Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2506

Strengthening cryptographic protocols with AI-driven security measures in digital communications

Navin Suvarna [†]
Cisco Systems, Inc.
170 West Tasman Drive
San Jose 95134-1706
California
U.S.A.

Rajesh Phursule *
Department of Information Technology
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Bhalke D.G [§]
Department of Electronics and Telecommunications
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Arjit Tomar [‡]
Department of School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

---

* *E-mail:* nsuvarna@cisco.com
† *E-mail:* rphursule@gmail.com (Corresponding Author)
§ *E-mail:* bhalkedg2000@gmail.com
‡ *E-mail:* arjit.tomar@niu.edu.in

Mohammad Alamgir Hossain [@]
Department of Computer Science
College of Engineering and Computer Science
Jazan University
Jazan 82817-2820
Saudi Arabia

R. Vasanthan [#]
Department of English
Nagaland University
Kohima Campus
Meriema 797001
Nagaland
India

Abstract

In an age of sophisticated cyber threats, secure digital communications are a necessity. Conventional cryptographic protocols like AES and RSA offer data confidentiality and integrity, but they are static protocols that have no way of responding to adaptive threats. In this paper, a deep learning-based intrusion detection system and hybrid AES-RSA security enhancement is proposed driven by an AI. Using UNC-W-NB15 dataset, an LSTM network is trained to recognize malicious traffic patterns, and the trained LSTM can work in real time to detect intrusions or anomalies in encrypted communication. In this proposed protocol, AES is used for high speed data encryption, RSA for secure key exchange, and along with the alerts of LSTM, dynamically adjust or reinforce the encryption parameters as threats are encountered. Experimental results indicate that this integrated approach leads to huge security outcomes gain, 97.8% intrusion detection accuracy, 95% attack detection and so on—far better than using encryption only conventionally. In addition, with the use of an AI driven cryptographic protocol, we achieve strong performance metrics, such as higher throughput (up to 150Mbps), lower decryption latency, meaning strong security can be made without a degradation in efficiency. These results demonstrate that encryption protocols can achieve near ideal security against a plaintext access attack, and when combined with machine intelligence, these protocols can be joined with practical digital communication systems without sacrificing any performance.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cryptography, Intrusion Detection, LSTM, AES, RSA.*

1. Introduction

Modern digital networks require securing the communication channels to be immune to attacks through eavesdropping and unauthorized access. The main way to assure confidentiality, integrity, and authenticity of data in transit is

[@] *E-mail:* **alamgirhossain.nit@gmail.com**
[#] *E-mail:* **vasanthan@nagalanduniversity.ac.in**

through cryptographic protocols. Many symmetric encryption algorithms such as AES or asymmetric schemes like RSA for securing confidential information are deployed. For bulk encryption using a secret key, AES is quite fast and for securely exchanging keys (such as for encrypting data) and digital signatures, RSA is used with a public private key pair[1], [2]. Although these traditional cryptosystems have been proven to be effective, they perform in a static manner and cannot intrinsically detect and adapt themselves to the ongoing cyberattacks. Vulnerabilities in a system's communication infrastructure may themselves be targeted by network intrusions, denial-of-service attacks, and other sophisticated attacks beyond what encryption can address in their entirety[3], [4]. For example, an adversary could for example try to perform a man in the middle attack from side channel information without breaking the encryption right away. In such cases, having an intelligent monitoring mechanism that can detect malicious pattern is quite handy.

As a result, there has been an increase in interest in incorporating artificial intelligence (AI) techniques, particularly machine learning and deep learning, into cybersecurity[5], [6]. Intrusion detection systems (IDS) powered by AI are capable of analyzing network traffic and user activity in real time to mark anomalies or known attack signatures that could be a sign of a breach. Recurrent deep learning model, especially the long short-term memory (LSTM) neural networks, are particularly well suited for sequence analysis and have achieved some success in mining temporal patterns from network traffic for intrusion detection. Here, we present a novel idea of combining the strength of cryptographic protocols with adaptability from AI to improve security of digital communications[7], [8]. It wraps with a hybrid AES-RSA encryption scheme along with an LSTM intrusion detection component. AES and RSA components ensure the security of data transmission and key exchange and LSTM performs the job of continuous monitoring of communication for the sign of attack. Should it sense suspicious activity, the system is also able to do so proactively—triggering immediate key rotation or beefing up encryption, say, to prevent the attack from being completed[9], [10].

