E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 17-10-2023
Accepted: 29-11-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 2; Issue 1; 2024; Page No. 562-567

Optimization of Cryptographic Algorithms through Deep Learning for Cyber Defense

[1]Soumya Paul and [2]Dr. Priya Vij

[1]Research Scholar, Department of Computer Science & Engineering, Kalinga University, Naya Raipur, Chhattisgarh, India
[2]Assistant Professor, Department of Computer Science & Engineering, Kalinga University, Naya Raipur, Chhattisgarh, India

Corresponding Author: Soumya Paul

Abstract

In an era marked by increasing cyber threats and data breaches, the efficiency and robustness of cryptographic algorithms have become paramount to ensuring digital security. Traditional cryptographic methods, while secure, often suffer from computational inefficiencies and are vulnerable to emerging attack vectors, especially in resource-constrained environments such as IoT and mobile networks. This study aims to explore and optimize cryptographic algorithms using deep learning techniques to enhance both security and performance in cyber defense applications.

The primary objective is to leverage artificial neural networks (ANNs) to analyze and improve the efficiency, adaptability, and resilience of popular cryptographic algorithms such as AES, RSA, and ECC. A deep learning framework is proposed to identify patterns in encryption-decryption processes and optimize key generation, encryption time, and resistance to attacks. The methodology involves training neural networks on large datasets of encrypted traffic and assessing performance using key metrics including execution time, accuracy, and entropy. Experimental results demonstrate that integrating deep learning models with conventional cryptographic schemes can significantly reduce computational overhead while maintaining or improving security standards. The findings suggest a promising direction for the development of intelligent, adaptive, and sustainable cryptographic systems suited for real-time cyber security applications. This research contributes to the growing field of AI-based cyber security by offering a novel, optimization-focused approach to modern cryptography.

Keywords: Cryptography, Deep Learning, Cyber security, Artificial Neural Networks (ANN), Algorithm Optimization, Encryption, Cyber Defense, Machine Learning, Secure Communication, Lightweight Cryptography, AES, RSA, ECC, Data Security, Threat Detection

1. Introduction

1.1 Background of Cybersecurity and Cryptography

In the digital age, cybersecurity has become a critical concern for individuals, organizations, and governments. As cyber threats continue to evolve in complexity and frequency, securing digital communications and data assets is more important than ever. Cryptography serves as a foundational element in cybersecurity, enabling secure transmission, authentication, and storage of sensitive information across networks. Algorithms such as AES, RSA, and ECC are widely used to safeguard systems against unauthorized access and data manipulation.

1.2 Importance of Optimization in Cryptographic Systems

While cryptographic algorithms are designed for security, they often require significant computational resources. This poses a challenge in environments such as IoT, mobile platforms, and embedded systems, where processing power and energy availability are limited. Optimization of cryptographic operations is therefore essential to improve speed, reduce power consumption, and enable real-time data protection without compromising security standards.

1.3 Rise of Deep Learning in Cyber Defense

Artificial intelligence, especially deep learning, has revolutionized various fields by providing intelligent systems that can learn, adapt, and make decisions. In cybersecurity, deep learning techniques such as Artificial Neural Networks (ANNs) have shown significant promise in identifying patterns, detecting anomalies, and predicting threats. These capabilities open up new possibilities for optimizing cryptographic algorithms, improving both efficiency and resilience against modern cyber-attacks.

1.4 Research Objectives and Scope

This research aims to investigate the application of deep learning, particularly ANN models, to optimize traditional cryptographic algorithms used in cyber defense. The primary objectives include:

- Enhancing the efficiency of cryptographic operations (e.g., encryption/decryption time).
- Reducing computational overhead in secure communications.
- Evaluating the robustness and adaptability of ANN-based optimization approaches.

2. Literature Review

2.1 Traditional Cryptographic Techniques and Their Limitations

Cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) have long been the standard for ensuring data confidentiality, integrity, and authentication. These algorithms are widely used due to their mathematical robustness and proven security properties. However, traditional cryptographic techniques face several limitations, particularly in terms of computational complexity and performance under constrained environments. For instance, RSA requires large key sizes to maintain security, which increases processing time and power consumption. Similarly, AES, although efficient in symmetric encryption, still requires significant computational effort during key generation and decryption in real-time systems. These limitations become more critical in mobile devices, IoT systems, and real-time cloud applications.

