Online at: https://researchtrendsjournal.com
ISSN No: 2584-282X
Indexed Journal
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 2; Issue 5; 2024; Page No. 132-137

Received: 08-07-2024
Accepted: 18-08-2024

A comparative study of traditional and ANN-Based Cryptographic Systems in IoT Security

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

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

Corresponding Author: Soumya Paul

Abstract

The exponential growth of the Internet of Things (IoT) has revolutionized connectivity across various domains but has also introduced significant security vulnerabilities due to the constrained nature of IoT devices. Traditional cryptographic techniques, though robust in standard computing environments, often fall short in resource-limited IoT settings due to their high computational demands. To address this challenge, the present study conducts a comparative analysis between conventional cryptographic methods (e.g., AES, RSA, ECC) and Artificial Neural Network (ANN)-based cryptographic systems in the context of IoT security.

The study aims to evaluate the effectiveness, efficiency, and adaptability of ANN-integrated cryptographic models compared to traditional algorithms under different IoT use-case scenarios. Using a simulation-based approach, various IoT environments such as smart homes and healthcare monitoring systems were emulated. Deep learning models, including feed forward and recurrent neural networks, were trained to optimize or support encryption tasks. Tools like Tensor Flow, NS3, and Python were used to implement and evaluate the cryptographic frameworks.

The results indicate that ANN-based systems exhibit enhanced adaptability, lower latency, and improved energy efficiency, particularly in real-time and low-power scenarios, without significantly compromising security. This study contributes to the evolving field of secure AI-driven IoT systems by offering empirical evidence on the potential of deep learning models to complement or enhance existing cryptographic protocols.

Keywords: IoT Security, Cryptography, Artificial Neural Networks (ANN), AES, RSA, ECC, Deep Learning, Lightweight Encryption, Cybersecurity, Smart Devices, Secure Communication, Resource-Constrained Systems, Real-Time Encryption, Machine Learning in Security, Cryptographic Optimization

Introduction

Background of IoT and Cybersecurity

The Internet of Things (IoT) has transformed the digital ecosystem by enabling smart connectivity among devices across domains such as healthcare, smart homes, agriculture, and industrial automation. With billions of devices expected to be interconnected, the security of transmitted data has become a growing concern. IoT devices often operate in open and dynamic environments, making them highly susceptible to cyberattacks such as data breaches, man-in-the-middle attacks, and device spoofing. Ensuring end-to-end data confidentiality, integrity, and authentication in such a vast and distributed architecture poses a significant cybersecurity challenge.

Importance of Cryptography in IoT

Cryptography serves as a fundamental building block in securing communication between IoT nodes. Encryption algorithms such as AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography) are widely used to safeguard sensitive information. These algorithms ensure that data is accessible only to authorized users, thereby maintaining trust and reliability in IoT systems. However, the successful deployment of cryptographic protocols in IoT relies heavily on the balance between security strength and computational efficiency.

Limitations of Traditional Cryptographic Systems in IoT Devices

Despite their robustness, traditional cryptographic techniques often demand high processing power, memory, and energy-resources that are severely limited in most IoT devices. The need for lightweight, low-latency, and energy-efficient security solutions is therefore critical. Traditional algorithms may also lack the flexibility to adapt dynamically to evolving attack patterns, leaving systems vulnerable in real-time threat environments.

Emergence of AI, Especially ANNs, in Enhancing Cryptographic Performance

Artificial Intelligence (AI), particularly Artificial Neural Networks (ANNs), has shown considerable promise in optimizing cybersecurity solutions, including cryptography. ANNs are capable of learning complex patterns from data, enabling adaptive and intelligent encryption mechanisms. These models can be integrated to improve key generation, dynamic encryption, anomaly detection, and protocol optimization, making cryptographic systems more resilient and context-aware in constrained IoT environments.

Research Objectives

1. To evaluate the performance and limitations of traditional cryptographic algorithms (e.g., AES, RSA, ECC) in IoT environments with constrained resources.
2. To investigate the use of Artificial Neural Networks (ANNs) in enhancing or optimizing cryptographic operations for secure IoT communication.
3. To compare traditional and ANN-based cryptographic systems based on key performance metrics such as encryption time, energy efficiency, and accuracy.
4. To propose a lightweight and adaptive cryptographic framework integrating ANN techniques for improved IoT security.

Literature Review

Traditional Cryptographic Algorithms Used in IoT (AES, RSA, ECC, etc.)