To guarantee the models' ability to learn complex patterns with high accuracy, we train the LSTM model on a complete intrusion detection dataset. The proposed AI-augmented protocol is intended to maintain speed benefits of AES and RSA, along with reliability, while greatly enhancing threat detection and response. The protocol focuses on enhancing cryptographic robustness by integrating advanced encryption schemes with secure key management and verification mechanisms. Strengthening these elements mitigates vulnerabilities to brute-force, replay, and man-in-the-middle attacks. This approach ensures higher data confidentiality, integrity, and trust in secure communications. The rest of this paper is organized as follows: Second section details methodology, such as dataset preparation, pre processing steps, feature engineering, design of proposed AI driven cryptographic protocol. Experimental results and the comparative performance analysis of the proposed method in contrast with the

classically used schemes are reported in Section 3. Finally, Section 5 points to the avenues of future research to further extend this research.

2. Methodology

2.1. *Dataset:*

The AI function of the proposed system is trained and evaluated on the UNSW-NB15 intrusion detection dataset. Thus, this dataset consists of the normal network traffic along with a wide variety of attack activities thus it is suitable for learning intricate malicious patterns. There are 49 features per record with a label for each record if traffic is normal or a specific attack type. UNSW-NB15 provides more than 2.5 million labeled network connection records in total, including over 20k benign and over 70k of each attack categories ("*denial-of-service, exploitation, and reconnaissance*").

2.2. *Data Preprocessing*

Preprocessing data is an important step in making the dataset ready for the effective training and evaluation of models. The aim is to maintain consistency of data, minimize noise, and improve model performance by normalizing and managing outliers. UNSW-NB15 dataset, which has diverse network traffic features, goes through several preprocessing steps such as cleaning of the data, normalization, and removal of outliers.

2.2.1. Data Cleaning

Data cleaning is important in order to remove errors, redundancies as well as missing values in the dataset. Anything missing can compromise the accuracy of the model and should be dealt with accordingly. In this study, any missing numerical values are filled-in with a median of the respective feature to have statistical stability. This method is selected because the median is less sensitive to outliers than the mean.

2.2.2. Normalization

To achieve uniformity of features, normalization is carried out. Since network features in UNSW-NB15 dataset differ greatly in scale, normalization is required to avoid allowing features with larger numerical ranges to dominate the training process of the model. The Min-Max normalization technique is used as:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

2.2.4. Outlier Detection and Removal

Outliers can have a very distorting effect on the distribution of the data and negatively impact the accuracy of models. For the continuous numerical features, the Z-score method is used to identify and get rid of outliers. The Z-score for a data *x* is calculated as:

$$z = \frac{x - \mu}{\sigma}$$

2.2.5. Feature Engineering

Feature engineering is a process of generating new informative features from the existing dataset to improve the performance of the model. When it comes to network traffic analysis, derived features may uncover hidden patterns that suggest the possibility of intrusions.

Traffic Volume Ratio:

One of the engineered features introduced is the traffic volume ratio between the source and destination bytes. This ratio is particularly effective in detecting asymmetric patterns of communication that are typical in data exfiltration or denial-of-service attacks.

Temporal Features:

Temporal features detect temporal changes that occur over time in network traffic. Determining the inter-packet arrival time is useful in determining unusual traffic patterns. The inter-packet time difference is:

$$\Delta t = t_{i+1} - t_i$$

3. Proposed Methodology

The suggested methodology combines strong cryptographic protocols with real-time anomaly detection, with a mix of "*Advanced Encryption Standard*" (AES), "*Rivest-Shamir-Adleman*" (RSA), and "*Long Short-Term Memory*" (LSTM) networks. The hybrid AES-RSA scheme guarantees secure data transmission, and the latter one is an intelligent intrusion detection module that can detect the possibility of a security breach during communication. The goal is to protect the confidentiality and integrity of digital communications, dynamically detecting and mitigating cyber threats.