2.2 Optimization Needs in Cybersecurity Frameworks

With the increasing demand for secure yet fast and lightweight encryption, the need to optimize cryptographic algorithms has become a central concern in cybersecurity frameworks. Optimization aims to reduce latency, computational cost, and energy consumption while preserving or enhancing the security level. In real-world scenarios-such as smart grids, healthcare systems, or autonomous vehicles-encryption must be both robust and efficient. Research in this area has explored methods like hardware acceleration, parallel processing, and algorithmic simplification, yet many of these solutions lack adaptability and scalability. Therefore, an intelligent, data-driven approach to optimization is required.

2.3 Applications of Deep Learning in Security Domains

Deep learning has emerged as a powerful tool in cybersecurity applications due to its ability to model complex patterns and detect anomalies in high-dimensional data. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep Belief Networks (DBNs) have been successfully applied in intrusion detection systems, malware classification, and behavioral biometrics. In the context of cryptography, deep learning has shown potential in cryptanalysis-identifying weaknesses in encryption schemes-as well as in enhancing algorithmic efficiency by learning optimal parameters and structures. Researchers have also explored the use of Artificial Neural Networks (ANNs) for dynamic key generation, prediction of cryptographic behavior, and classification of encrypted vs. non-encrypted traffic.

2.4 Comparative Studies on Cryptographic Performance

Numerous studies have benchmarked traditional cryptographic algorithms based on various performance indicators such as execution time, memory usage, throughput, and entropy. Comparative analyses often highlight trade-offs between security level and efficiency. For instance, ECC offers similar security to RSA with smaller key sizes, making it more efficient for mobile devices. However, it is still limited when deployed in real-time high-traffic environments. While some works have suggested lightweight cryptographic algorithms, these often compromise security to gain speed. Emerging research combining cryptographic techniques with AI-based optimization, particularly using deep learning, suggests promising results in achieving both security and performance.

2.5 Identified Research Gaps

Despite considerable progress in both cryptography and machine learning, several gaps remain in the integration of deep learning for optimizing encryption algorithms. Most existing studies either focus on cryptanalysis or security monitoring, rather than enhancing the cryptographic processes themselves. Moreover, limited research addresses how neural networks can be trained to learn efficient encryption/decryption processes or assist in dynamic key management. There is also a lack of comprehensive frameworks that evaluate the real-time performance of such integrated models under varied cyber-attack scenarios. These gaps present opportunities for exploring deep learning-based optimization models that can offer adaptive, sustainable, and high-performance cryptographic solutions.

3. Research Methodology

3.1 Research Design

This study adopts an experimental and analytical research design to evaluate the potential of deep learning models in optimizing cryptographic algorithms for cyber defense. The methodology involves the development of a simulation environment, integration of selected cryptographic schemes, training of deep learning models, and subsequent performance evaluation. The aim is to assess how neural networks can improve the efficiency, adaptability, and security of cryptographic operations across varying workloads and network conditions.

3.2 Selected Cryptographic Algorithms

Three widely used cryptographic algorithms were selected for optimization and analysis:

- **Advanced Encryption Standard (AES):** A symmetric block cipher known for its speed and reliability.
- **Rivest–Shamir–Adleman (RSA):** An asymmetric algorithm widely used for secure data transmission but known for its computational overhead.
- **Elliptic Curve Cryptography (ECC):** Offers equivalent security with smaller keys compared to RSA, making it efficient for resource-constrained systems.

These algorithms were chosen to represent a balanced mix of symmetric and asymmetric cryptographic systems with varying computational complexities.

3.3 Deep Learning Models Used

The following deep learning architectures were employed to learn and optimize cryptographic patterns:

- **Convolutional Neural Networks (CNN):** Utilized for recognizing patterns in encrypted traffic and feature extraction.
- **Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM):** Used to model sequential dependencies in cryptographic operations such as key generation and encryption flow.
- **Deep Neural Networks (DNN):** Applied to classify, predict, and adjust encryption parameters dynamically for performance enhancement.

The models were trained to identify optimization opportunities such as reducing encryption/decryption time and improving key management efficiency.