IoT security has long relied on well-established ciphers such as AES for symmetric encryption, RSA for public-key exchange, and ECC for lightweight public-key operations. Benchmark studies on sensor and edge-class hardware consistently show that RSA's large key sizes incur prohibitive delays, while AES offers good throughput but still draws notable energy when key expansion and multiple rounds are executed on 8- or 16-bit microcontrollers. Comparative experiments on embedded boards and ARM Cortex-M devices confirm that ECC delivers equivalent security to RSA with far smaller keys, yet its scalar-multiplication step remains costly under tight real-time deadlines. Recent surveys have therefore explored alternative "lightweight" ciphers (e.g., PRESENT, ASCON, SIMON/SPECK) that better fit sub-milliwatt budgets but may sacrifice maturity or widespread tool support.

Challenges in IoT Security (Low Power, Limited Computation, Real-Time Requirements)

Typical IoT nodes possess kilobytes of RAM, a few MHz of CPU, and are often battery-powered for months or years. This extreme resource profile clashes with the multi-round, math-intensive nature of classical ciphers, creating latency spikes and rapid energy drain. Constrained devices must also negotiate intermittent connectivity, which amplifies the need for fast hand-shakes and minimal packet overhead. Furthermore, edge deployments require cryptographic agility to respond to evolving threat models, yet firmware updates are infrequent and costly. These combined constraints motivate a shift toward security primitives that are computation- and energy aware by design.

Applications of Artificial Neural Networks in Cryptography

AI researchers have begun leveraging Artificial Neural Networks (ANNs) to improve or complement cryptographic processes. Deep nets have been trained to accelerate key generation heuristics, predict optimal cipher configurations under fluctuating loads, and detect anomalous patterns in encrypted traffic with high precision. In intrusion detection contexts, CNN and LSTM architectures outperform traditional statistical methods at spotting malformed or replayed packets in smart-home traffic. Experimental work has also shown that ANNs can learn substitution–permutation mappings, enabling adaptive lightweight encryption that tunes its round count to available energy.

Previous Comparative Studies and Performance Benchmarks

Several empirical studies compare classical and lightweight algorithms across metrics such as encryption time, power draw, memory footprint, and entropy. Results generally rank ChaCha20, Twofish, and ECC as the most IoT-friendly among traditional options, while PRESENT and ASCON dominate the lightweight class. However, most benchmarks evaluate algorithms in isolation rather than within full protocol stacks, and few include AI-assisted variants, leaving a gap in holistic performance evidence.

Identified Research Gaps

Current literature rarely compares ANN augmented cryptographic systems head-to-head with their conventional counterparts on real IoT hardware. Moreover, most studies stop short of integrating post quantum or hybrid AI–PQC schemes, even though quantum threats are increasingly realistic. There is also limited work on explain ability and trust calibration when neural models make security critical decisions, a vital aspect for regulatory adoption. These gaps underscore the need for a systematic comparative study—such as the one proposed in this paper—covering performance, energy, and security robustness of traditional versus ANN based cryptography across representative IoT scenarios.

Research Methodology

Research Design and Approach

This study adopts an experimental-comparative research design, aiming to evaluate the performance of traditional cryptographic algorithms against ANN-enhanced methods in simulated IoT environments. A quantitative approach is employed, involving both benchmarking and statistical analysis to assess performance indicators such as latency, power efficiency, and encryption quality.

Selected Traditional Cryptographic Algorithms for Comparison

Three widely used cryptographic algorithms are selected for baseline comparison:

- AES (Advanced Encryption Standard) – symmetric block cipher known for its speed and security.
- RSA (Rivest-Shamir-Adleman) – asymmetric algorithm frequently used for key exchange.
- ECC (Elliptic Curve Cryptography) – lightweight alternative to RSA, suitable for IoT.

These were chosen based on their prevalence in IoT systems and their differing computational demands.

ANN-Based Optimization/Enhancement Techniques

Artificial Neural Networks (ANNs) are used to optimize key aspects of cryptographic operations, such as:

- Key generation enhancement using feed forward DNNs.
- Dynamic encryption strength adaptation via LSTM models based on system load.
- Intrusion detection integration using CNN for encrypted traffic analysis.

ANN models are trained on labeled datasets representing normal and anomalous encryption patterns to optimize responsiveness and accuracy.

IoT Simulation Environment Setup (Smart Home, Healthcare, etc.)

