A Frame-Based Architecture for Enhanced Secure IoT Communication with Ascon-128a

The First International Conference on Intelligent Aerial Access and Applications - IAAA 2025

Huu-Tu Hoang, Duc-Hung Le

The University of Science - VNU, Ho Chi Minh City, Vietnam
Faculty of Electronics and Telecommunications

dd/MM/2025

TABLE OF CONTENTS

MOTIVATION

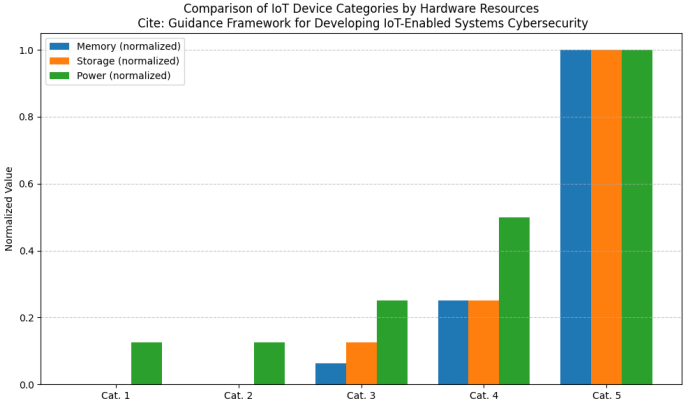
- Most IoT devices operate with constrained computational capabilities and limited resources.

Bảng 1: Classification of IoT devices based on hardware capabilities.

Category	CPU	RAM	Storage	Power	Example
Category 1	8-bit, 16 MHz	$\leq$ 32 KB	Small	$\leq$ 1 W	Arduino Mega
Category 2	32-bit, 80 MHz	32–80 KB	Small	$\leq$ 1 W	NodeMCU ESP-12
Category 3	Single-core, 1 GHz	80 KB–512 MB	$\leq$ 4 GB	1–2 W	Raspberry Pi Zero
Category 4	Quad-core, 1.2 GHz	512 MB–2 GB	$\leq$ 8 GB	2–4 W	Raspberry Pi 3
Category 5	Quad-core, 2 GHz	$\geq$ 8 GB	$\geq$ 32 GB	High	Jetson TX2

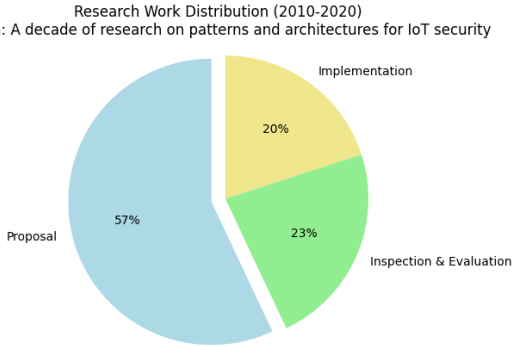
MOTIVATION

- Most IoT devices operate with constrained computational capabilities and limited resources.



MOTIVATION

- Research on implementing complete IoT architectures remains limited.