3.4 Data Sources

The study employed both simulated and real-world datasets:

- Simulated datasets were generated using encryption scripts in Python for various file sizes and formats to create diverse workloads.
- Real network data included packet traces from public datasets such as CICIDS 2017 and UNSW-NB15, providing encrypted traffic patterns and cyber-attack scenarios for training and testing.

3.5 Tools and Technologies

The implementation and experimentation used the following tools:

- **Python:** Programming language used for algorithm implementation and data preprocessing.
- **Tensor Flow and Keras:** Frameworks for building and training deep learning models.
- **Wireshark and NS3:** For network traffic simulation, packet capture, and analysis.
- **Open SSL:** For encryption/decryption performance testing using real cryptographic protocols.
- **Jupyter Notebook & Pandas:** For interactive development and data analysis.

3.6 Evaluation Metrics

The performance of the deep learning-optimized cryptographic algorithms was evaluated based on the following metrics:

- **Execution Time (MS):** Time taken for encryption and decryption processes.
- **Energy Efficiency (mWh):** Estimated power consumption during cryptographic operations.
- **Accuracy (%):** Classification accuracy of the deep learning models in detecting optimal parameters.
- **Entropy:** Measure of randomness in the encrypted output to ensure strong security.
- **Throughput (Mbps):** Volume of data processed per second.
- **CPU and Memory Utilization (%):** System resources consumed during execution.

4. System Design and Implementation

4.1 Architecture of the Proposed Optimization Model

The proposed system is designed to integrate deep learning into the cryptographic workflow to optimize performance and security parameters. The architecture consists of the following layers:

1. **Data Input Layer:** Accepts plaintext data or network traffic samples for encryption.
2. **Cryptographic Layer:** Applies conventional cryptographic algorithms (AES, RSA, ECC).
3. **Monitoring Layer:** Captures metrics (execution time, CPU usage, entropy, etc.) from cryptographic operations.
4. **Deep Learning Optimizer:** A trained ANN model analyzes collected metrics and recommends adjustments (e.g., block size, key size, operation sequence).
5. **Feedback Loop:** Optimized parameters are applied dynamically for the next encryption cycle.

4.2 Integration of Deep Learning with Cryptographic Systems

The integration is achieved by embedding a neural network model between the encryption layers and the system monitoring tool. Here's how it functions:

- During runtime, system metrics are fed into the ANN model.
- The model evaluates the performance and suggests optimal parameters such as key length, cipher mode, or algorithm type.
- These suggestions are automatically implemented using API-level integration with OpenSSL or custom cryptographic scripts.

This approach allows the system to adapt encryption parameters in real-time, ensuring an optimal balance between speed, resource usage, and security strength.

4.3 Training and Testing Phases

- **Training Phase**
  - Dataset: Combined simulated and real-world traffic encrypted using various algorithms.
  - Features: Key size, data size, entropy, CPU usage, encryption time.
  - Output: Optimal configuration recommendation (e.g., select AES with 128-bit key and CBC mode for files <1MB).
  - Toolchain: TensorFlow/Keras with a fully connected DNN, trained for 100 epochs.
- **Testing Phase**
  - Real-time encrypted traffic from NS3 simulations and CICIDS dataset.
  - Evaluation includes comparisons between standard and ANN-optimized cryptographic setups.

Table 1: Sample Input Features for ANN Model

Feature	Data Type	Description
Data Size (KB)	Numerical	Size of input file or packet
Key Length (bits)	Categorical	128, 192, 256 for AES, 1024–4096 for RSA
Algorithm Type	Categorical	AES, RSA, ECC
Execution Time (ms)	Numerical	Time taken for encryption/decryption
Entropy Score	Numerical	Randomness of ciphertext
CPU Usage (%)	Numerical	System resources used during encryption

4.4 Security and Performance Parameters

The optimized cryptographic system was evaluated using the following metrics:

Table 2: Performance Comparison (AES Example)

Metric	Traditional AES	ANN-Optimized AES	Improvement (%)
Execution Time (ms)	18.5	12.2	34.05%
Entropy Score	7.92	7.95	+0.38%
CPU Usage (%)	47	33	29.79%
Energy Consumption (mWh)	14.5	9.7	33.10%

These results demonstrate significant improvements in execution efficiency and resource usage, with negligible trade-offs in encryption strength (entropy). The ANN-based approach dynamically adapts to various file sizes and threat scenarios, maintaining high levels of security while optimizing system performance.

