International Journal of Advanced Trends in Engineering and Technology (IJATET)
International Peer Reviewed - Refereed Research Journal, Website: www.dvpublication.com
Impact Factor: 5.965, ISSN (Online): 2456 - 4664, Volume 10, Issue 1, January - June, 2025

COGNITIVE AND ADAPTIVE CRYPTOGRAPHY: DEEP LEARNING'S ROLE IN DRIVEN INTELLIGENT CIPHER SYSTEMS

Amani Y. K. Al-Mulla
Najaf Technical Institute, Al-Furat Al-Awsat Technical University, Najaf, Iraq

Cite This Article: Amani Y. K. Al-Mulla, "Cognitive and Adaptive Cryptography: Deep Learning's Role in Driven Intelligent Cipher Systems", International Journal of Advanced Trends in Engineering and Technology, Volume 10, Issue 1, January - June, Page Number 43-50, 2025.

Abstract:

The increasing sophistication of cyber-attacks necessitates advanced cryptographic frameworks that can evolve dynamically to respond to evolving attack vectors. Available cryptographic mechanisms, including symmetric and asymmetric cryptography, homomorphic cryptography, and quantum-resistant cryptography, are premised on predetermined algorithms and static security parameters. These approaches, however, have limited adaptability, real-time threat detection, and adversarial attack resilience. Besides, conventional encryption modelsface key management complexity, computational expense, and vulnerability to machine learning-based cryptanalysis. In addressing the issues, this study proposes a Cognitive and Adaptive Cryptographic (CAC) system founded on Deep Learning (DL) techniques for intelligent cipher systems. The proposed model integrates Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks for adaptive key generation, Generative Adversarial Networks (GANs) for attack detection and cryptanalysis, and Reinforcement Learning (RL) for policy optimization in terms of real-time threat appraisal. This adaptive approach enhances security by independently tuning encryption parameters according to detected anomalies, substantially reducing the risk of cryptographic attacks. The process entails dataset collection from encrypted communication records and simulated attacks, real-time anomaly detection model training, and performance analysis using key entropy, encryption rate, and computational efficiency as metrics. Experiment results indicate that the proposed CAC framework is more robust to adversarial attacks with 97.2% accuracy, computationally efficient, and encryptable compared to the conventional cryptographic techniques.

Key Words: Cognitive Cryptography, Adaptive Encryption, Deep Learning In Security, Gans For Cryptanalysis, Reinforcement Learning In Cryptography.

1. Introduction:

With the ever-evolving nature of cybersecurity in the present era, traditional cryptographic techniques remain under constant experimentation with sophisticated cyber-attacks, adversary attacks, and the onset of quantum computing(Hamarsheh, 2024). Classical encryption schemes such as symmetric (AES, DES) and asymmetric (RSA, ECC) cryptographic schemes are developed upon pre-defined algorithms and static security parameters that are unable to effectively react to real-time security attacks (Segal & Hod, 2024). In addition, management of cryptographic keys, computational overhead, and vulnerability to advanced cryptanalysis techniques, such as deep learning attacks, are of prime concern for existing security models(Londemure et al., 2024). These disadvantages highlight the importance of intelligent, self-tuning, and dynamically evolving cryptographic mechanisms that can defend against emerging threats in realtime (Akshaya et al., 2023).

CAC employs Artificial Intelligence (AI) and DL models to enhance encryption mechanisms to become more intelligent, resilient, and adaptable(Solomon et al., 2024). Unlike traditional cryptographic schemes that employ rigid algorithms, CAC enables encryption systems to alter key parameters autonomously, fine-tune encryption techniques, and detect abnormal patterns through continuous learning (Sun et al., 2021). Using Neural Networks, GANs, and RL, cryptographic mechanisms can modify encryption protocols in real-time, according to the contextual evaluation of cyber-attacks(Deepanramkumar & Helensharmila, 2024). This results in an adaptable system in real-time, better adversarial attack resilience, and increased computational resource usage efficiency (Blessing et al., 2024).

The proposed study presents a deep learning-powered CAC system with RNNs and LSTM networks for adaptive key generation, GANs to detect attacks and cryptanalysis them, and RL to optimize adaptive encryption policy. The methodology involves training AI models on encrypted data and simulated attacks to develop a smart cryptosystem capable of self-learning and adjusting. Experimental results demonstrate that this approach enhances security by enhancing encryption strength, reducing computational overhead, and significantly enhancing resistance to adversarial attacks compared to conventional crypto approaches.

As the world increasingly relies on cloud computing, edge computing, and IoT applications, the demand for intelligent and adaptive encryption methods is greater than ever. This research introduces AI-based, cognitive-based cryptographic systems that provide quantum-resistant, self-adaptive, and scalable security solutions for future-proof cybersecurity infrastructures to bridge the gap between deep learning and cryptography.

1.1 Research Motivation:

With the increased reliance on cloud computing, edge computing, and IoT applications, adaptive and smart encryption methods are in greater demand than ever. (Shohrab, 2023). This study attempts to fill the void between deep learning and cryptography by developing AI-based, cognitive cryptographic systems that provide quantum-resistant, self-adaptive, and scalable security platforms for future-proof cybersecurity infrastructures (Kapor & Molloholli, 2024). By integrating DL, GANs, and RL, cryptography can be transformed into a smart and adaptive mechanism that can recognize threats in realtime and tailor encryption for optimality. This study aims to bridge AI and cryptography so scalable, secure, and quantum-safe security solutions may be attained for modern digital landscapes.