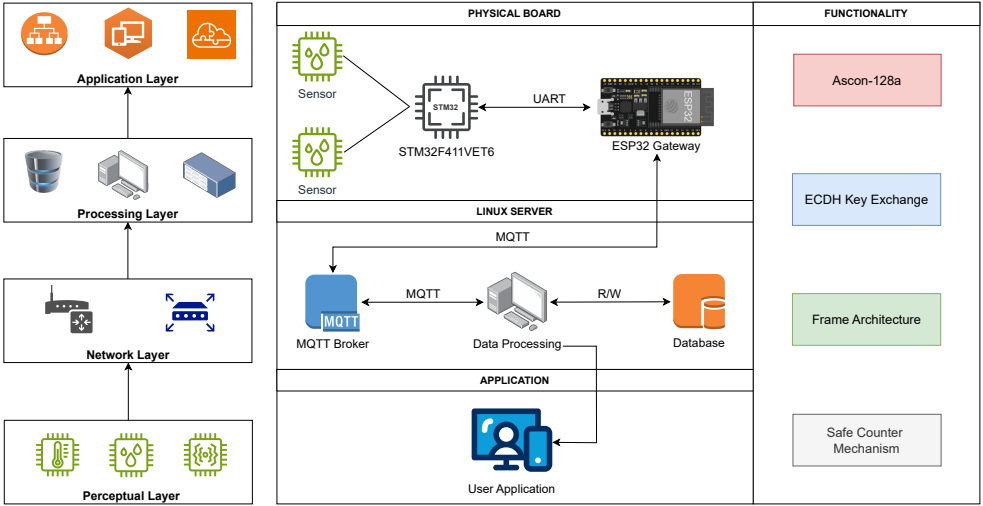


Objectives and Contributions

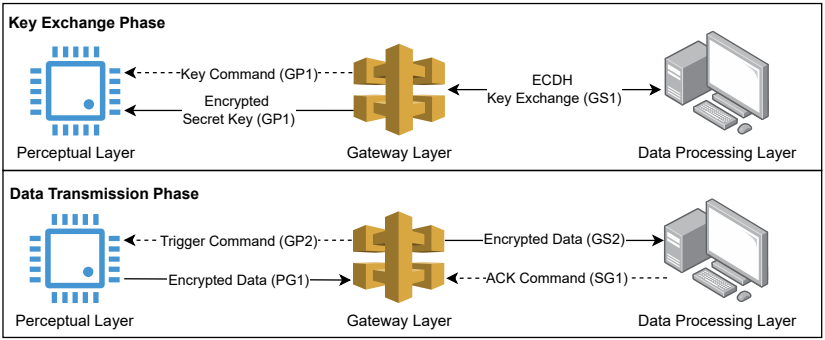
This work aims to develop a complete IoT architecture that fulfills the following goals:

1. Compatible with a **wide range** of hardware platforms.
2. Ensures **data integrity** and **confidentiality** during transmission.
3. Provides mechanisms to **mitigate common attacks**.
4. **Implementation** on real hardware and performance benchmarking.
5. Can be used as a **reference** framework for future IoT implementations.

SYSTEM ARCHITECTURE

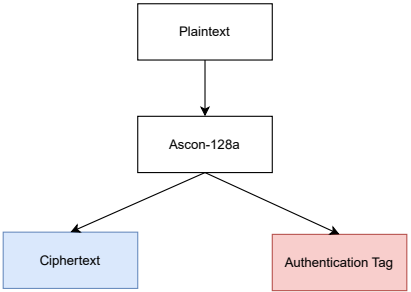


COMMUNICATION MODEL

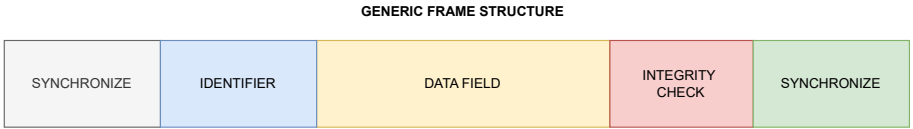


THE ASCON-128a LIGHTWEIGHT CRYPTOGRAPHIC

- Finalist of the NIST Lightweight Cryptography Standardization.
- Designed for constrained devices.
- Support AEAD providing both confidentiality and integrity.
- Used in this system to encrypt data and generate Auth Tag for each frame.



