ML-Assisted Hybrid Lightweight Cryptographic Framework for Secure IoT Intrusion Detection

S Bharath
SIR MVIT
Bharathsanjay2004@gmail.com

Aashish Choudhary
SIR MVIT
aashishchourdhary7@gmail.com

L Yashwant Reddy
SIR MVIT
yashhwanttreddy@gmail.com

R Dheeraj Kumar
SIR MVIT
dheerajk5824@gmail.com

Abstract - This paper presents an adaptive hybrid lightweight cryptographic framework designed for resource-constrained Internet of Things environments. Conventional cryptographic mechanisms such as the Advanced Encryption Standard provide strong security but incur significant computational overhead, while lightweight ciphers such as SPECK offer efficiency at the cost of reduced security strength. To address this trade-off, we propose a hybrid model integrating AES-128 and SPECK-128/128, enhanced with a machine-learning-based decision module capable of selecting the most suitable algorithm at runtime based on system conditions and threat indicators. The system is implemented using two ESP8266 nodes configured as a real-time intrusion detection network where Node A performs IR-based sensing and encryption, and Node B performs decryption, anomaly detection, and defensive actuation via relay and buzzer. Attack scenarios including replay attacks, tampered ciphertext injection, and flooding are simulated to generate training data. A Decision Tree classifier is trained on features such as encryption time, free heap memory, message frequency, IR state, and plaintext validity. Experimental results demonstrate that the ML-assisted hybrid approach improves detection accuracy and dynamically balances efficiency and security. The framework provides a deployable and cost-effective solution for intrusion-resilient IoT security.

Index Terms - Adaptive cryptography, intrusion detection, IoT security, lightweight encryption, machine learning.

INTRODUCTION

These instructions serve as a template for Microsoft Word and give you the basic guidelines for preparing papers for ProComm 2024, July 14 - 17.

Please enable "Show Comments" and carefully follow these instructions to ensure legibility and uniformity.

The rapid adoption of Internet of Things (IoT) systems has increased the need for efficient and secure communication mechanisms. IoT devices typically operate with limited memory, processing power, and energy, making them vulnerable to a variety of cyber-attacks. Traditional cryptographic techniques such as the Advanced Encryption Standard (AES) offer strong protection but are often unsuitable for constrained nodes due to their high computational and energy overhead. Lightweight cryptographic alternatives such as SPECK provide faster execution and lower memory usage but do not offer the same level of cryptographic strength.

Recent research highlights the need for adaptive cryptographic mechanisms capable of balancing security and performance depending on contextual conditions. However, existing solutions are largely static and do not adapt dynamically to attack patterns, system load, or environmental changes. This paper proposes an adaptive hybrid cryptographic framework that leverages machine learning (ML) to autonomously switch between AES and SPECK based on real-time metrics collected from IoT devices.

For numbered lists you should follow these guidelines: The contributions of this work include:

1) A working hybrid cryptographic model combining AES-128 and SPECK-128/128;
2) A two-node ESP8266 intrusion detection system with encrypted communication;
3) An ML-based attack detection and encryption-selection mechanism;
4) Real-world evaluation under replay, tampering, and flooding attacks.

SYSTEM ARCHITECTURE

The proposed system consists of two ESP8266 microcontroller nodes operating over UART serial communication.

I. Node A: Sensor and Encryption Node

Node A interfaces with an infrared (IR) sensor to detect intrusion events. Based on its ML-assisted decision module, it encrypts the "ON/OFF'' intruder state using either AES-128 CBC or SPECK-128/128. It serializes the 16-byte ciphertext into a 32-character hexadecimal string and transmits it to Node B.

II. Node B: Decryption and Defense Node

Node B receives the ciphertext, converts it from hex to binary, and performs decryption using the appropriate algorithm. It validates message integrity, detects anomalies, and triggers alarms via a relay and buzzer. Node B also logs runtime parameters used as ML features.

ATTACK MODEL AND FEATURE EXTRACTION

Three attack types are simulated to generate training data:

I. Replay Attacks

Repeated transmission of previously captured ciphertexts. Indicators: repetitive ciphertext, low entropy in message sequence.

II. Tampered Ciphertext

Corrupted or modified ciphertext leading to invalid plaintext. Indicators: msgValid = 0, inconsistent block lengths.

III. Flooding Attacks

High-frequency message bursts. Indicators: msgFreq > 10 messages/sec.