Simulated IoT scenarios are developed to reflect realistic use cases:

- **Smart Home Environment:** Includes connected devices like smart locks, lights, and thermostats.
- **Healthcare Monitoring System:** Involves wearable health trackers and real-time patient data transmission.

Network behavior is simulated using NS3 (Network Simulator 3), and system behavior is modeled using pre-defined device profiles and communication patterns.

Data Sources and Feature Selection

- Synthetic traffic data is generated for encryption/decryption simulations using NS3 and Python scripts.
- Public datasets from IoT-related repositories (e.g., UNSW-NB15, CICIDS) are used for ANN training.
- Key features extracted include encryption time, packet size, CPU usage, memory consumption, and entropy.

Tools and Frameworks

The study utilizes the following tools:

- Tensor Flow and Keras – for building and training ANN models.
- Python – for cryptographic scripting and integration.
- Open SSL – for executing traditional encryption schemes.
- NS3 – for simulating network environments.
- Power TOP and Sys Stat – for profiling power and performance metrics.

Evaluation Metrics

The following metrics are used to compare traditional and ANN-based systems:

- Latency (ms) – Time taken for encryption/decryption.
- Power Consumption (mW) – Energy used during cryptographic operations.
- Throughput (kbps) – Amount of data securely transmitted per second.
- Entropy (bits) – Randomness and unpredictability in the ciphertext.
- Success Rate (%) – Accuracy in data delivery and cryptographic success without compromise.

System Architecture and Implementation

IoT Cryptographic Framework (Traditional vs. ANN-Based)

The proposed architecture includes two parallel frameworks for evaluation:

- **Traditional Cryptographic Pathway:** Implements standard algorithms such as AES, RSA, and ECC for encryption/decryption operations, applied directly on IoT data packets.
- **ANN-Based Cryptographic Pathway:** Integrates trained ANN models into the cryptographic pipeline to optimize tasks such as dynamic key selection, adaptive encryption strength, or anomaly detection prior to encryption.

Both frameworks are deployed in identical IoT simulation environments to ensure fair comparison.

Model Training and Testing Phases for ANN

- **Data Collection:** Features such as packet size, transmission delay, device type, and current load are collected from simulated environments.
- **Training Phase:** ANN models (e.g., DNN for key optimization, LSTM for traffic prediction) are trained on pre-labeled datasets using TensorFlow and Keras.
- **Testing Phase:** The trained models are integrated into real-time simulation workflows to evaluate performance under dynamic conditions.

Models are validated using 80/20 train-test split and 5-fold cross-validation to ensure generalizability.

Integration with Encryption Processes

- The trained ANN is linked directly to encryption modules via Python scripts.
- For example, in AES-based systems, the ANN dynamically determines optimal block size and number of rounds based on input entropy and system resource status.
- In RSA, ANN assists in selecting smaller but sufficiently secure key sizes based on prior attack pattern prediction.

Table 1: Integration Roles of ANN in Cryptographic Systems

Function	Traditional Approach	ANN-Enhanced Approach
Key Generation	Fixed-size, static	Adaptive, optimized by ANN
Encryption Configuration	Manual, pre-defined	Dynamic, system-aware (ANN-driven)
Threat Detection	Rule-based IDS	Anomaly detection via CNN or LSTM
Resource Allocation	Uniform across nodes	Context-aware via neural prioritization

Real-Time Simulation Setup and Device Profiles

- **Simulation Platform:** NS3 is used to model the network behavior of connected IoT devices under smart home and healthcare scenarios.
- **Devices Simulated:** Smart thermostats, locks, motion sensors, wearable health monitors, and gateway nodes.
- **Traffic Patterns:** Simulated using periodic sensor readings, alert bursts, and firmware updates.
- **Scenarios:** Each cryptographic configuration (traditional vs. ANN) is tested under normal operation, peak traffic, and simulated attack conditions (e.g., replay, packet sniffing).

Results and Analysis

Performance Metrics: Traditional vs. ANN-Based Systems

The study evaluates both systems based on several key performance indicators:

- Encryption/Decryption Time (ms)
- Power Consumption (mW)
- Encryption Entropy (bits)
- Throughput (kbps)
- Success Rate (%)

Each metric is recorded under identical IoT simulation conditions for both cryptographic frameworks.