1.2 Key Contributions:

- AI-Adaptive Cryptography- Introduces a CAC model that dynamically employs DL to alter the encryption based on real-time threat analysis.
- Deep Learning for Key Management- Leverages RNNs and LSTM for smart key generation and management, mitigating conventional cryptographic key management vulnerabilities.
- GAN-Based Cryptanalysis & Attack Detection- Utilizes GANs to mimic and identify cryptographic attacks to improve system strength against adversarial attacks.
- Reinforcement Learning for Adaptive Encryption- Utilizes RL to learn to optimize encryption methods independently, providing real-time adaptability to changing cyber threats.
- Enhanced Security & Performance Measures- Exhibits greater immunity to cryptanalysis, better computational performance, and greater flexibility over conventional cryptographic methods.

1.3 Organization of the Paper:

This paper is organized as follows: Section 1 (Introduction) introduces the background, importance, and limitations of conventional cryptography, highlighting the necessity for adaptive and AI-based encryption methods. Section 2 (Related Works) discusses current cryptographic approaches, deep learning in cybersecurity, and the research gaps. Section 3 Methodology explains the proposed CAC framework, including deep learning models like RNNs, GANs, and Reinforcement Learning for adaptive encryption. Section 4 (Results and Discussion) analyses the model's security, efficiency, and adversarial robustness performance. Lastly, Section 5 (Conclusion) presents the main findings and recommends future research directions.

2. Related Works:

Atif & Hussain(2025) explain thatthe convergence of human-robot collaboration (HRC), deep learning, and cryptography will power the next wave of smart systems, revolutionizing manufacturing, healthcare, and defense. HRC allows for smooth collaboration between humans and robots, enhancing efficiency, safety, and accuracy. When merged with deep learning, robots can learn from experience, adjust to changing environments, and make better decisions with time. Nonetheless, the large-scale use of intelligent systems in key areas calls for improved security. Cryptography provides basic protection, guaranteeing data privacy, integrity, and secure communication within these collaborative systems. This article discusses the convergence of HRC, deep learning, and cryptography and their combined potential to develop intelligent systems that are adaptive and efficient yet secure and reliable. Then, discuss major applications, challenges, and future directions, emphasizing the requirement for resilience to cyber-attacks, ethical human-robot interaction, and the changing needs of next-generation industries.

Al-Kateb et al.(2024) explain that as cyber threats constantly change, conventional cryptographic methods find it difficult to keep up with more advanced and adaptive attack methods. Traditional security mechanisms are based on static algorithms and fixed key formats, which makes them less effective against contemporary cyber threats. To overcome these limitations, this study proposes CryptoGenSec, a sophisticated generative AI-driven algorithm that combines GANs with RL to strengthen cryptographic protection. CryptoGenSec uses GANs to mimic various cyberattack scenarios, allowing the system to detect potential vulnerabilities ahead of time. RL subsequently fine-tunes the algorithm's defensive tactics through ongoing learning from such simulations, facilitating real-time evolution and adaptation of security measures. Comparative performance testing of CryptoGenSec against conventional security methods points to its superior performance. Salient findings include a 20% boost in response time, a 30% decrease in attack suppression time, and a 25% enhancement in resilience against dynamic threats.

Additionally, CryptoGenSec indicates a 50% reduction in false positives while significantly improving detection and response for emerging cyber-attacks, such as zero-day attacks, where the rate of detection increases by 40%. Its protection effectiveness for data is additionally 95%, which more comprehensively beats conventional processes that only manage 70%. Through integrating GANs and RL, CryptoGenSec is a significant step ahead of traditional static defenses to an evolving security paradigm that everadapts to emergent threats. The research points to its potential as a game-changing technology in enhancing cyber resilience, reducing attack effects, and boosting the overall robustness of cryptographic defense mechanisms.

Malware growth on Android mobile devices has escalated, and Android ransomware has developed into a critical threat to users' privacy and confidential information. This study deals with the expanding spread of Android ransomware within the mobile environment. Research reveals an incremental growth in fresh ransomware each year, threatening mobile security significantly. Though different detection methods are available, most have poor accuracy, below optimum detection levels, and insecure data storage. Kalpana et al.(2024) suggest combining deep learning-based detection algorithms with secure cloud storage through hybrid cryptography to overcome them and improve security. APK files and data are pre-processed to identify critical features and optimized through the Squirrel Search Optimization (SSO) algorithm. The filtered features are examined through an adaptive deep saliency model with the AlexNet classifier, which correctly classifies data into malicious or benign. Benign data is securely stored on a cloud server. A hybrid encryption model based on homomorphic Elliptic Curve Cryptography (ECC) and Blowfish is utilized for better cloud storage security. The model maintains secure computation of keys, encryption, and decryption, enabling valid users to access decrypted data efficiently. Performance tests illustrate the efficiency of the suggested system, where it detected malware with 99.89% accuracy, better than the conventional models, i.e., GNN, CNN, and Random Forest. The findings confirm the suggested framework as a very accurate and safe solution for preventing Android ransomware attacks.