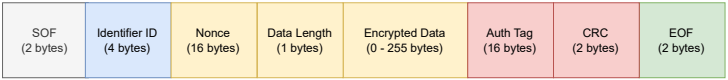
FRAME ARCHITECTURE



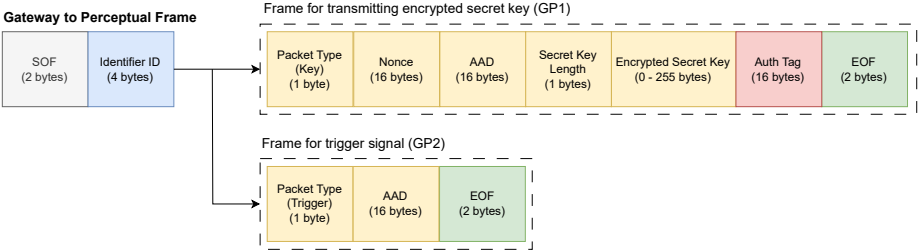
FRAME ARCHITECTURE

Perceptual to Gateway Frame

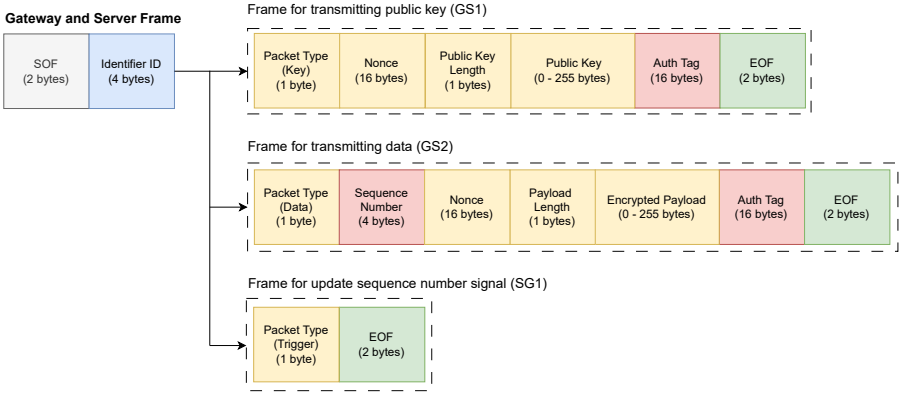
Frame for transmitting encrypted data (PG1)