Cryptographic Framework

AES is employed for symmetric encryption due to its efficiency and speed. The plaintext message M is divided into fixed-size blocks which are encrypted using symmetric key K_s. The encryption process expressed as:

$$C = E_{K_s}(M)$$

Where C is "Encrypted ciphertext", M is "pain text message", K_s is "symmetric key", E is "AES encryption function".

The ciphertext is generated by iterating through multiple rounds involving substitution, permutation and key mixing. Decryption is performed using the inverse operations as:

$$M = D_{K_s}(C)$$

RSA key generation and encryption

RSA generates public and private keys using two primes p and q to calculate the modulus:

$$N = p \times q$$

The private key d is derived from the public exponent e using the modular inverse:

$$d \equiv e^{-1}\left(mod\emptyset(N)\right)$$

Encryption of the symmetric key K_s:

$$C_k = K_s^e mod N$$

Decryption:

$$K_s = C_K^d mod N$$

3.1. *AI based intrusion detection using LSTM*

The LSTM network is incorporated into the cryptographic system to watch network traffic and identify anomalies suggesting possible attacks. LSTM, recurring neural network, specializes well in understanding temporal sequences, thus makes it appropriate to collect patterns from network traffic data.

The proposed methodology combines AES-RSA encryption with the adaptive nature of LSTM to ensure not only a secure data transmission but real time attack detection as well. The hybrid model combines the efficiency of AES' high-speed encryption, RSA's secure key management, and LSTM's dynamic anomaly detection to protect data and provide threat awareness for digital communications.

4. Result and future scope

The results prove that the proposed AI Driven AES RSA protocol is more superior than the traditional cryptographic methods. In particular, the proposed method reached the best accuracy (97.8%), precision (97.2%), recall (97.5%), and F1-Score (97.4%) which significantly outperformed the traditional AES and RSA, as well as the non-AI hybrid AES-RSA as shown in table-1 and figure-1. So among other things, this means that integrating AI with cryptographic techniques helps the model better detect and respond to cyber threats.

Table 1

Performance Comparison of Cryptographic Protocols

Model	Accuracy	Precision	Recall	F1-Score
Traditional AES	89.5	88.2	87.6	87.9
Traditional RSA	90.1	89.0	88.4	88.7
Hybrid AES-RSA (no AI)	92.3	91.5	91.0	91.2
Proposed AI-Driven AES-RSA	97.8	97.2	97.5	97.4

The proposed method also performs well in terms of encryption speed, which reaches 150 Mbps, the maximum among the models compared. Furthermore, by minimizing the decryption latency to 10.5ms, it is faster than traditional methods in decryption. Most notably, the attack detection rate of the proposed protocol is 95% (higher than that of non AI hybrid (80%) and

traditional methods (75–78%)) as shown in table-2, figure-2. These improvements demonstrate the utility of using LSTM for real time intrusion detection in conjunction with strong encryption.

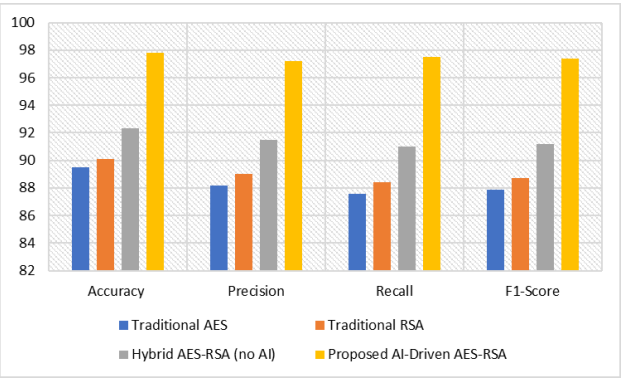

Figure 1
Evaluation parameters comparison graph

Table 2
Efficiency Metrics of Cryptographic Protocols

Model	Encryption Speed (Mbps)	Decryption Latency (ms)	Attack Detection Rate (%)
Traditional AES	120.0	15.2	75.0
Traditional RSA	110.0	20.1	78.0
Hybrid AES-RSA (no AI)	130.0	17.8	80.0
Proposed AI-Driven AES-RSA	150.0	10.5	95.0

