Lightweight Hybrid Encryption Framework (LHEF) for Secure and Efficient Data Protection in Cloud and IoT Environments

Sneha Hari Kanthale*,Sagar Vyavahare**

Department of Computer Science

CKT ACS College, New Panvel (Empowered Autonomous), Mumbai University

Email: snehakanthale66@gmail.com

Email: gns.sagar@gmail.com

----------**********----------

Abstract

Cloud computing and Internet of Things (IoT) environments generate massive volumes of data that require secure and efficient protection mechanisms. Traditional encryption techniques either provide strong security with high computational cost or high efficiency with lower security guarantees. This study proposes a Lightweight Hybrid Encryption Framework (LHEF) that combines Elliptic Curve Cryptography (ECC) for secure key exchange and ChaCha20 for fast data encryption. A simulation-based approach is used to evaluate performance using multiple parameters such as encryption time, decryption time, and key generation time. Data processing and analysis were conducted using structured simulation logs and visualization tools. The results indicate that LHEF achieves a balanced trade-off between security and performance compared to RSA and standalone symmetric encryption. The study highlights the effectiveness of hybrid encryption in modern cloud and IoT environment.

Keywords - Hybrid Encryption, IoT Security, Cloud Security, ECC, ChaCha20, RSA, Data Protection.

----------**********----------

I. INTRODUCTION

The rapid expansion of cloud computing and Internet of Things (IoT) technologies has significantly transformed modern digital systems by enabling continuous data exchange across distributed environments. IoT devices such as sensors, smart devices, and embedded systems generate large volumes of data that are transmitted to cloud platforms for storage and processing. However, this increased connectivity also introduces serious security challenges, including data breaches, unauthorized access, and cyber threats.

Traditional encryption techniques have been widely used to ensure data confidentiality and integrity. Public-key cryptography, particularly RSA, provides strong security but requires large key sizes and high computational power, making it unsuitable for resourceconstrained IoT devices [1]. On the other hand, symmetric encryption algorithms such as ChaCha20 provide high-speed encryption with low computational overhead, making them efficient for realtime data processing. However, symmetric encryption faces challenges in secure key distribution [2]. Elliptic Curve Cryptography (ECC) has emerged as a lightweight alternative, offering strong security with smaller key sizes, making it suitable for IoT environments [5], [6]. However, ECC alone may not be efficient for encrypting large datasets due to computational overhead.

To address these challenges, hybrid encryption techniques combine asymmetric and symmetric encryption methods. These approaches use asymmetric cryptography for secure key exchange and symmetric cryptography for efficient data encryption. Although hybrid encryption improves performance and security, many existing solutions lack proper evaluation frameworks and comparative analysis tools [7], [8].

This study proposes a Lightweight Hybrid Encryption Framework (LHEF) that integrates ECC and ChaCha20 to achieve both security and efficiency. A simulation-based system is developed to evaluate performance across different platforms. The study provides a comparative analysis of LHEF with traditional encryption methods and demonstrates its effectiveness in cloud and IoT environments.

Research Gap

Existing research primarily focuses on individual encryption techniques without integrating both security and efficiency. Additionally, limited studies provide simulation-based performance evaluation and visualization of hybrid encryption frameworks. This study addresses these gaps by proposing a hybrid model and analyzing its performance using structured simulation data.

Research Objectives

- To design a lightweight hybrid encryption framework.
- To evaluate performance using simulation techniques.
- To compare LHEF with RSA and ChaCha20.
- To analyze encryption efficiency in IoT and cloud environments.

II. MATERIALS AND METHODS

A. Research Design

This study adopts a simulation-based experimental design to evaluate the performance of different encryption techniques. The analysis focuses on:

- Encryption time
- Decryption time
- Key generation time
- Integrity verification time

B. Data Sources and Sampling

The study uses a dataset generated through simulation logs consisting of multiple encryption operations across different platforms. The dataset includes:

- LHEF (ECC + ChaCha20)
- RSA-2048
- ChaCha20

Dataset Attributes

Encryption method

File size

Encryption time

Decryption time

Key generation time

Platform type

Timestamp

Simulation scenarios were designed to ensure balanced comparison across different encryption techniques.

C. DATA COLLECTION AND WORKFLOW

Research Workflow:

Input Data

↓

Encryption Simulation

↓

Performance Measurement

↓

Data Storage

↓

Analysis

↓

Visualization

↓

Result Interpretation

D. DATA ANALYSIS TECHNIQUES

Descriptive Analysis: Measurement of average execution time

Comparative Analysis: Performance comparison across methods

Efficiency Evaluation: Trade-off between security and speed

Visualization: Graph-based performance analysis

III. Results and Discussion

A. Encryption Time Analysis

The analysis shows that RSA has the highest encryption time due to complex computations. ChaCha20 demonstrates the lowest encryption time, while LHEF provides moderate performance with improved security.

B. Decryption Time Analysis

Similar trends are observed in decryption time, where RSA is the slowest and ChaCha20 is the fastest. LHEF maintains a balance between performance and security.

C. Key Generation Analysis

RSA requires significant time for key generation, whereas ECC-based key generation in LHEF is faster and more efficient.

D. Discussion

The results highlight that LHEF effectively balances security and performance. While RSA provides strong security, it is inefficient for IoT devices. ChaCha20 is efficient but lacks secure key exchange. LHEF overcomes these limitations by combining both

techniques, making it suitable for modern distributed systems.

Limitations of the Study

- Simulation-based results may differ from real-world implementation
- Network latency not considered
- Limited platform diversity
- Hardware constraints not included

IV. CONCLUSION AND RECOMMENDATIONS

This study presents a Lightweight Hybrid Encryption Framework (LHEF) that combines ECC and ChaCha20 to achieve secure and efficient data protection. The results demonstrate that LHEF provides better performance than RSA while maintaining higher security than standalone symmetric encryption.

RECOMMENDATIONS

- Implement LHEF in real-world IoT systems
- Integrate cloud-based encryption services
- Extend analysis to large-scale datasets
- Apply machine learning for adaptive encryption
- Conduct real-time performance evaluation

V.REFERENCES

[1] P. Chapkovski et al., "Public-key cryptography and performance limitations," 2024.

[2] D. J. Bernstein, "ChaCha20 stream cipher," 2008.

[3] W. Stallings, *Cryptography and Network Security*, 2017.

[4] NIST, "Digital Signature Standard," 2013.

[5] N. Koblitz, "Elliptic Curve Cryptography," 1987.

[6] V. Miller, "Use of ECC in cryptography," 1985.

[7] IEEE, "Cloud security frameworks,"

201
5