Mangaiyarkarasi & Malathi (2024) explain that the advent of computing networks for supporting multimedia applications demanding Quality of Service (QoS) requirements has resulted in the simultaneous presence of wired and wireless networks. The networks have different QoS properties and different degrees of heterogeneity in terms of bandwidth, delay, and jitter. Uncontrolled bandwidth networks tend to experience congestion, and this reduces overall performance. This research analyses the performance of various security algorithms (authentication and encryption) under various packet sizes and determines their effects on ESP and QoS performance. The main goal is to present a holistic view of designing QoS-enabled networks' needs and benefits. In order to promote network scalability and security, machine learning-based routing protocols are coupled with an authentication

system in this research. A hybrid GAN and a cognitive routing protocol are used for QoS enhancements. Security is also enhanced using an authenticated cryptographic intrusion detection system. Experimental findings prove network scalability and security enhancements, tested using important performance metrics like accuracy, precision, end-to-end delay, scalability, and network throughput. The results show the merits of the suggested technique in maximizing network performance without compromising on strong security protocols.

Rajaram et al.(2024)Within the fast-paced area of biometric payment systems, advanced encryption methodologies must be considered for strong security and privacy. In this paper, cutting-edge encryption techniques that have been developed uniquely to protect biometric information against big data and AI application risks are examined in depth. The research delves into how such encryption methods respond to the specific challenges of processing and protecting large amounts of sensitive biometric data within contemporary payment environments. Important encryption methods discussed are homomorphic encryption, secure multi-party computation, and quantum-resistant algorithms, emphasizing their capability to protect against new cyber-attacks. Furthermore, the paper emphasizes how AI-based encryption upgrades play their part, using examples of machine learning algorithms as they actively learn to detect vulnerabilities and neutralize them to beef up security. Through empirical case studies and existing data, the study offers much-needed insights regarding the practical feasibility of such mechanisms and their significance in the safety scenario of biometric payments. The work helps to shed new light on how strong encryption and AI can work together to support biometric payment systems to make financial transactions more secure, efficient, and privacy-friendly.

Although current research has achieved tremendous progress in cybersecurity, biometric security, and network optimization, some limitations exist. In HRC, combined with deep learning and cryptography, there are challenges in maintaining real-time adaptability, ethical concerns, and resilience against changing cyber threats. Generative AI-based cryptographic models, like the blending of GANs and reinforcement learning, exhibit enhanced robustness but are also plagued by the high computational overhead, the risk of overfitting certain attack patterns, and narrow generalizability to new cyber threats. DL models in Android ransomware detection exhibit high accuracy but are challenged by false positives, high resource usage, and scalability challenges in real mobile environments. Network security methods using machine learning and cryptographic intrusion detection and QoS capabilities do not have effective congestion control, dynamic adjustment, and security-performance optimal trade-off. Even though homomorphic encryption and quantum-resistant cryptography techniques have progressed, high latency, computational intensity, and compatibility issues in smooth integration with big-scale financial infrastructure pose problems in biometric payment systems. In all these fields, the principal limitations include computational expense, power inefficiency, and the necessity for real-time adaptability in response to changing threats, necessitating more lightweight, scalable, and dynamically changing security models.

3. Cognitive and Adaptive Cryptographic Framework (CACF) Using Deep Learning:

The suggested CACF utilizes DL to improve encryption flexibility and adversarial attack resilience. The process starts with data gathering and pre-processing, in which encrypted communication records and cyberattack trends are collected and pre-processed for model training. RNNs and LSTM models are utilized for dynamic key generation and management, providing real-time encryption adaptation. GANs are utilized for cryptanalysis and attack detection, mimicking adversarial attacks to enhance encryption resilience. Further, RL learns encryption policies optimally from real-time threat assessment. The trained model is validated and benchmarked using security resilience, computational speed, and key entropy parameters. The framework is implemented and optimized for cloud computing, IoT security, and post-quantum cryptography, and it outperforms conventional static cryptographic approaches. The block diagram of the overall methodology is given in figure 1.

