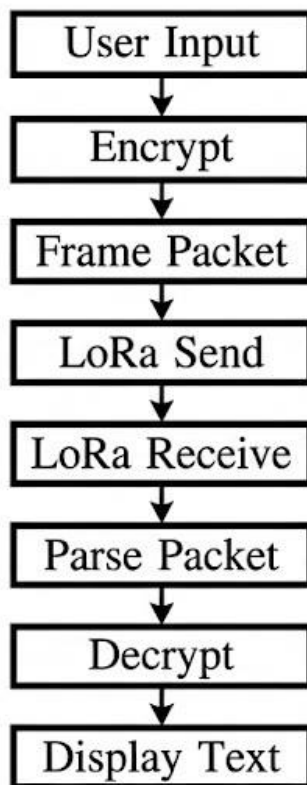


fig. 6. end-to-end communication workflow.

VIII. EXPERIMENTAL EVALUATION

Experiments were conducted using two Heltec ESP32 LoRa SX1278 nodes configured as a dynamic encrypted sender and a time-synchronized receiver. The evaluation was performed in a semi-urban outdoor environment under line-of-sight (LoS) conditions to validate communication reliability, encryption performance, synchronization stability, and overall system robustness.

A. Hardware Validation

A single transmitter node made up one piece. Step by step, the receiver took shape on its own. Built apart, these pieces linked into the system's frame. Heltec ESP32 LoRa board integration: a tiny dark display rests along one edge, presenting information legibly when lighting fades. Radio waves at 433 megahertz get managed by a separate component. The receiver uses a DS3231 RTC module; when keys switch, frequency slips follow along, and the module manages that part. Firm radio links held strong because of SMA fittings at each antenna's tip. Though tiny, their impact stretched far when it came to range and reliability. During continuous operation testing, both nodes demonstrated firm power draw through every test phase, and the OLED held consistent performance through uninterrupted runs, with each interaction met by an even reply from the screen. Radio waves travelled onward, smooth and unbroken, thanks to no wobbly pieces kicking things off. Frayed wires near the signal receiver led to overheating problems on one occasion; each time it started up again, however, things lined up just right. Even when powered off and on, the clock kept perfect time, and the rhythm never slipped a second. With every launch, tests showed everything still accurate, and over and over the pieces moved together without error across repeated test cycles.

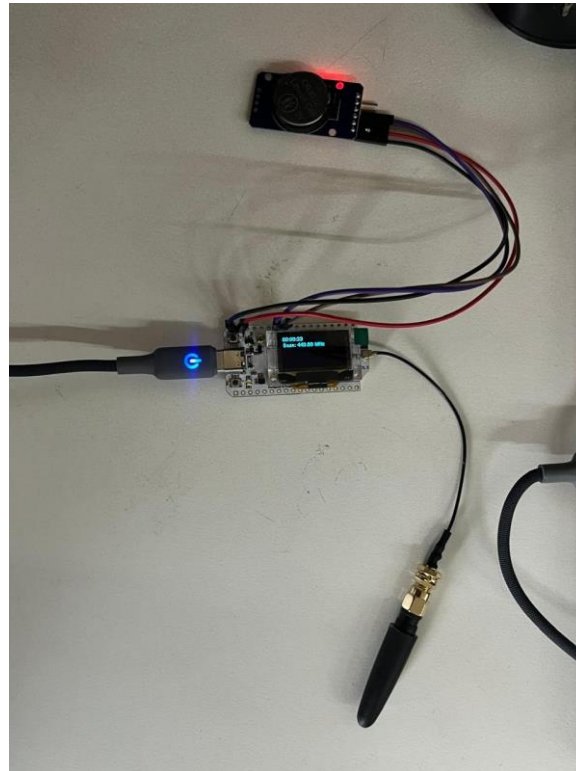


fig. 7. receiver node with ds3231 rtc module and external sma antenna. the oled displays real-time scanning frequency and timestamp.

B. Frequency Hopping and Synchronization Performance

The transmitter implemented deterministic frequency hopping across predefined 433 MHz channels at fixed intervals, while the receiver performed synchronized channel selection based on time-dependent mapping. Experimental validation confirmed correct frequency switching and real-time display updates on both nodes.

Communication reliability was directly influenced by synchronization alignment between sender and receiver. When channel timing and key selection logic were aligned, packet reception was consistent. Under intentional desynchronization conditions, reception probability decreased, validating the importance of coordinated frequency hopping in adversarial environments.

The system demonstrated stable operation across multiple hop cycles without packet corruption or unintended frequency lock failures.