Table 2: Average Performance Metrics Comparison

Metric	AES (Traditional)	RSA (Traditional)	ANN-AES	ANN-RSA
Encryption Time (ms)	5.6	10.2	3.4	6.1
Power Consumption (mW)	75	105	52	84
Entropy (bits)	7.1	7.3	7.8	7.9
Throughput (kbps)	325	210	410	300
Success Rate (%)	96.2	94.5	98.1	97.3

Execution Time and Power Efficiency Comparison

- ANN-enhanced cryptographic systems showed up to 35% faster execution times, thanks to optimized key processing and adaptive encryption logic.
- Energy profiling with tools like Power TOP revealed a 25–40% reduction in power consumption in ANN-based systems-crucial for battery-operated IoT devices.

Entropy and Encryption Robustness Analysis

Entropy measures were computed to evaluate the randomness and strength of the cipher text. ANN-based systems produced consistently higher entropy values, suggesting more unpredictable and secure encrypted outputs.

- ANN-enhanced AES achieved ~7.8 bits of entropy per byte, compared to 7.1 for traditional AES.
- These improvements result from dynamic key adaptations and entropy-boosting neural transformations during encryption.

Scalability and Adaptation in Varying IoT Use Cases

The framework was tested across two primary simulation environments:

- **Smart Home Scenario:** High device density but low traffic per node.
- **Healthcare Monitoring:** Fewer nodes but higher data sensitivity and periodic traffic.

Findings

- ANN-based cryptography adapted more efficiently in both settings, with minimal impact on latency during traffic bursts.
- Traditional systems experienced performance drops (~20% slowdown) under load, while ANN-enhanced systems maintained adaptive encryption without bottlenecks.

Discussion

Insights on When ANN-Based Models Outperform Traditional Methods

The results indicate that ANN-based cryptographic systems consistently outperform traditional algorithms in several specific scenarios:

- Dynamic environments where traffic load, device behavior, and energy availability fluctuate (e.g., smart homes, wearable devices).
- Resource-constrained conditions, where ANN models adjust encryption intensity or key lengths based on current device capabilities.
- Adaptive threat response, where ANN models identify patterns of potential cryptographic attacks (e.g., replay, side-channel) and dynamically adjust parameters or initiate alerts.

In contrast, traditional cryptography maintains static encryption logic and lacks contextual adaptability, leading to inefficiencies in modern, decentralized IoT ecosystems.

Trade-offs in Complexity, Interpretability, and Real-Time Performance

While ANN-based systems introduce adaptive intelligence, they also carry certain trade-offs:

- **Model Complexity:** Implementing deep neural networks adds layers of computational logic that may be heavy for ultra-low-power devices.
- **Interpretability:** Unlike deterministic cryptographic algorithms, neural network decisions are not inherently transparent, raising concerns in high-security contexts.
- **Real-Time Constraints**: Although ANN-enhanced encryption is faster in average cases, initial model training and tuning require significant resources, which may delay deployment in latency-sensitive environments.

Therefore, a hybrid approach-using ANN models only for key generation, threat detection, or pre-processing-is recommended for edge deployments.

Security Implications and Threat Resistance

The ANN-enhanced cryptographic systems demonstrated:

- Higher entropy and randomness, making ciphertext more resistant to brute-force and pattern-based attacks.
- Improved detection of anomalies and unusual key patterns, potentially flagging unauthorized access attempts or compromised nodes.
- Dynamic key renewal, reducing the attack surface in long-duration communication sessions.

However, adversarial machine learning remains a threat; model poisoning or evasion attacks could be used to manipulate ANN behavior if not properly secured.

Applicability in Commercial/Industrial IoT Deployments

The findings suggest strong potential for ANN-based cryptographic enhancements in the following domains:

- **Healthcare IoT:** Where patient data requires both high confidentiality and real-time processing.
- **Industrial Automation:** ANN-driven optimization can support secure communication between PLCs, sensors, and SCADA systems with adaptive encryption loads.
- **Smart Grids and Utilities:** Real-time ANN models can balance encryption depth with performance in grid-sensitive operations.
- **Home Automation Devices:** ANN-lite versions can be embedded in hubs or cloud intermediaries to offload cryptographic load from endpoint devices.

Conclusion

Summary of Findings: This study has conducted a detailed comparison between traditional cryptographic algorithms (such as AES and RSA) and Artificial Neural Network (ANN)-enhanced cryptographic techniques in the context of Internet of Things (IoT) environments.

Key observations include

- ANN-based systems achieved better performance in terms of encryption time, power efficiency, and entropy.
- Adaptive behavior of ANNs allowed improved scalability and responsiveness under varying network loads and device constraints.
- In simulation environments (e.g., smart home and healthcare), ANN-augmented encryption consistently maintained stronger security metrics with less computational overhead.