5. Results and Discussion

5.1 Performance Comparison: Optimized vs. Traditional Methods:

The proposed ANN-based optimization framework was tested against traditional cryptographic implementations (AES, RSA, ECC) across various datasets and environments. The results demonstrate that the optimized models significantly outperformed the baseline versions in terms of execution speed, CPU usage, and energy efficiency.

Table 3: Overall Performance Comparison

Algorithm	Method	Avg. Execution Time (ms)	CPU Usage (%)	Entropy Score	Energy Use (mWh)
AES	Traditional	18.5	47	7.92	14.5
AES	ANN-Optimized	12.2	33	7.95	9.7
RSA	Traditional	101.6	62	7.88	31.2
RSA	ANN-Optimized	78.4	45	7.90	22.5
ECC	Traditional	34.7	53	7.89	19.3
ECC	ANN-Optimized	25.6	39	7.91	13.4

5.2 Analysis of Computation Time, Accuracy, and Resource Usage

Execution Time: The ANN-optimized system reduced encryption and decryption time by 25–35%, depending on the algorithm and data size.

Accuracy: In classification tasks for selecting optimal configurations, the neural network achieved over 94% accuracy, validating the model's reliability in predicting the best cryptographic settings.

Resource Usage: CPU usage and energy consumption dropped significantly with optimization. This makes the system more suitable for battery-operated or real-time environments.

5.3 Strengths and Limitations of the Proposed System

Strengths

- **Adaptive Optimization:** Automatically adjusts encryption parameters in response to workload or environmental constraints.
- **Resource Efficiency:** Demonstrates substantial reduction in computation time and power usage.
- **Security Retention:** Maintains strong entropy levels, confirming no compromise in encryption quality.
- **Scalability:** Easily extendable to other cryptographic schemes and environments.

Limitations

- **Model Training Time:** Deep learning models require significant initial training time and dataset preparation.
- **Black-Box Nature:** ANN decisions are often difficult to interpret, which may reduce trust in high-security systems.
- **Overhead for Small Tasks:** For very lightweight encryption tasks, ANN-based optimization may add unnecessary computational layers.

5.4 Use Case or Scenario-Based Evaluation

1. IoT Devices

- Scenario: Encrypted communication between smart home devices.
- Results: 30% improvement in execution time and lower energy usage made the ANN-optimized AES highly suitable.

2. Cloud Storage Encryption

- Scenario: Uploading encrypted files to cloud.
- Results: Reduced CPU usage during bulk file encryption helped in load balancing and energy savings.

3. Smart Grid Communication

- Scenario: Real-time data encryption between grid nodes.
- Results: Optimization provided faster encryption cycles, enabling timely secure transmission of control signals.

Table 4: Use Case-Based Observations

Use Case	Algorithm	Optimized Method Benefit
IoT Devices	AES	Low power, fast encryption
Cloud Storage	RSA	Reduced CPU load in multi-user system
Smart Grid	ECC	Low latency for real-time communication

6. Conclusion

6.1 Summary of Findings

This study presented a novel approach to optimizing traditional cryptographic algorithms using deep learning techniques, particularly Artificial Neural Networks (ANNs). Through systematic experimentation with widely used algorithms such as AES, RSA, and ECC, the research demonstrated that ANN-based optimization can significantly reduce execution time, CPU usage, and energy consumption without compromising the cryptographic strength or entropy of the encrypted data.

Key results showed

- Up to 35% improvement in execution speed,
- 25–30% reduction in CPU usage, and
- Enhanced adaptability in real-time and resource-constrained environments like IoT and cloud computing.

6.2 Contributions to the Field

This research contributes to the evolving field of AI-enhanced cybersecurity in several ways:

- Introduced a hybrid framework combining deep learning with cryptographic systems for real-time performance optimization.
- Validated the model across diverse use cases, including IoT networks, cloud storage, and smart grid infrastructures.
- Demonstrated scalability and sustainability, making it suitable for both high-volume and low-power computing environments.
- Advanced the application of ANN models beyond cryptanalysis, positioning them as active agents in cryptographic decision-making and automation.

6.3 Limitations

Despite its promising outcomes, the study is not without limitations:

- High training time and model complexity may be a barrier for real-time learning or frequent retraining in limited-resource environments.
- Black-box nature of neural networks can make interpretability and transparency difficult in sensitive or regulated systems.
- Generalization challenges may arise when applying the trained models to entirely new cryptographic schemes or threat patterns.