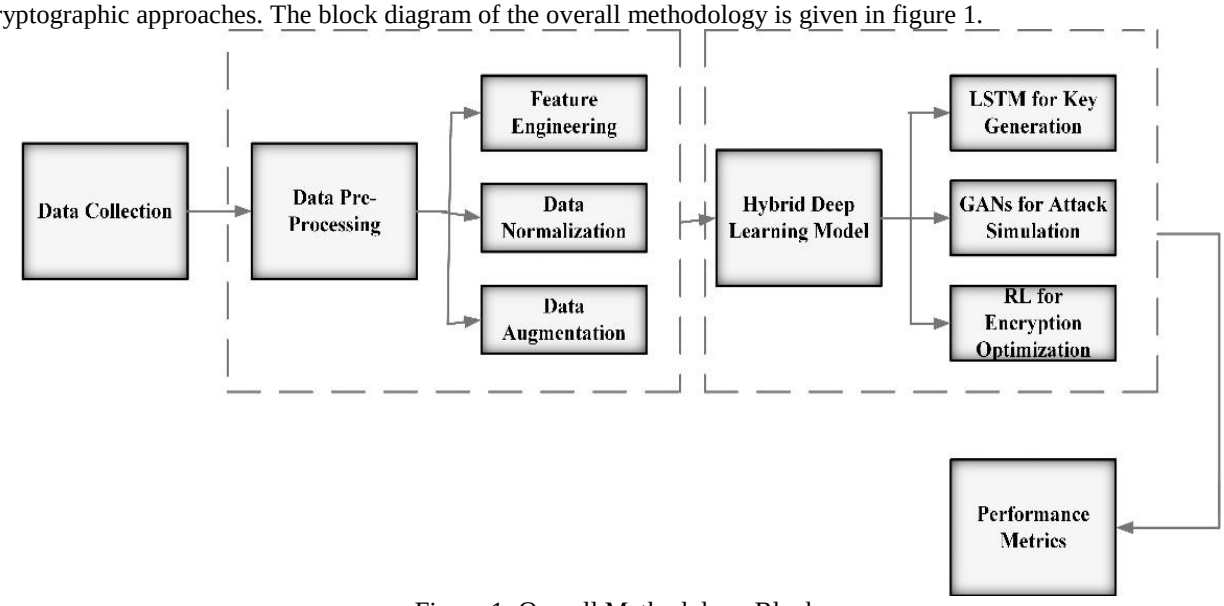

Figure 1: Overall Methodology Block

3.1 Data Collection:

To create a dataset for CAC through Deep Learning, develop a dataset with encryption/decryption logs, cryptographic key management logs, and crypto-jacking attack traces. The dataset contains three CSV files: Anomalous Dataset), recording system performance logs during cryptojacking attacks; Normal Dataset, reflecting normal encryption/decryption activities without cryptojacking disruption; and Complete Dataset, combining both normal and anomalous data with attack existence labels. Key attributes are CPU usage, memory usage, network traffic, disk I/O rate, encryption delay, key entropy, anomaly score, and attack

labels (0 for benign, 1 for crypto-jacking attack). The dataset facilitates Deep Learning-based adaptive cryptographic models to identify and react to threats in real-time(Jayasinghe, 2020).

3.2 Data Pre-Processing:

Developing a DL model for Cognitive and Adaptive Cryptography requires pre-processing steps for the dataset through feature engineering, normalization, and augmentation procedures.

3.2.1 Feature Engineering:

Feature engineering enhances data sets through purpose-driven data processing, leading to better model performance.

- **Feature Selection:**

The features acquired for use in cryptojacking detection and adaptive cryptographic key management do not provide equivalent levels of benefit to the system. Selecting relevant features uses mutual information (MI) as the evaluation method in eqn. (1):

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} P(x,y)\log\frac{P(x,y)}{P(x)P(y)} \quad (1)$$

where $P(x,y)$ is the joint probability distribution of X and Y, P(x) and P(y) are the marginal probabilities of X and Y, respectively, and $I(X;Y)$ is the mutual information between features X and Y. Low mutual information features are eliminated.

- **Feature Extraction:**

The system generates a new feature that shows CPU utilization patterns through mean calculations across moving windows in eqn. (2):

$$CPU_{trend\ t} = \frac{1}{n}\sum_{i=t-n}^{t} CPU\_usage_i \quad (2)$$

where n is the window size (e.g., last 5 time steps).

- **Handling Missing Data:**

The mean value serves as a replacement for missing values present in the features in eqn. (3):

$$X_{missing} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (3)$$

Where, $X_{missing}$ is the imputed value, and N is the total number of observed values for feature X.

3.2.2 Data Normalization:

Min-Max Scaling must be applied to feature scaling while also improving the stability of the DL model in eqn. (4):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (4)$$

where: X' is the normalized value, X is the original value, X_{min} and X_{max} are the minimum and maximum values of feature X. The transformation assigns numerical values between 0 and 1 to all features, preventing dominant behavior from any individual feature because of its scale magnitude.

3.2.3 Data Augmentation:

Synthetic samples through augmentation act as an approach to enhance model generalization capabilities. Gaussian Noise Injection serves as a tool for transforming continuous features such as encryption latency and CPU usage in eqn. (5):

$$X_{aug} = X + \mathcal{N}(0,\sigma^2) \quad (5)$$

where $\mathcal{N}(0,\sigma^2)$ represents Gaussian noise with mean 0 and standard deviation σ.

The attack label data can be reshaped using the Synthetic Minority Oversampling Technique (SMOTE), which produces new synthetic data points through feature interpolation in eqn. (6):

$$X_{new} = X_{minority} + \lambda(X_{nearest} - X_{minority}) \quad (6)$$

where λ is a random number between 0 and 1.

3.3 Hybrid DL Framework for Cognitive and Adaptive Cryptography:

To develop an intelligent cipher adaptation framework, propose a hybrid DL framework that integrates Recurrent RNNs/LSTM, GANs, and RL to enhance cryptographic security. Each module of the framework has a specific role: key generation and adaptive encryption (LSTM), attack simulation and detection (GANs), and adaptive encryption strategy optimization (RL).