Key Contributions

- A comprehensive benchmarking framework for evaluating cryptographic performance in IoT systems.
- Implementation of a novel ANN-based cryptographic enhancement model, demonstrating clear advantages in dynamic and constrained environments.
- Insights into real-world applicability of AI-driven encryption, particularly in domains requiring lightweight, secure, and scalable security frameworks.

Limitations of the Current Study

- Model complexity may hinder direct implementation on extremely low-power IoT devices without further optimization or hardware acceleration.
- The study used simulated environments, which may not fully reflect real-world unpredictability or network anomalies.
- Only a limited set of cryptographic algorithms and ANN architectures were tested; future work could expand to hybrid encryption models or quantum-resistant algorithms.

Future Scope

Applying Models to Post-Quantum Cryptography for IoT

As quantum computing threatens traditional encryption, future research can focus on integrating ANN-based models with post-quantum cryptographic algorithms (e.g., lattice-based, hash-based methods). This will help assess whether machine learning can optimize key management and improve adaptability in quantum-resistant protocols tailored for IoT ecosystems.

Real-World Deployment in Smart Cities or Edge Computing

A critical next step involves testing ANN-augmented cryptographic models in real-world environments, such as smart cities, connected vehicles, and industrial IoT. Deploying these models in edge computing frameworks can validate their latency handling, energy performance, and scalability under operational workloads.

Lightweight Neural Networks for Ultra-Low Power Devices

To enable practical adoption in microcontroller-based or battery-operated IoT devices, future research should explore designing lightweight ANN architectures (e.g., TinyML, pruning, quantization) that maintain cryptographic performance without overburdening the hardware.

Enhancing Model Interpretability and Transparency

One limitation of ANN-based encryption systems is the black-box nature of decision-making. Future work can explore explainable AI (XAI) approaches to improve model interpretability, making it easier to validate cryptographic behavior and ensure compliance in security-critical applications.

References

1. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson Education; c2017.
2. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017;88:10–28. https://doi.org/10.1016/j.jnca.2017.04.002.
3. Zhang Y, Deng RH, Liu X, Zheng D. Lightweight and privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Internet of Things Journal. 2019;6(2):3756–3766. https://doi.org/10.1109/JIOT.2018.2878058.
4. Sadeghi AR, Wachsmann C, Waidner M. Security and

privacy challenges in industrial Internet of Things. Proceedings of the 52nd Annual Design Automation Conference. 2015:1–6. https://doi.org/10.1145/2744769.2747942.
5. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access. 2020;7:82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045.
6. Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal. 2019;6(4):6822–6834. https://doi.org/10.1109/JIOT.2019.2903874.
7. Kaur R, Kaur M. Efficient encryption algorithm using deep learning for IoT security. Journal of Information Security and Applications. 2021;58:102804. https://doi.org/10.1016/j.jisa.2021.102804.
8. Abomhara M, Køien GM. Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015;4(1):65–88. https://doi.org/10.13052/jcsm2245-1439.411.
9. Farooq MU, Waseem M, Khairi A, Mazhar S. A critical analysis on the security concerns of Internet of Things (IoT). International Journal of Computer Applications. 2015;111(7):1–6. https://doi.org/10.5120/19547-1280.
10. Zeng Y, Ni J, Yang Y. Lightweight machine learning encryption algorithm for secure IoT communications. Future Generation Computer Systems. 2021;118:91–99. https://doi.org/10.1016/j.future.2021.01.021.
11. Mohammadi M, Al-Fuqaha A, Sorour S, Guizani M. Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials. 2018;20(4):2923–2960. https://doi.org/10.1109/COMST.2018.2844341.
12. Lin H, Bergmann NW. IoT privacy and security challenges for smart home environments. Information. 2016;7(3):44. https://doi.org/10.3390/info7030044.
13. Bost R, Popa RA, Tu S, Goldwasser S. Machine learning classification over encrypted data. Network and Distributed System Security Symposium (NDSS). 2015. https://doi.org/10.14722/ndss.2015.23191.
14. Kumar P, Tripathi R, Raw RS. A novel deep learning framework for secure authentication in IoT-based smart home. Journal of Supercomputing. 2022;78:12359–12382. https://doi.org/10.1007/s11227-021-04083-7.
15. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography: NISTIR 8309. U.S. Department of Commerce; c2019. https://doi.org/10.6028/NIST.IR.8309.