Future research should explore explainable AI techniques, transfer learning for cryptographic models, and lightweight neural architectures tailored for embedded and edge devices.

7. Future Scope

7.1 Expansion to Quantum-Resistant Cryptography

As quantum computing advances, traditional cryptographic algorithms like RSA and ECC may become vulnerable to quantum attacks. A logical extension of this research is to apply deep learning techniques to post-quantum cryptographic algorithms such as lattice-based, hash-based, and multivariate cryptography. Integrating ANN-based optimization with quantum-resistant encryption could significantly improve the performance and adaptability of next-generation secure communication systems. Furthermore, deep learning could assist in selecting the most efficient quantum-safe schemes for specific use cases based on real-time requirements.

7.2 Real-Time Deployment in Industrial Settings

While this study demonstrated the feasibility of ANN-based optimization in a simulated environment, the next step involves real-time deployment in industrial applications such as:

- Smart manufacturing systems,
- Cloud service providers,
- Healthcare and financial sectors, and
- Critical infrastructure (e.g., smart grids, transport).

This would require developing lightweight and stable models capable of running on edge devices or within constrained networks without sacrificing performance. Collaboration with industry partners could further help tailor the optimization framework to practical constraints like regulatory compliance, data privacy, and interoperability.

7.3 Enhancement of Deep Learning Architectures

The current research utilized standard ANN, CNN, RNN, and LSTM models. Future work could explore:

- Transformer-based architectures for understanding complex sequential dependencies in encryption routines,
- Reinforcement learning for dynamic adaptation to varying threats or system loads, and
- Explainable AI (XAI) to improve the transparency and trustworthiness of deep learning decisions in cryptographic settings.

Moreover, combining multi-modal learning (e.g., integrating traffic pattern data, device metadata, and cryptographic parameters) may further improve model accuracy and generalization.

References

1. Al-Janabi S, Al-Shourbaji I. A study of cyber security awareness in educational environment in the Middle East. Journal of Information & Knowledge Management. 2016;15(01):1650001. DOI: 10.1142/S0219649216500018.
2. Bhardwaj A, Singh R. Hybrid cryptographic algorithm using AES and RSA for secure data transmission. Procedia Computer Science. 2021;178:381–388. DOI: 10.1016/j.procs.2020.11.027.
3. Goodfellow I, Bengio Y, Courville A. Deep learning. MIT Press; c2016.
4. Hossain MS, Muhammad G, Alamri A. Smart healthcare monitoring: A voice pathology detection paradigm for smart cities. Multimedia Systems. 2019;25(5):565–575. DOI: 10.1007/s00530-018-0597-6.
5. Keshk M, Turnbull B, Alazab M. A novel hybrid deep learning model for detecting malicious URLs. Electronics. 2021;10(21):2625. DOI: 10.3390/electronics10212625.
6. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy. 2017;41(10):1027–1038. DOI: 10.1016/j.telpol.2017.09.003.
7. Li Y, Xu X, Zhao S. Cryptographic applications of neural networks: A comprehensive survey. IEEE Access. 2019;7:170774–170795. DOI: 10.1109/ACCESS.2019.2955506.
8. Liu H, Lang B, Liu M, Yan H. CNN and RNN based payload classification methods for attack detection. Knowledge-Based Systems. 2020;163:332–341. DOI: 10.1016/j.knosys.2018.09.023.
9. Rizvi STH, Zulkernine M. A lightweight encryption scheme for smart devices. Future Generation Computer

Systems. 2018;84:211–221. DOI: 10.1016/j.future.2018.02.047.
10. Shokri R, Shmatikov V. Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015:1310–1321. DOI: 10.1145/2810103.2813687.
11. Stallings W. Cryptography and network security: Principles and practice (7th ed.). Pearson; c2017.
12. Sarker IH. Machine learning: Algorithms, real-world applications and research directions. SN Computer Science. 2021;2:160. DOI: 10.1007/s42979-021-00592-x.
13. Yadav S, Rao UP. An efficient deep learning-based classification model for cyber threat detection. Computer Networks. 2020;173:107221. DOI: 10.1016/j.comnet.2020.107221.