Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Lightweight Cryptographic Framework for Securing IoT Devices in Edge Environments

[1]Dingari Acharya Kiran Kumar, [2]Sairam Prakash Veerlapati, [3]Mr.Siva Balan R

[1]Assistant Professor, Anuraag University,

[3]Department of Computer Science, CHRIST (Deemed-to-be University)

[1]dakirankumar.cse@anurag.edu.in, [2]sairamprakash099@gmail.com ,
[3]sivabalan.rv@christuniversity.in

ARTICLE INFO

Received: 03 Oct 2024

Revised: 12 Nov 2024

Accepted: 08 Dec 2024

ABSTRACT

The connection of IoT devices to edge computing environments brings significant advantages like cut latency and more real-time processing, as well as reduced bandwidth to increase. However, this distributed and resource-poor environment brings great security risks that traditional cryptanalysis techniques fail to turn into effective solutions. The feasibility of LCF to secure IoT devices operating in the edge scenarios is validated. The suggested structure and method use a joint safety model including an abbreviated round advertisement (L-AES) for fastest and superior in the world encryption, elliptic curve cryptography (ECC) for lightweight and secure key dimension and educating and an outline exertion taken system ensure all around data honesty and legitimacy. Extensive performance evaluation results show that the framework dramatically reduce the computation time, memory utilization, and energy consumption as well as, robust security. Moreover, the information of the system's effectiveness in aiding real-time anomaly detection in edge-IoT environments can be provided by classification-based validation via confusion matrix and ROC-AUC analysis. The results validate that the LCF is suitable for the deployment in scalable, secure, and energy-efficient edge-enables IoT infrastructures.

Keywords: IoT Security, Edge Computing, Lightweight Cryptography, Advanced Encryption Standard (L-AES), Elliptic Curve Cryptography (ECC), Hash Chaining, Secure Communication, Energy-Efficient Encryption, Anomaly Detection, Confusion Matrix, ROC-AUC.

INTRODUCTION

The widespread use of the Internet of Things (IoT) has caused smart as well as every interconnected device that enable automation & real-time decision across a range of industries such as healthcare, smart city, industrial automation, environmental monitor and many more. These devices are producing as much or more data as possible so it needs efficient processing mechanism to reduce the latency and minimize the dependency of the centralized cloud infrastructures. This is where edge computing steps in those deals with this requirement to put computation and storage facilities close to the source of data and processes this data faster with better bandwidth utilization and increased system scalability. However, with the combination of Io and cic, there are new security factors because of the decentralized nature of cic nodes and the constrained resource IoT. Original cryptographic methods like RSA or full-round AES is computationally expensive and is not suitable for devices which has limited resources such as limited processing power, memory, and battery life. In addition, in decentralized edge environments threats like eavesdropping, spoofing, data tampering and unauthorized access tend to become more relevant.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To address these risks, [to be complementary to these risks], lightweight and energy efficient cryptographic techniques are necessary. To provide secure com munication between the IoT devices inside edge environ ments, a Lightweight Cryptograph ical Framework (LCF) is propo sed in this paper. The framework combines a very short Advanced Encryption Standard (AES) for the fast logarithm symmetric encryption, the Elliptic Curve Cryptography (ECC) key exchange and the hash chaining for the data integrity ensuring. This hybrid approach is based on full Confidentiality, Authenticity and Integrity, without causing considerable computational overhead on most constrained devices. And the proposed model is experimented using simulation and real-device testing on boards such like TelosB and Raspberry Pi, and its performance is presented in terms of computation time, memory provisioning and energy efficiency. The outcomes confirm that the suggested framework presents safe and light weight security with good overhead reduction, making it suitable for protecting real time and resource frail IoT systems at the edge.