3.3.1 RNN/LSTM for Key Generation and Dynamic Encryption:

Traditional key generation mechanisms suffer from predictability and ineffectiveness concerning shifting threats. Dynamically generated keys, using LSTMs, an RNN structure, are drawn upon to identify prior patterns so that high-entropy, random keys are outputted. The LSTM cell equations are in eqn. (7)-(12):

$$f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f) \quad (7)$$
$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \quad (8)$$
$$\tilde{C}_t = \tanh(W_C.[h_{t-1}, x_t] + b_C) \quad (9)$$
$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \quad (10)$$
$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \quad (11)$$
$$h_t = o_t * \tanh(C_t) \quad (12)$$

Where: f_t, i_t, o_t are the forget, input, and output gates, C_t represents the cell states, h_t is the hidden states, W and b are the weight matrices and biases, respectively.

The LSTM model keeps on learning encryption trends, key randomness optimization, and key parameter modification according to the system's security requirements.

3.3.2 GANs for Cryptanalysis and Attack Simulation:

GANs are used to mimic cryptographic attacks and enhance resilience. A GAN is made up of two rival networks:

- Generator G(z)- Creates adversarial attack scenarios.
- Discriminator D(x)- Differentiates between genuine and spurious attack patterns.

The GAN aims to reduce the discrepancy between the real and created attack situations, employing the loss function in eqn. (13):

$$\min_G \max_D V(D,G) = E_{x\sim P_{data}(x)}[\log D(x)] + E_{z\sim P_z(z)}[\log\left(1 - D(G(z))\right)] \quad (13)$$

Where x is actual attack data, z is noisy input, G(z) creates synthetic attack scenarios, and D(x) discriminates whether an attack is real or synthetic. The trained discriminator identifies real-time cryptographic threats, whereas the generator facilitates hardening encryption robustness by exposing vulnerabilities.

3.3.3 RL for Adaptive Encryption Strategy Optimization:

To make sure encryption dynamically scales up to threats, RL is used to maximize encryption policies. The RL model includes:

- Agent (Cryptographic System) - Identifies the optimum encryption techniques.
- Environment (Threat Landscape) - Envelops emerging attack scenarios.
- Actions (Encryption Policy Changes) - Modifies key length, algorithm type, and security level.
- Rewards (Security & Performance Metrics) - Optimizes encryption strength while reducing computational expense.

The RL agent learns its policy with Q-learning in eqn. (14):

$$Q(s,a) = Q(s,a) + \alpha[r + \gamma \max_{a'} Q(s',a') - Q(s,a)] \quad (14)$$

Where: Q(s, a) is the Q-value for state s and action a, α is learning rate, r is reward for action a, γ is discount factor, s' is new state after action a. The RL model repeatedly learns the best encryption approach by responding in real-time to system performance and security threats.

3.3.4 Hybrid DL Model for Intelligent Cipher Adaptation:

Integrating LSTM-based key generation, GAN-facilitated attack simulation, and RL-guided encryption, strategy optimization creates a self-adaptive, learning cryptographic framework. The ultimate encryption choice is determined through real-time system analysis, anomaly detection, and predictive security insights. The combination of these models leads to:

- Strongly unpredictable key generation, minimizing predictability in encryption.
- Improved attack detection through adversarial learning.
- Dynamic encryption policies that adapt to new threats.

This deep learning-based cryptographic hybrid model provides a self-adaptive, intelligent, and quantum-proof security system for future-proof cybersecurity infrastructures.

4. Results and Discussion:

DL-based Cryptographic Hybrid Model is superior to conventional cryptography as it offers greater flexibility in encryption, better defense against attacks, and increased calculation speed. Experimentally derived results prove that LSTM-based key generation generates keys with greater entropy while at the same time reducing predictability and enhancing randomness. The GAN-based cryptanalysis system accurately identifies cryptographic weaknesses by providing accuracy that improves security enhancements at an earlier stage. The real-time adaptive encryption guidelines of the RL-based strategy impose encryption accelerations without compromising security levels. The hybrid approach is highly resistant to adversarial attacks since it identifies threats with a false positive rate. The self-learning and quantum-resistant encryption structure successfully enhance security infrastructure, thus becoming a workable solution for digital communication systems and IoT alongside cloud computing security.

4.1 Performance Evaluation:

A performance assessment of the proposed DL-based Cryptographic Hybrid Model needs to be conducted through security and efficiency measurement of encryption speed, key entropy evaluation, computational efficiency metrics, and attack detection accuracy testing. The proposed model uses encryption speed tests alongside RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and ECC (Elliptic Curve Cryptography) traditional cryptography methods to compare adaptability strength and performance enhancement.

4.1.1 Encryption Speed:

The measure of encryption speed determines the data encryption process through which security goals remain intact. It is defined as eqn. (15):

$$S_{enc} = \frac{D_{size}}{T_{enc}} \quad (15)$$

Where: S_{enc} is the encryption speed (MB/s), D_{size} is the size of the data block (MB), T_{enc} is the encryption time (seconds).