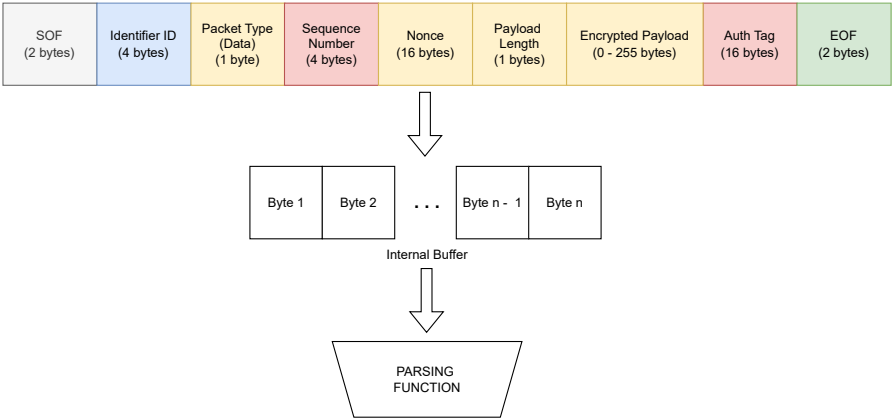
Gateway to Perceptual Frame



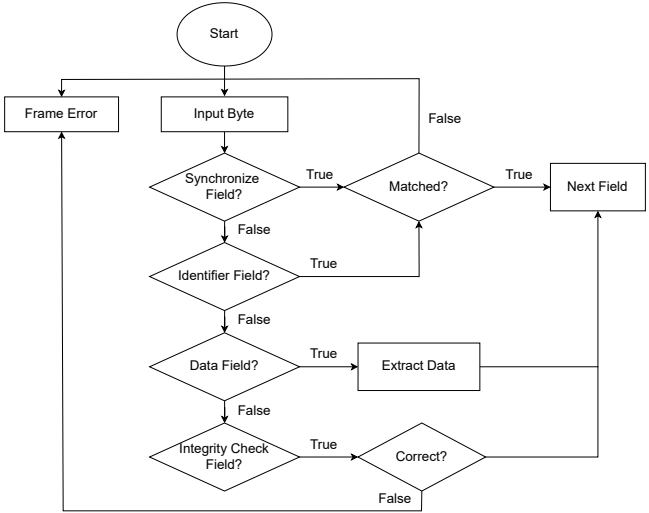
FRAME ARCHITECTURE



FRAME PARSING PROCESS



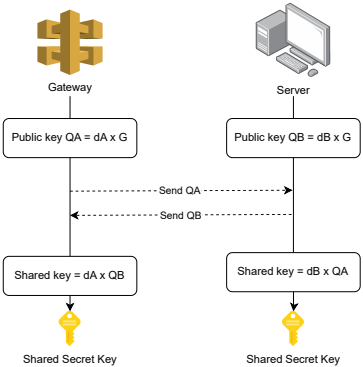
PARSING FUNCTION



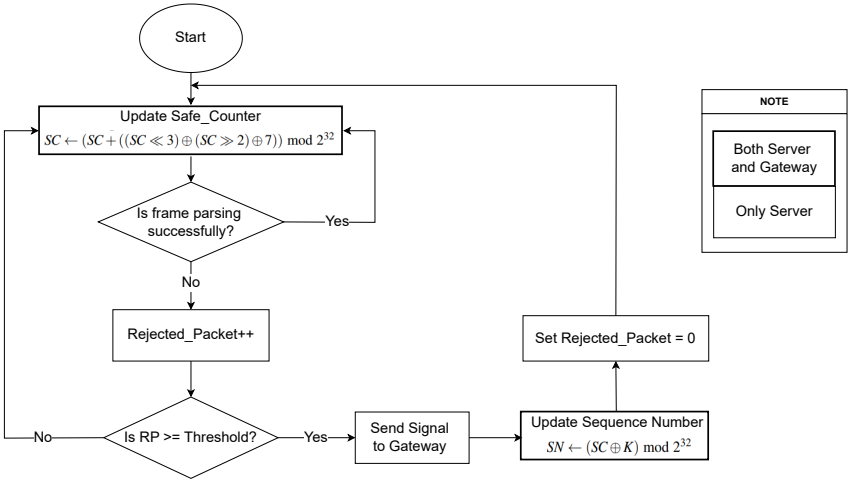
DYNAMIC KEY EXCHANGE

Frame for transmitting public key (GS1)

SOF (2 bytes)	Identifier ID (4 bytes)	Packet Type (Key) (1 byte)	Nonce (16 bytes)	Public Key Length (1 bytes)	Public Key (0 - 255 bytes)	Auth Tag (16 bytes)	EOF (2 bytes)

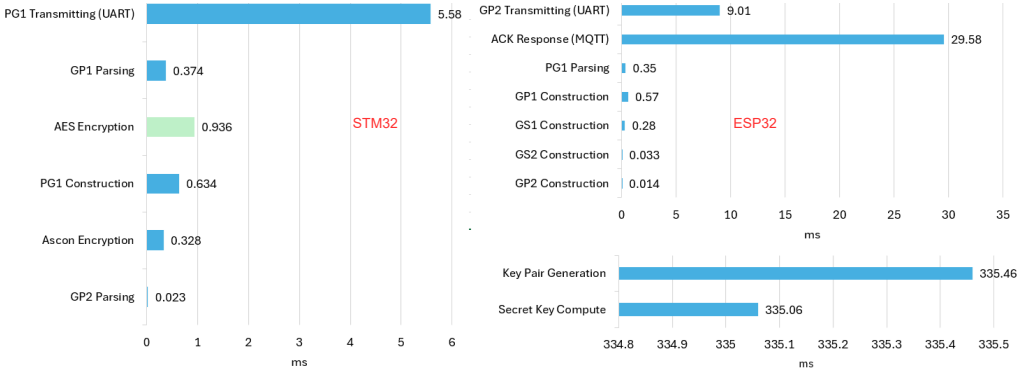


SAFE COUNTER MECHANISM

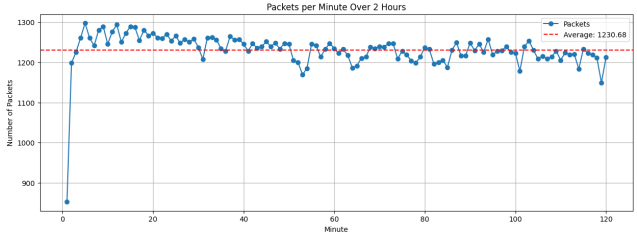


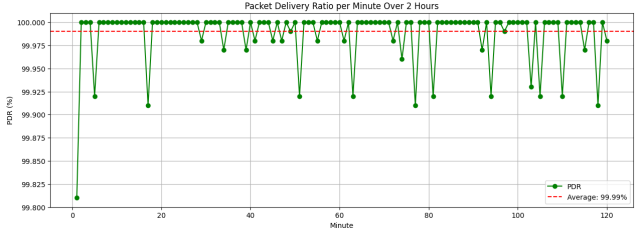
TIME EXECUTIONS

Total transmission time averages 49.91 ms.