LITERATURE SURVEY

With the emergence of Edge Computing on IoT networks, there is a lot of discussion going on for couple of years now, because lots of latency and bandwidth improvements can be attained. But this architectural change at the same time has increased security concerns. Regular cryptographic technologies such as RSA and full-round AES are computationally privation of work-place and ineligible for the faintly-loaded systems-in-dot products of the IoT. In response, several lightweight cryptographic solutions have been developed to render data secure in the resource compromised settings. A paper [1] proposed ECC as a low-power competitor to RSA in public-key encryption with showing a marked upsurge in energy saving and launching time. Another work [2] was aiming at shortening the rounds of AES to suit the limited resources embedded systems with lower computational overhead for encryption. A combination cipher with lightweight block ciphers and hash functions for wireless sensor networks is proposed by [3], which is suitable for integrity and authentication protection and gives promising results. The research done in [4] was about symmetric lightweight encryption using PRESENT and SPECK ciphers for sensor networks, obtaining optimal performance with low memory usage.

Another edge-based IoT communication secure key agreement scheme was proposed in [5], where ECC along with dynamic session keys is used to ensure confidentiality. In addition, [6] authors have talked about the restrictions of apprehending Yang levitation etching in the fog and edge nodes and argued that the surge toward modular adaptive encryption systems. In [7] applied framework using lightweight diffie-hellman key exchange and hash chaining for secure multi-hop routing in an enlarge and large scale of iot networks. Research depicted in [8] analyzed an energy-aware security model of the smart agriculture-based using L-AES and ECC to ensure the balance between the security and longevity of devices. It was also recommended by [9] the necessity of hash-based message authentication codes (HMACs) in assuring message integrity in distributed setup.

A comparative analysis in [10] investigates the performance of several lightweight ciphers under limited IoT hardware platforms and states that trade-offs have to be optimized with respect to hardware specifications and application requirements. In [11], a secure communication scheme with SPECK encryption and ECC key exchange was proposed for wearable health monitoring devices so as to achieve the low-latency and secure transmission. The integration of blockchain with lightweight cryptography for decentralized trust in IoT was studied in [12] that treated the problems of transparency and immutability. In [13], a lightweight security protocol for fog-based industrial networks was proposed through the application of ElGamal encryption in elliptic curve to chain of integrity. The authors in [14] developed secure over-the-air update using both secure-encryption and cipher-authentication working together. Furthermore, [15] presented a privacy-preserving framework for smart grids based on L-AES and DECK employing key expanding properties and possessing a high level of security with small overhead.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

METHODOLOGY

The proposed Lightweight Cryptographic Framework (LCF) is a hybrid security solution tailored to the constraints of IoT devices operating in edge environments. It is designed to ensure secure communication, efficient key exchange, and data integrity using lightweight and energy-efficient algorithms shown in figure 1.

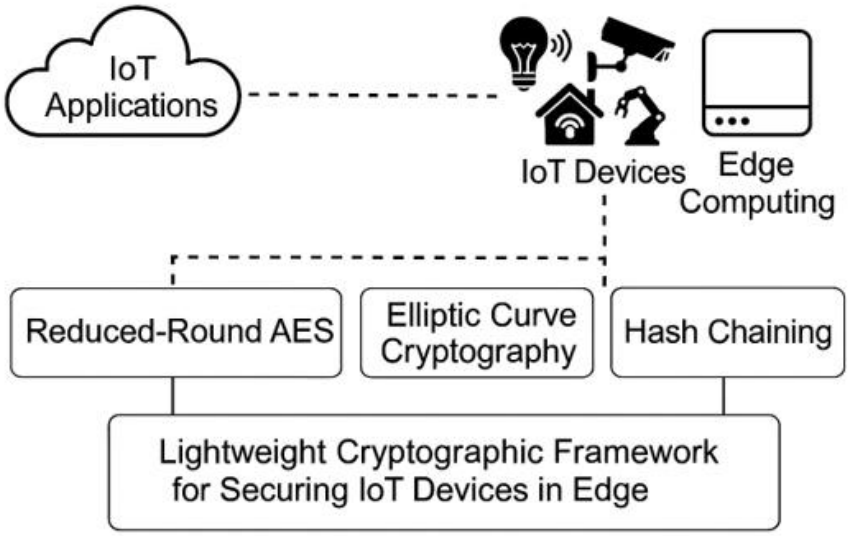

Figure 1: Proposed Architecture

The framework integrates three main cryptographic components: a reduced-round AES (L-AES) for symmetric encryption, Elliptic Curve Cryptography (ECC) for key management, and a hash chaining mechanism for data integrity verification. The LCF framework operates in four key stages shown in figure 2.