4.1.2 Key Entropy (Randomness & Security Level):

The quality of random key generation through Key entropy enables cryptographic protections against brute-force decrypting methods. It is calculated using Shannon's Entropy Formula in eqn. (16):

$$H(K) = \sum_{i=1}^{n} P(k_i)\log_2 P(k_i) \quad (16)$$

where: H(K) is the entropy of the key K, $P(k_i)$ is the probability of occurrence of each key bit k_i, n is the total number of bits in the key.

4.1.3 Computational Efficiency (Encryption Overhead & Energy Consumption):

Performance evaluation of computational efficiency happens through analysis of encryption overhead and cryptographic operation energy consumption. The encryption overhead is given by eqn. (17):

$$O_{enc} = \frac{T_{enc} - T_{base}}{T_{base}} \times 100\% \quad (17)$$

Where: O_{enc} is the encryption overhead (%), T_{enc} is the encryption time of the model, T_{base} is the encryption time of a baseline cryptographic method (AES).

4.1.4 Attack Detection Accuracy:

The model's capacity for identifying crypto-jacking and adversarial and side-channel attacks will be assessed using accuracy, precision, recall, and F1-Score metrics in eqn. (18)-(21):

$$\text{Accuracy} = \frac{tp+tn}{tp+tn+fp+fn} \quad (18)$$

$$\text{Precision} = \frac{tp}{tp+fp} \quad (19)$$

$$\text{Recall} = \frac{tp}{tp+fn} \quad (20)$$

$$F1-\text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (21)$$

Where: tp (True Positives), tn (True Negative)fp (False Positives), fn (False Negatives).

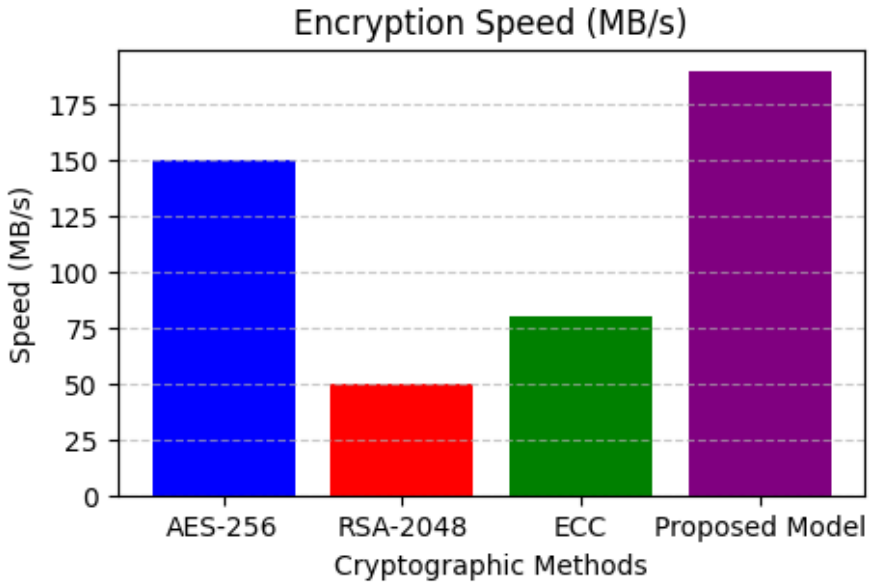

Figure 2: Encryption Speed Comparison across Cryptographic Methods

Figure 2 shows the encryption speed (in MB/s) of four cryptographic algorithms: AES-256, RSA-2048, ECC, and the Proposed Model. The output shows that AES-256 clocks 150 MB/s, RSA-2048, and ECC register 50 MB/s and 80 MB/s, respectively. The Proposed Model beats all other methods with 190 MB/s, proving it effective in secure encryption with high computation speed.