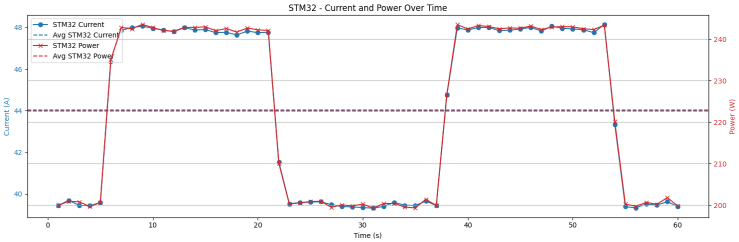


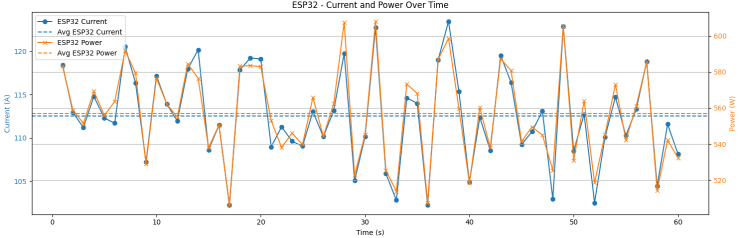
PACKET DELIVERY RATIO





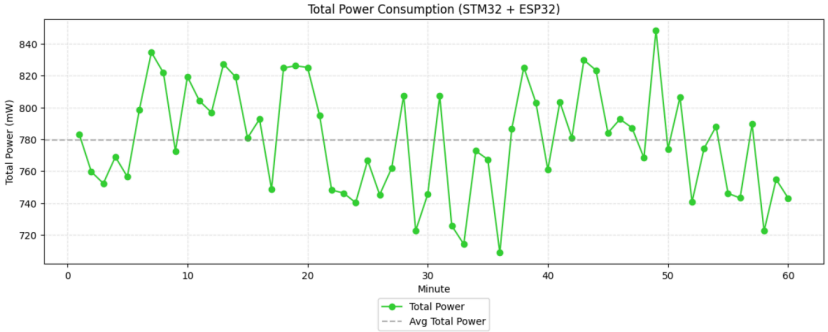
POWER CONSUMPTION





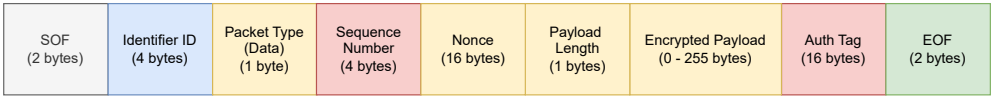
POWER CONSUMPTION

Total power consumption averages 779.43 mW.



PAYLOAD EFFICIENCY

Analyze based on the GS2 frame and 3 bytes data.



With 3 bytes data, total frame size is 49 bytes $\Rightarrow$ Payload efficiency is $\frac{3}{49} \approx 6.12\%$

PAYLOAD EFFICIENCY

Bảng 2: Payload efficiency with different payload lengths

Payload Length	Total Frame Size	Efficiency
3 bytes	49 bytes	6.12%
10 bytes	56 bytes	17.85%
20 bytes	66 bytes	30.30%
50 bytes	96 bytes	52.08%

$\Rightarrow$ The larger the payload, the higher the payload efficiency.

ACHIEVEMENTS

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

1. Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
2. Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
3. Kỹ thuật trao đổi khóa trên đường cong Elliptic.
4. Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
5. Mật mã hóa nhẹ Ascon-128a.
6. Cơ chế bảo mật *Safe Counter*.

DISADVANTAGES

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

1. Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
2. Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
3. Kỹ thuật trao đổi khóa trên đường cong Elliptic.
4. Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
5. Mật mã hóa nhẹ Ascon-128a.
6. Cơ chế bảo mật *Safe Counter*.

FUTURE WORK

Các kỹ thuật được triển khai thành công trên phần cứng và máy chủ.

1. Các kỹ thuật giao tiếp được triển khai theo đúng yêu cầu đặt ra.
2. Xây dựng kiến trúc khung truyền linh hoạt bao gồm cấu trúc và phân giải.
3. Kỹ thuật trao đổi khóa trên đường cong Elliptic.
4. Kỹ thuật tọa khóa phiên dựa trên hàm băm Ascon-Hash.
5. Mật mã hóa nhẹ Ascon-128a.
6. Cơ chế bảo mật *Safe Counter*.

Thank you for your attention!