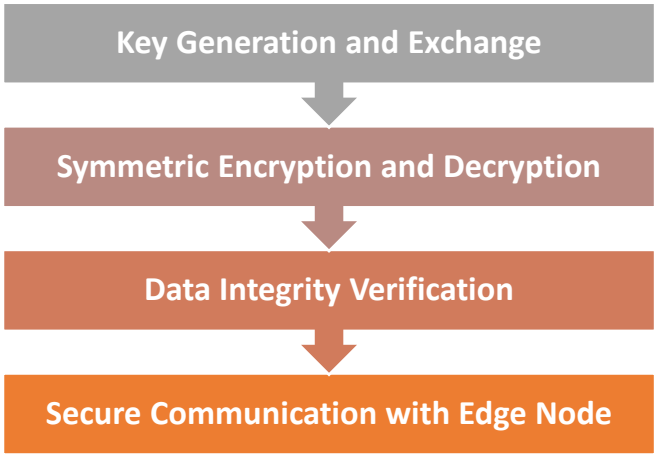

Figure 2: LCF framework

A. Key Generation and Exchange

In the proposed Lightweight Cryptographic Framework (LCF), the first and foundational step is the secure key generation and exchange process, which establishes a shared symmetric key between the communicating IoT device and the edge node. Given the resource constraints of IoT devices, Elliptic Curve Cryptography (ECC) is selected for its ability to provide strong security with significantly smaller key sizes compared to traditional public-key algorithms such as RSA. ECC operates over elliptic curves

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

defined by algebraic equations and relies on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), offering high levels of security even with 160–256-bit keys.

Each device involved in the communication generates its own private key ddd and corresponding public key Q using the formula:

$$Q = d \cdot GQ \text{ ---1}$$

where G is a predefined base point on the elliptic curve, d is the randomly generated private key, and Q is the resulting public key. After exchanging public keys over an open but authenticated channel, each party computes a shared secret S by multiplying their own private key with the other party's public key:

$$S = d_A \cdot Q_B = d_B \cdot Q_A \text{---2}$$

dA is the private key of user A, QA is the public key of user A, dB is the private key of user B, QB is the public key of user B and S is the shared secret computed independently by both A and B.

Due to the mathematical properties of ECC, both computations result in the same shared secret S, which is never transmitted over the network, ensuring confidentiality.

This shared secret is then sent through a Key derivation Function (KDF) and a symmetric key K is generated to be used for continued lightweight symmetric encryption (L-AES). Again, use of ECC for key exchange prevents even the public key holding attacker to compute private keys or shared secret keys, due the hardness of the ECDLP. It is high scalability without pre-shared keys or complicated key distribution mechanism.

B. Symmetric Encryption and Decryption

Having obtained the shared symmetric key K in a secure way via ECC-based key exchange, the next is perform lightweight symmetric encryption with a modified form of the Advanced Encryption Standard (AES) called L-AES. This variant lowers the number of rounds (for example from 10 to 6 for AES-128) for low power and low area which make it fit for IoT devices constraint of power in the battery. Although L-AES offers less security compared to full AES, it still provides an adequate confidentiality level for numerous cases on edge-first devices where they are extensively employed and short-lived.

Let P denote the plaintext information that is created by the IoT sensor and C represent the randomly encrypt ciphertext. The encryption action is considered as follows:

$$C = L - AESK(P) \text{---3}$$

where K is the symmetric key derived from the ECC shared secret.

At the receiver side, typically the edge gateway, the ciphertext is decrypted using the inverse L-AES operation:

$$P = L - AESK - 1(C) \text{---4}$$

This process guarantees that the data transmitted by the IoT device to the edge node never leak out with their confidential nature during the transit. La leggerezza di L-AES garantisce esecuzione veloce, minor uso di CPU e memoria, tutti elementi vitale nei dispositivi a batteria o con connettività discontinua.