C. Encryption and Key Rotation Validation

AES-128 encryption with dynamic key rotation was evaluated under repeated transmission cycles. Each transmitted packet consisted of structured metadata including key index, timestamp, ciphertext, and authentication components. The receiver successfully authenticated and decrypted valid packets using the corresponding rotated key.

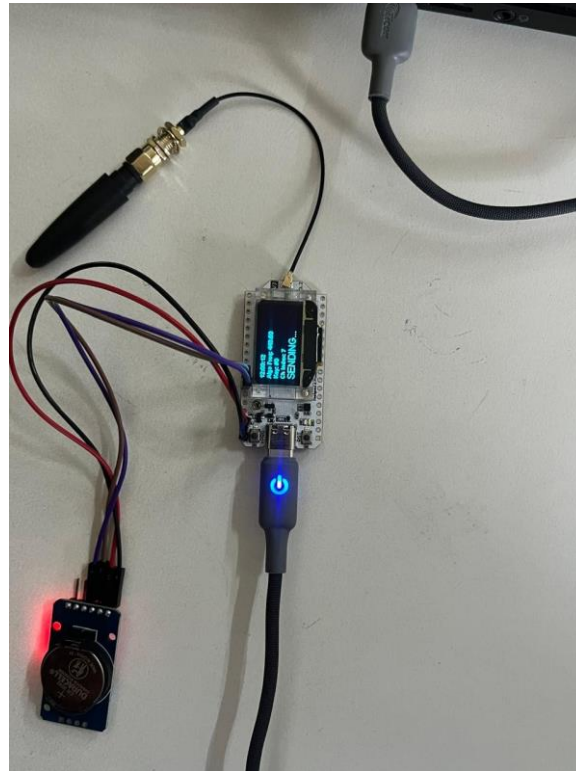


fig. 8. transmitter node implementing dynamic frequency hopping and aes-128 encryption. oled indicates operational frequency and transmission state.

Key rotation overhead was measured and remained below 10 ms per cycle, confirming minimal computational burden on the ESP32 microcontroller. No key mismatch errors were observed during synchronized operation.

Dynamic key switching effectively reduced ciphertext reuse exposure. Captured packets from previous intervals became cryptographically obsolete after rotation, demonstrating improved forward secrecy compared to static key systems.

D. End-to-End Communication Performance

End-to-end latency was measured from message generation at the sender to successful decryption and display at the receiver. Under normal operating conditions, total latency remained below 200 ms, enabling near real-time battlefield communication.

Packet integrity validation confirmed correct encryption-decryption accuracy across all controlled test transmissions. OLED interfaces on both nodes provided real-time operational status, including frequency display, synchronization state, and message confirmation.

E. Performance Metrics

The measured performance metrics are summarized below. Experimental results indicate:

- AES encryption latency: 38 ms
- Key rotation overhead: < 10 ms
- Packet delivery ratio (PDR): 97.8%
- Communication range: up to 3 km (Line of Sight)

The system maintained stable indoor and outdoor transmission performance with no observed replay acceptance or decryption failures under synchronized conditions.

IX. SECURITY ANALYSIS

The system assumes adversaries capable of passive listening and replay attacks. Dynamic key rotation significantly reduces vulnerability to brute-force attacks since captured ciphertext becomes obsolete after each interval.

X. CONCLUSION

This work introduces a secure and resilient communication system for battlefield environments using AES-128 dynamic key switching. Experiments confirm low latency, long-range coverage, and strong resistance to key compromise, demonstrating substantial improvement over static-key systems.

REFERENCES

- [1] F. Adelantado et al., "Understanding the Limits of LoRaWAN," IEEE Communications Magazine, 2017.
- [2] R. Merkle, "Protocols for Public Key Cryptosystems," IEEE S&P, 1980.
- [3] M. Simplicio Jr. et al., "Lightweight Cryptography for Wireless Sensor Networks," IEEE IoT Journal, 2019.
- [4] S. Raza et al., "SVELTE: Real-time intrusion detection in IoT," IEEE TMC, 2018.
- [5] J. Granjal et al., "Security for the IoT: A Survey," IEEE Commun. Surveys, 2015.

- [6] K. Mikhaylov et al., "LoRaWAN Security Analysis," ICUMT, 2019.
- [7] Z. Qin et al., "Lightweight Authentication for LoRaWAN," IEEE Access, 2020.
- [8] D. He et al., "Certificateless Cryptography for Lightweight Devices," IEEE Systems Journal, 2016.
- [9] P. Kumar et al., "Secure Communication for Military IoT," IEEE MILCOM, 2020.
- [10] A. Das, "Lightweight Cryptography for IoT Security," IEEE Access, 2021.
- [11] J. Hernandez and A. Somani, "AES Acceleration on ESP32," IEEE Embedded Systems Letters, 2020.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.