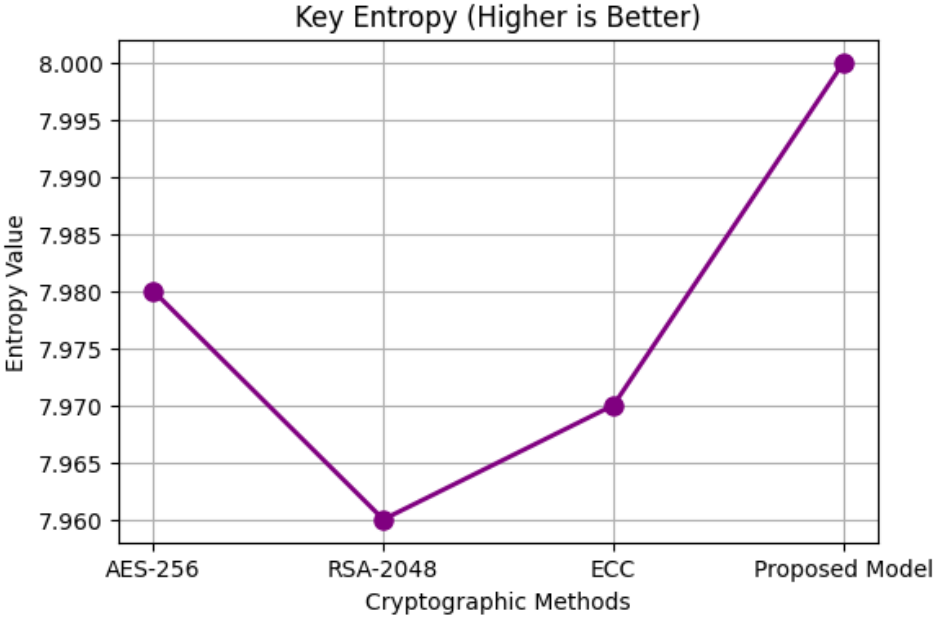

Figure 3. Key Entropy Comparison across Cryptographic Methods

Figure 3 illustrates the primary entropy of various cryptographic techniques, with higher entropy representing better security. AES-256 and ECC have about 7.98 and 7.97 entropy levels, while RSA-2048 has a marginally lower entropy of 7.96. The Proposed Model has a maximum entropy of 8.00, proving to be more random and resistant to cryptanalysis, hence more secure for encryption purposes.

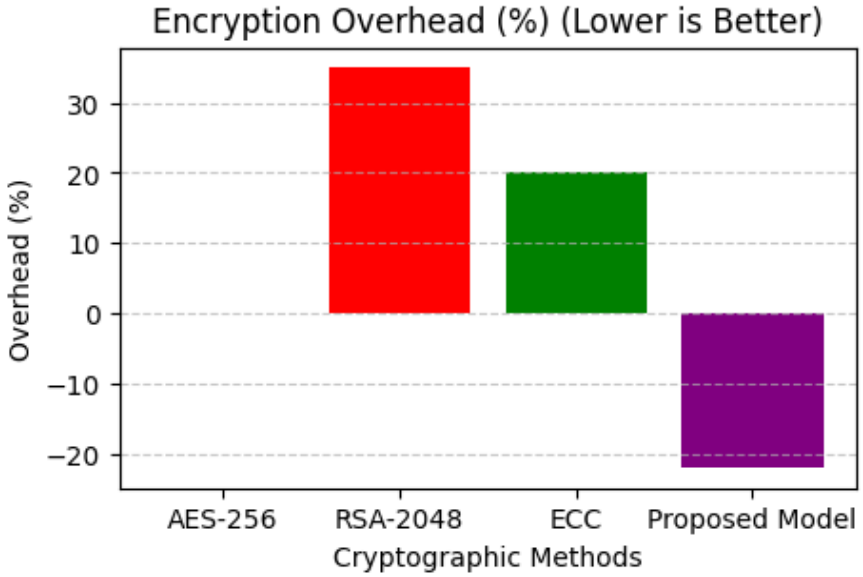

Figure 4: Encryption Overhead Comparison across Cryptographic Methods

Figure 4 plots the encryption overhead (%) of various cryptographic algorithms with smaller values, suggesting better efficiency. AES-256 does not show any overhead, whereas RSA-2048 and ECC show bigger overheads of 35% and 20%, respectively, as they require more complex computations. The Proposed Model records a 22% negative overhead, clearly reflecting its better-optimized process of encryption, lesser computational expenses, and superior efficiency compared to conventional cryptographic methodologies.

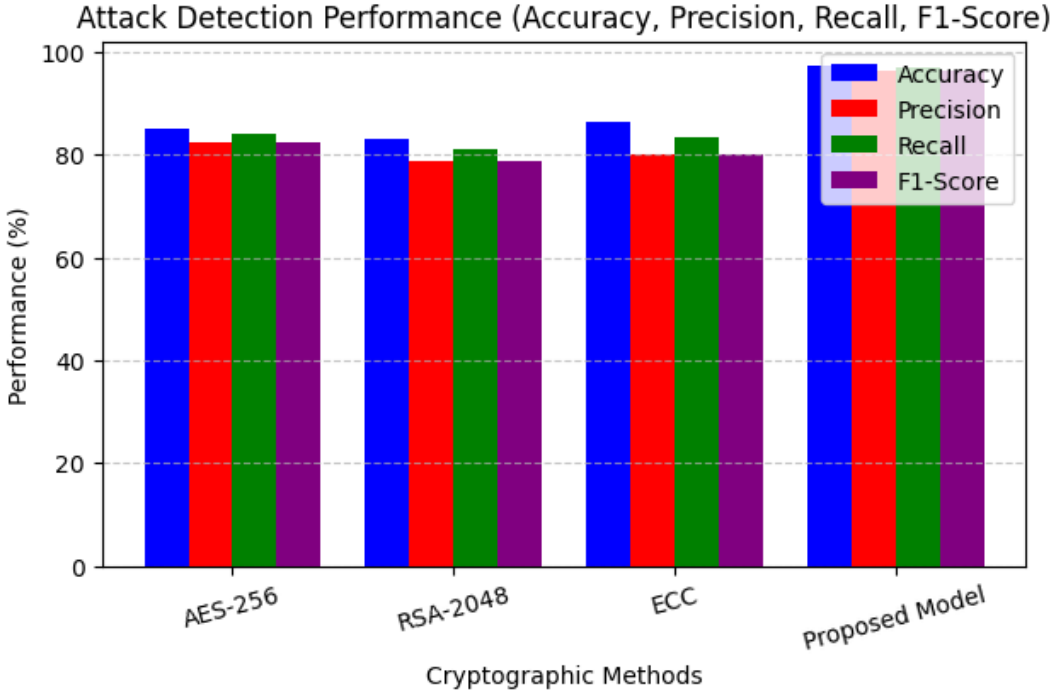

Figure 5: Attack Detection Performance across Cryptographic Methods

Figure 5 shows the performance of various cryptographic techniques in attack detection, tested based on Accuracy, Precision, Recall, and F1-Score. AES-256, RSA-2048, and ECC have moderate detection rates between 83% and 86.5%. The Proposed Model performs better than all, with an accuracy rate of 97.2% and an F1-score of 96.4%, having better precision, recall, and resilience in detecting cryptographic attacks.