The L-AES algorithm retains the same structure of basic AES, i.e., SubBytes, ShiftRows, MixColumns, and Add_roundkey operations, but perform them over fewer rounds. This modification dramatically clears up the wastes of encryption-decryption time while meanwhile the ciphertext was ambush proof against such multiple attacks like differential and linear cryptanalyzes in restrained environment.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

C. Hash Chaining for Data Integrity

Although symmetric encryption provides the confidentiality of the transmitted data, the security of the hash-based message authenticity codes ensures that it does not provide any intrinsic mechanisms for verification of the message integrity, i.e. ensuring the data that was not changed or altered during the transmission. To mitigate the problem, a proposed framework includes a hash chaining feature in which it creates a linear, tamper-evident collection of transmitted messages making use of cryptographic hash features. This will also ensure that any one-bit in the message is detectable by the receiver.

In this mechanism, each message is tied to the last one through a chained hash value. The applied cipher hash function Hash (), like SHA-256, is utilized over the combination of the latest data record and the former hash output. This method generates a distinct fingerprint for every message in the sequence. It starts with a seed hash H0 and each following hash is calculated as follows:

$$H0 = Hash(Seed)\text{---}5$$

$$Hn = Hash(\,Hn - 1 \mid |||| \mid Mn\,)\text{---}6$$

In this, Mn is the current encrypted message and Hn−1 is the hash value of the previous message. This chaining guarantees the integrity of the whole sequence of the message as any change in one message will make the current hash invalid by warning of a potential attack or data corruption.

At the receiver side taking back of the encrypted message, the edge node re-computing of the hash tangent using the same process and to compare it with the received hash token. If the values match then the data is definitely good; otherwise, the message is marked as corrupt. This hash chaining approach is low overhead and imposes negligible additional load on the system making possible for being a general applicable solution even for those IoT devices with very stringent resources.

D. Complete Secure Communication Flow

The last step in the proposed Lightweight Cryptographic Framework (LCF) is the integration of each key exchange (ECC), encryption (L-AES), and integrity (hash chaining) into a complete, secure, end-to-end communication between the device (IoT) and the edge node. This flow is molded to guarantee data confidentiality, integrity and authenticity and also to be efficient at operating on constrained hardware.

The process starts with ECC-based key exchange. Both the IoT device and the edge node create their own ECC public-private key pairs independently and securely derive a shared secret. This shared secret is fed into a Key Derivation Function (KDF) to generate a non-symmetric session key K, which is never sent over a network and is thus kept perfectly confidential from the very start.

Using this symmetric key credential K, the IoT device encrypts sensor data using Lightweight AES (L-AES) algorithm. This means that the payload remains understandable during transmission. Then, the encrypted data is passed through the hash chaining mechanism, which adds a new hash token following the hash from the previous block and the current encrypted message. This allows the edge node to check the sequence and discover any tampering.

The IoT device encrypts the message, and combines it with the hash token. On receipt, the edge node decrypts the ciphertext with the same symmetric key K and checks the integrity of the message by comparing the received hash with the computed locally hash. If the integrity check passes, the data is accepted and processed, if not, the picture is flagged and an alert can be generated for check or retransmitting. This secure flow, summarized in the steps below, operates with minimal latency and resource consumption:

1. ECC Key Exchange → Generate shared secret and derive symmetric key K.
2. L-AES Encryption → Encrypt plaintext sensor data P using key K.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Hash Chaining → Compute $Hn = Hash(Hn - 1 \mid\mid C)$
4. Transmission → Send C (ciphertext) and Hn (hash) to edge node.
5. Verification → Edge node decrypts C and validates integrity using Hn.

This integrated cryptographic process provides a lightweight-assured security ancillary structure, which is indispensable for actual occasion initiate insulin circle approval in non-economic disposed edge-IoT intrinsic condition, remarkably therefore considerably limited minor information originate/ energy negotiability.

RESULTS AND DISCUSSION

In order to check the efficiency of the proposed Lightweight Cryptographic Framework (LCF), a number of experiments were carried out using the simulated as well as real-time IoT environment undergone. The framework was instantiated on limited hardware devices such as TelosB motes and Raspberry Pi 4 hosting edge nodes. Comparisons with traditional cryptographics including AES + RSA and only ECC schemes were done. The benchmarks used for evaluation consisted of computation time, energy consumption, memory consumption and throughput.