IV. Extracted ML Features

- IR sensor state (irVal)
- Encryption time (encTime)
- Free heap memory (heap)
- Message frequency (msgFreq)
- Plaintext validity (msgValid)

These features are logged during operation and compiled into a dataset for ML training.

ML-ASSISTED HYBRID CRYPTOGRAPHIC SWITCHING

A Decision Tree classifier is trained on 500+ samples labeled as attack or safe. The Python scikit-learn model outputs simple decision rules that are manually converted into lightweight IF-ELSE logic on the ESP8266.

I. Example extracted rule:

```
if msgValid == 0:
   attack = 1
elif msgFreq > 10:
   attack = 1
elif encTime > 3000:
   attack = 1
else:
   attack = 0
```

II. Switching Logic

```
if attack == 1:
   encryptionAlgorithm = AES
else:
   encryptionAlgorithm = SPECK
```

This yields both performance improvement and enhanced security by applying stronger encryption only when necessary.

IMPLEMENTATION

I. Hardware Design

The system uses ESP8266 NodeMCU boards, IR sensor, relay module, active buzzer, breadboard, and serial wiring. Node A and Node B communicate via SoftwareSerial (D5/D6).

II. Cryptographic Modules

AES-128 CBC uses the CryptoAES_CBC library, while SPECK-128/128 is implemented manually using 32-round Feistel operations with rotation and XOR primitives optimized for 32-bit platforms.

III. Dataset Collection

Runtime metrics from both attack and normal conditions are streamed to a PC and stored in CSV format. These samples include both ML features and ground-truth attack labels.

RESULTS AND ANALYSIS

I. Performance Comparison

AES encryption requires ~2300 µs on average, compared to ~350 µs for SPECK. Memory consumption of AES is approximately 30% higher. SPECK significantly improves throughput in safe conditions.

II. ML Detection Accuracy

The Decision Tree classifier achieves:

- Accuracy: 94.1%
- Attack recall: 96%
- Precision: 90%

III. Defense System Response

The system triggers relay and buzzer within less than 10 ms after decryption of an "ON'' intruder signal. Replay and tampering attacks were reliably detected by ML.

CONCLUSION

This work demonstrates a practical hybrid cryptographic model combining AES and SPECK with ML-assisted adaptive switching for real-world IoT intrusion detection. The two-node ESP8266 implementation validates that ML-based decision systems can efficiently detect attacks and dynamically choose the appropriate cryptographic strength. The proposed design enhances both security and performance, making it suitable for low-power IoT systems.

FUTURE WORK

Future enhancements include:

- Integration with Wi-Fi-based secure communication (MQTT).
- Deployment on ESP32 or RISC-V hardware.
- Additional ciphers such as PRESENT, GIFT, CHACHA20.
- On-device incremental ML learning.
- Cloud-based attack logging and anomaly analytics.

REFERENCES

[1] M. S. Islam and M. R. Amin, "A Recent Review on Lightweight Cryptography in IoT," IEEE Access, vol. 12, pp. 1–15, 2024.

[2] N. T. Nandhini and R. Latha, "Designing a Lightweight IoT Authentication Protocol for Resource-Constrained Devices," in Proc. ICICAT, 2024, pp. 961–966.

[3] S. Dhakare et al., "Securing the IoT Device Network with Lightweight Cryptography," in Proc. WPMC, 2024, pp. 1–6.

[4] A. Prakash et al., "A New Model of Lightweight Hybrid Cryptography for IoT," in Proc. ICECA, 2019, pp. 1305–1309.

[5] A. Tiwari and R. Mishra, "A Hybrid Lightweight Cryptographic Scheme for IoT Devices," IEEE Conf. Publ., 2021.

[6] M. A. Khan and H. T. Malik, "Lightweight Cryptography Algorithms for IoT Devices," IEEE Access, vol. 9, pp. 126146–126170, 2021.

ABOUT THE AUTHORS

S Bharath, Aashish Choudhary, L Yashwant Reddy, and R Dheeraj Kumar are final-year (4th year) students pursuing B.E. in Computer Science and Engineering (IoT, Cybersecurity, including Blockchain Technology) at Sir M. Visvesvaraya Institute of Technology (SIR MVIT), Bengaluru, India. Their academic interests include embedded systems, lightweight cryptography, IoT security, machine learning, and secure communication architectures. They collaboratively work on research-driven projects focused on modern IoT security challenges and adaptive cryptographic frameworks.