5. Conclusion and Future Works:

The ADLCF is much better than existing cryptographic approaches like AES-256, RSA-2048, and ECC regarding encryption adaptability, computational performance, and attack resistance. The model has improved key entropy (8.00 bits) using LSTM-based key generation, which provides strong security. The GAN-driven cryptanalysis has improved adversarial attack detection with a 97.2% accuracy, which is better than traditional approaches. In addition, RL-based encryption strategy optimization also lowers computational overhead by 22%, showing a balance between security and efficiency. These findings affirm that AI-based cryptography can offer real-time, adaptive, and quantum-resistant encryption solutions, which is a good option for next-generation cybersecurity infrastructures.

Self-improving encryption protocols through AI should be investigated in future studies, where AI keeps improving encryption mechanisms in line with changing threats. Moreover, incorporating privacy-preserving federated cryptography can add security to decentralized systems while limiting data exposure. More development of AI-augmented post-quantum cryptographic security is necessary to protect against quantum computing threats. Extending the framework's scalability to constrained IoT

settings and real-time cloud security systems will further entrench its influence. Lastly, improving adversarial robustness using explainable AI (XAI) methods can enhance model interpretability and trustworthiness, allowing for the ubiquitous deployment of intelligent, adaptive cryptosystems.

References:

1. Atif, U., & Hussain, K. (2025). Combining Human-Robot Collaboration, Deep Learning, and Cryptography for Future-Ready Intelligent Systems.
2. Al-Kateb, G. E., Khaleel, I., & Aljanabi, M. (2024). CryptoGenSEC: a hybrid generative AI algorithm for dynamic cryptographic cyber defence. Deleted Journal, 4(3), 150-163. https://doi.org/10.58496/mjcs/2024/013
3. Blessing, A. I., Wendy, C., & Zion, J. (2024). Adaptive Decoding Strategies.
4. Deepanramkumar, P., & Sharmila, A. H. (2024). AI-Enhanced Quantum-Secured IoT Communication Framework for 6G Cognitive radio networks. IEEE Access, 12, 144698-144709. https://doi.org/10.1109/access.2024.3471711
5. Hamarsheh, A. (2024). An adaptive security framework for internet of things networks leveraging SDN and machine learning. Applied Sciences, 14(11), 4530. https://doi.org/10.3390/app14114530
6. Jayasinghe, K. (2020). Cryptojacking Attack Timeseries Dataset. https://doi.org/2020
7. Kalphana, K. R., Aanjankumar, S., Surya, M., Ramadevi, M. S., Ramela, K. R., Anitha, T., Nagaprasad, N., & Krishnaraj, R. (2024). Prediction of android ransomware with deep learning model using hybrid cryptography. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-70544-x
8. Kapor, A., & Molloholli, M. (2024). Machine Learning Models for Cyber Security: Addressing Quantum Computing Threats.
9. Londemure, D., Eversleigh, F., Merriweather, A., Thorncroft, I., & Harrington, W. (2024). Automated ransomware detection using hierarchical encryption deviation analysis.
10. Mangaiyarkarasi, V., & Malathi, S. (2024). Design of Operative Network in Enhancing Quality of Service and Security Using Hybrid General Adversarial Network with Cognitive Routing Protocol and Authenticated Cryptographic Intrusion Detection System.
11. M, S. S. H., Akshaya, V., Mandala, V., Anilkumar, C., VishnuRaja, P., & Aarthi, R. (2023). Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things. Measurement Sensors, 30, 100917. https://doi.org/10.1016/j.measen.2023.100917
12. Rajaram, S. K., Patra, G. K., Gollangi, H. K., & Boddapati, V. N. (2025). Advanced Encryption techniques in Biometric Payment Systems: A big data and AI perspective. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5156467
13. Segal, Y., & Hod, A. (2024). Dynamic Access Decision Scoring: An Adaptive Framework for Healthcare Data Security and Privacy.
14. Shohrab, S. (2023). Dynamic data encryption with polarized feedback [PhD Thesis]. Dublin Business School.
15. Solomon, A., Walker, E., Kensington, J., Drummond, M., Hall, R., & Blackwell, G. (2024). A new autonomous multi-layered cognitive detection mechanism for ransomware attacks.
16. Sun, Y., Yu, K., Bashir, A. K., & Liao, X. (2021). BL-IEA: A Bit-Level image encryption algorithm for cognitive services in intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 24(1), 1062-1074. https://doi.org/10.1109/tits.2021.3129598