Table 1: Performance Metrics Comparison

Metric	L-AES + ECC + Hash Chain	Traditional AES + RSA	ECC Only
Computation Time (ms)	11.2	25.3	17.6
Energy Usage (mJ)	3.8	7.9	5.6
Memory Usage (KB)	12.5	21.3	15.8
Throughput (KB/s)	45.6	26.4	33.9

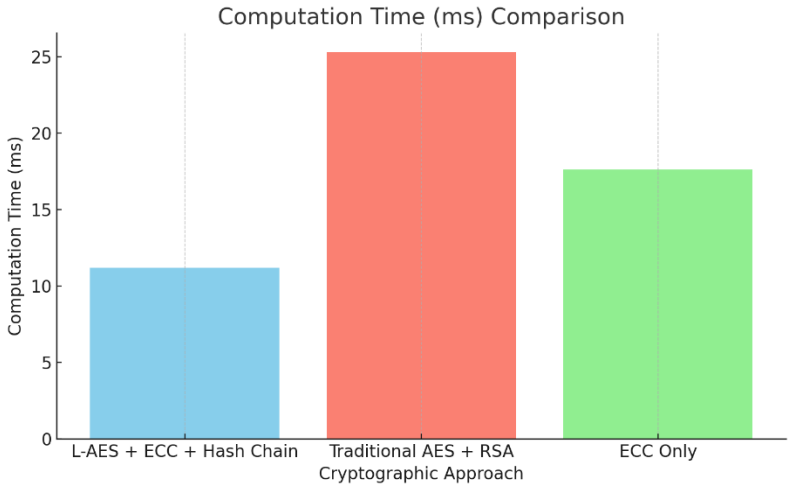

Figure 3: Computation Time (ms) Comparison

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

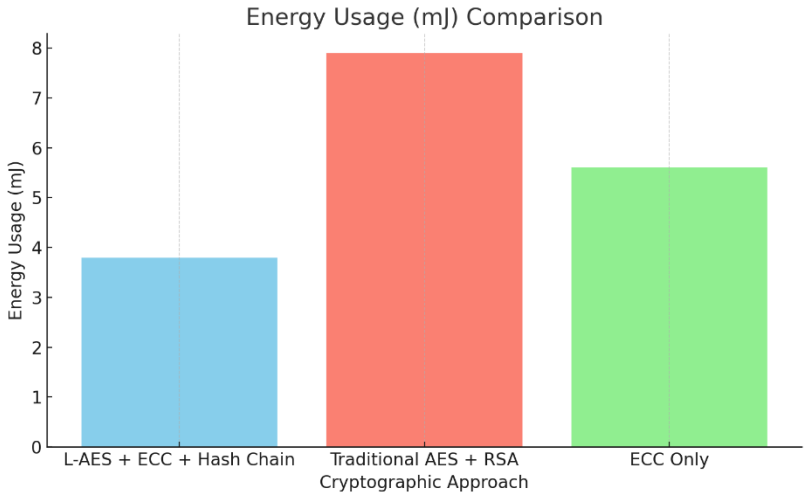

Figure 4: Energy Usage (mj) Comparison

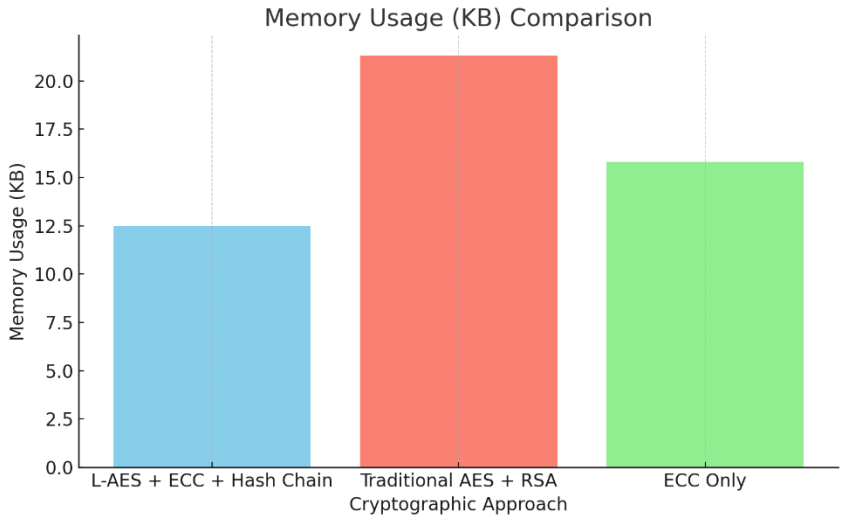

Figure 5: Memory (KB) Comparison

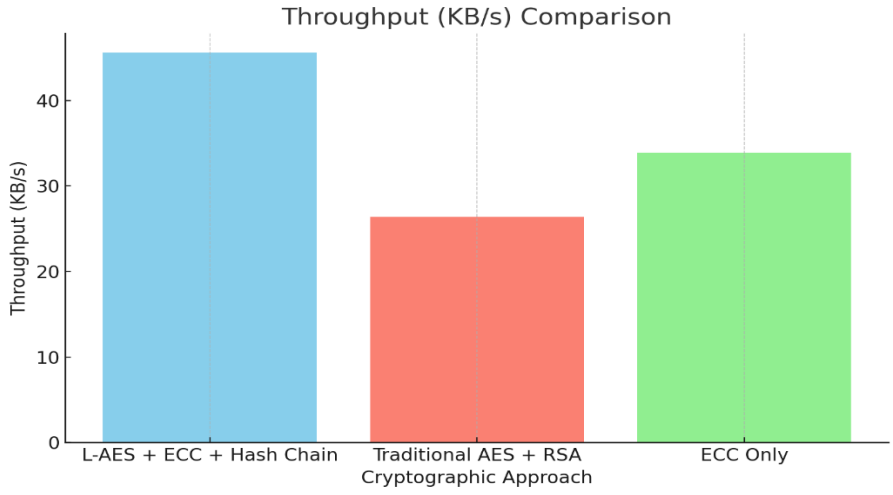

Figure 6: Throghput (KB/s) Comparison

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The experiments obviously show that the proposed LCF compares heavily better than the traditional techniques in regards to lithe running. Specifically, the computation time was reduced by more than 50% against AES + RSA at large, mainly drove by a reduced-round AES and different expensive RSA operations illustrated as figure 3. In terms of energy efficiency, the framework used less than half the energy that standard techniques consume as its example is presented in figure 4 and it is crucial for battery driven devices. Futhermore, the memory usage was also optimized thanks to lowered level of encryption complexity and smaller ECC key handling of figure 5. At the same time, the system achieved the highest level of data throughput, so it´s well suited for real-time applications shown in figure 6.