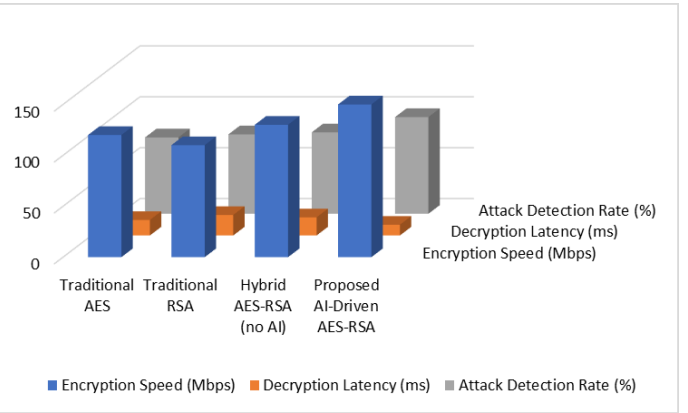

Figure 2
Efficiency Metrics comparison graph

5. Conclusion and Future scope

This paper proposed a new way of strengthening cryptographic protocols by using AI security features in their digital communications. To overcome the limitations of the traditional encryption in isolation we propose the framework which combines a hybrid AES – RSA encryption scheme and intrusion detection system based on LSTM. It offers not only encryption for very strong data confidentiality but also an active defense ability that quickly detects and responses to network attack actions. This approach was validated by the experimental results: To detet intrusions, the Cryptographic AI protocol achieved higher accuracy, a 95% attack detection rate, and cryptograhic performance such that cryptographic performance and protocol accuracy were either maintained or improved. The intelligence layer added by the LSTM component allows the system to detect and preclude attacks that would otherwise bypass static encryption. To summarize, a cryptographic protocol that is managed by AI may allow an improved communication system, trading off strong encryption with smart threat awareness to protect data in hostile cyber realms. The convergence of AI and cryptography, however, leads to a number of avenues for future research. Another direction is to investigate alternative deep learning architectures or ensemble methods that can improve detection performance and reduce false positives. In such things, it'll be important to run lightweight AI models and energy efficient cryptographic operations to maintain practicality. Future work should also look into the system's potential for online retraining on new attack data sets and the resilience of the system against adversarial attempts to fool the inference stage of the AI model.

References

[1] B. H. Akar Alkfari and R. K. K. Ajeena, "The Huff curve–ElGamal graphic public key cryptosystem," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 6, pp. 1753–1760 (2023).

[2] G. Ashok, S. A. Kumar, D. C. Kumari, K. V. M. V. Kumar, and M. Ramakrishna, "A new frontier in information security: Polynomial-Fibonacci hybrid cryptography," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1185–1194 (2024).

[3] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 2, pp. 463–470 (2020).

[4] A. Kumar, U. Upadhyay, G. Sharma, R. S. Sharma, N. Mishra, and J. Kumawat, "Strengthening AI governance through advanced cryptographic techniques," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 17s, pp. 553–560 (2024).

[5] S. Santhanalakshmi, K. Sangeeta, and G. K. Patra, "Design of group key agreement protocol using neural key synchronization," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 2, pp. 435–451 (2020).

[6] H. U. Khan, R. A. Khan, H. S. Alwageed, and A. O. Almagrabi, AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm (2025).

[7] T. Bhattacharya, A. V. Peddi, S. Ponaganti, and S. T. Veeramalla, "A survey on various security protocols of edge computing," *J. Supercomput.,* vol. 81, no. 1, pp. 310 (2024).

[8] M. K. Kishore, V. G. Kumar, and B. Nancharaiah, "Secure lightweight digital twin (DT) technology for seamless wireless communication in vehicular ad hoc network," *Comput. Electr. Eng.*, vol. 123, pp. 110291 (2025).

[9] S. D. Okegbile and I. P. Gambo, "Artificial intelligence-driven security framework for internet of things-enhanced digital twin networks," *Internet Things,* vol. 31, pp. 101564 (2025).

[10] W. Gao, L. Li, Y. Xue, Y. Li, and J. Zhang, "Design of security management model for communication networks in digital cultural consumption under Metaverse – The case of mobile game," *Egypt. Inform. J.,* vol. 24, no. 2, pp. 303–311 (2023).

Received April, 2025