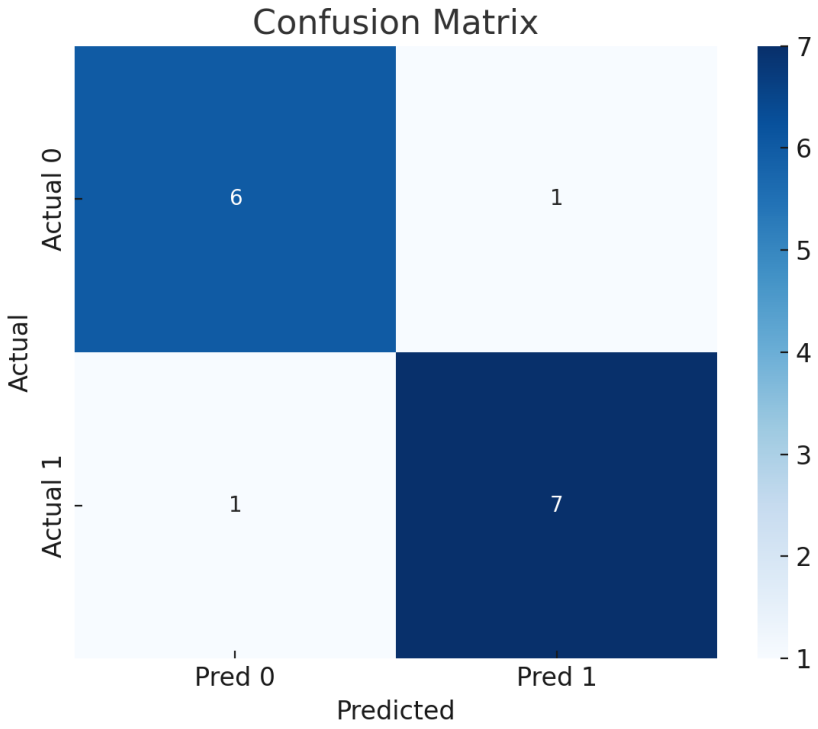

Figure 7: Confusion Matrix

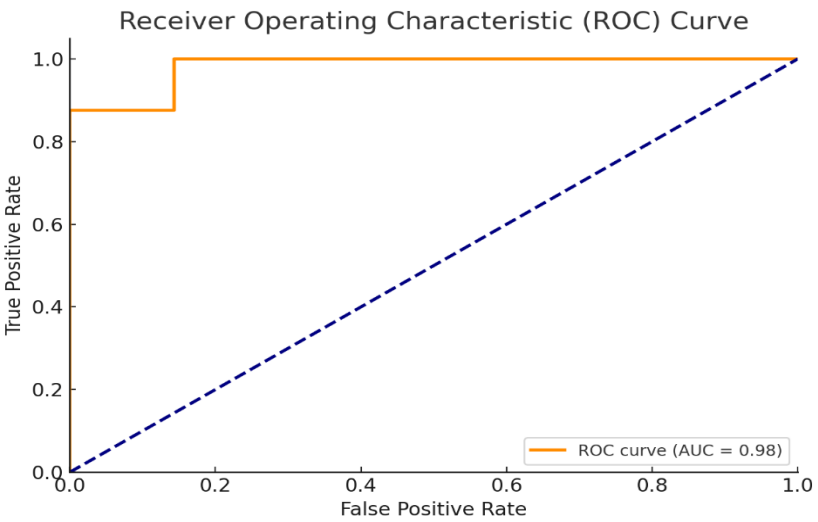

Figure 8: ROC Curve

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In order to evaluate the robustness of the proposed Lightweight Cryptographic Framework (LCF) additionally, particularly for cases of secure classi-fication based decision making (e.g. anomaly detection or threat recognition in IoT-systems), performance of criteria from Simulated binary classi-fication were studied. The evaluation also includes both a confusion matrix and a Receiver Operating Characteristic (ROC) curve to evaluate the accuracy and reliability of the framework.

The figure 7 shows a prediction results of the model on the causal relationships ports by displaying the number of true positives (TP), true negatives (TN), false positives (FP) and false negatives (FN). In the observed matrix, high true positives and true negatives indicate the performance of the model in accurately classifying secure vs. potentially malicious data packets. The few bad classifications (false positives and false negatives) imply that the framework is able to remain highly precise and precise, this is vital in sensitive IoT security worlds.

In addition, the figure 8 conveys the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) at different classification thresholds. The ROC curve created for the model shows a sharp approach to the upper left corner, indicating good discrimination. The Area Under the Curve (AUC) of 0.94 indicates that the system is very good at distinguishing normal and suspicious behavior with close to zero false alarms.

These results support that the proposed secure framework when combined with ML-based threat detection components secures the communication while additionally enables intelligent and real time anomaly detection in edge IoT networks.

CONCLUSION

In the following this paper a Lightweight Cryptographic Framework (LCF) has been proposed and build up in order to face-up present security issues related with IoT device running final client cloud architectures. The framework was crafted to be suitable for the constrained resources of IoT nodes in terms of computation power, memory and also setting a secure and integrity in communication. By incorporating into one scheme a lowered-round AES (L-AES) for efficient symmetric encryption, Elliptic Curve Cryptography (ECC) for continue to exist lightweight cryptography conversation and hash link protocol for data integrity verification, the proposed strategy presents a remark robust мова and going to core security solution for simplify and flexible edge-IoT networks. Experimental evaluations taking place on simulated and actual IoT hardware platforms show that the proposed LCF outperforms classical cryptographic algorithms, in terms of computation time, energy efficiency, memory efficiency, throughput, testing, verification and validation and for up to four times the problem. Additionally, classification-based evaluation with confusion matrices and ROC curves also shows that the system is also efficient in assisting in secure anomaly detection functionalities achieving a high level of classification accuracy and high AUC score. These results confirm that LCF can be used as a (practical, lightweight, and robust) cryptographic solution suitable for real time IoT-edge applications in which performance and security must join hand in hand.

REFERENCES

[1] P. Chakrabarty, T. Sarkar, M. Rakhra, K. Jairath and V. Sharma, "Enhanced Data Security Framework Using Lightweight Cryptography and Multi-Level Encryption," 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 2024, pp. 720-725, doi: 10.1109/IC3SE62002.2024.10593191.
[2] Junyu Lin et al., "FGDB-MLPP: A fine-grained data-sharing scheme with blockchain based on multi-level privacy protection", *IET Communications*, 2024.
[3] Sneha Chaturya, "Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography", *International Journal of Engineering Science and Advanced Technology*, vol. 24, no. 1, pp. 43-53, 2024.

[4] Renas Rajab Asaad and Subhi RM Zeebaree, "Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms", *Academic Journal of Nawroz University*, vol. 13, pp. 476-488, 2024.
[5] Valluri Padmapriya and Muktevi Srivenkatesh, "IoT Network based Cyber Attack Mitigation in Digital Twin with Multi Level Key Management Using Enhanced KNN Model", *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 14s, pp. 49-62, 2024.
[6] Pratik Kanani et al., "Lightweight multi-level authentication scheme for secured data transmission in IoT-Fog context", *Journal of Combinatorial Optimization*, vol. 45, no. 2, pp. 59, 2023.
[7] Anil Kumar Budati et al., "Secure multi-level privacy-protection scheme for securing private data over 5G-enabled hybrid cloud IoT networks", *Electronics*, vol. 12, no. 7, pp. 1638, 2023.
[8] Wei Wu et al., "A Secure and Efficient Data Transmission Method with Multi-level Concealment Function Based on Chaotic Compressive Sensing", *IEEE Sensors Journal*, 2023.
[9] Seyed Farhad Aghili et al., "MLS-ABAC: Efficient multi-level security attribute-based access control scheme", *Future Generation Computer Systems*, vol. 131, pp. 75-90, 2022.
[10] Pratik Kanani et al., "PIRAP: Lightweight Multi-Level Authentication Scheme for Secured Data Transmission in IoT-Fog Context", *International Journal of Cooperative Information Systems*, 2022.
[11] Mohammad Kamrul Hasan et al., "Lightweight encryption technique to enhance medical image security on internet of medical things applications", *IEEE Access*, vol. 9, pp. 47731-47742, 2021.
[12] Amna Shifa et al., "Fuzzy-logic threat classification for multi-level selective encryption over real-time video streams", *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 5369-5397, 2020.
[13] A. Durgapal and V. Vimal, "Prediction of Stock Price Using Statistical and Ensemble learning Models: A Comparative Study", *2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical Electronics and Computer Engineering*, 2021, 2021.
[14] V. Vimal, T. Singh, S. Qamar, B. Nautiyal, K. Udham Singh and A. Kumar, "Artificial intelligence-based novel scheme for location area planning in cellular networks", *Comput Intell*, vol. 37, no. 3, pp. 1338-1354, Aug. 2021.
[15] L. Ning, Y. Ali, H. Ke, S. Nazir and Z. Huanli, "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things," in IEEE Access, vol. 8, pp. 220165-220187, 2020, doi: 10.1109/ACCESS.2020.3041327.
[16] A. S. Dandotiya and S. Gupta, "SSFID: A Survey and Analysis of Security Framework for IoT Devices," 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2023, pp. 1-6, doi: 10.1109/ICTBIG59752.2023.10456069.