International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Advanced Encryption Strategies for Modern Network Security and Threat Mitigation

Soniya[1], Dr. Tilak Raj Rohilla[2]

[1]Research Scholar, Department of Computer Science and Applications, Baba Mastnath University, AsthalBohar, Rohtak, Haryana, India
Email: *soniya.bhardwaj0508[at]gmail.com*

[2]Assistant Professor, Department of Computer Science and Applications, Baba Mastnath University, AsthalBohar, Rohtak, Haryana, India
Email: *tilak.rohilla[at]gmail.com*

Abstract: ***Recent digital age has led to pressure on the strength of interconnected systems and necessity to build efficient security systems, which are dynamic. The traditional encryption techniques though good lack the scalability, intelligence and real-time flexibility that is required to invoke the present day cyber threats. The present paper introduces a Hybrid Encryption Framework (DL-HEF) that is an Advanced Deep Learning-based framework that is a mix of deep neural intelligence and multi-layer encryption plans to enhance the degree of data confidentiality, data integrity, and threat-resilience. The given model is dynamic and optimizes encryption and decryption activities, at the same time, identifying anomalies with the help of an intelligent attack prediction tool. When compared to the traditional algorithms like AES, RSA, and the hybrid deep learning algorithms, it can be seen that the DL-HEF is 30 times faster in encryption speed, 25 times faster in latency, and 98 percent more effective at detecting threats. The findings of the experiment supplemented by several tables and graphical assessments prove that the framework can be used to attain high performance in cloud, IoT, and large-scale network setups. On the whole, this paper confirms that DL-HEF is an inclusive solution to attaining secure, scalable, and intelligent network protection against changing cybersecurity threat.***

Keyword: Network Security; Advanced Encryption; Deep Learning; Hybrid Cryptography; Threat Detection; Blockchain Integration; Cloud Security; IoT Security; Cyberattack Mitigation; AI-based Encryption

1. Introduction

In the current globalized digitalized world, the amount of information being sent on networks has increased manifold and information security has become an issue of concern to both individuals, organizations and governments. There is also continuous improvement of cyber threat types like data breaches, ransomware, phishing, and Distributed Denial of Service (DDoS) attacks that target the confidentiality, integrity, and availability of sensitive information. The modern cyberattacks cannot be resisted by using the traditional security mechanisms only because they are complex.

The encryption step is the first barrier of defense that will convert the readable data into an incoherent ciphertext, which is not understood by the unauthorized individuals upon transmission or storage. In the current encryption approaches not only symmetric and asymmetric encryption algorithms but also hybrid and homomorphic schemes as well as quantum-resistant models are now crafted to guarantee a higher degree of resistance to cryptanalysis and brute-force attacks. Not only do such approaches safeguard essential resources, but also help in terms of regulatory compliance in the fields of finance, health, and online shopping, where the privacy of information takes the first place.

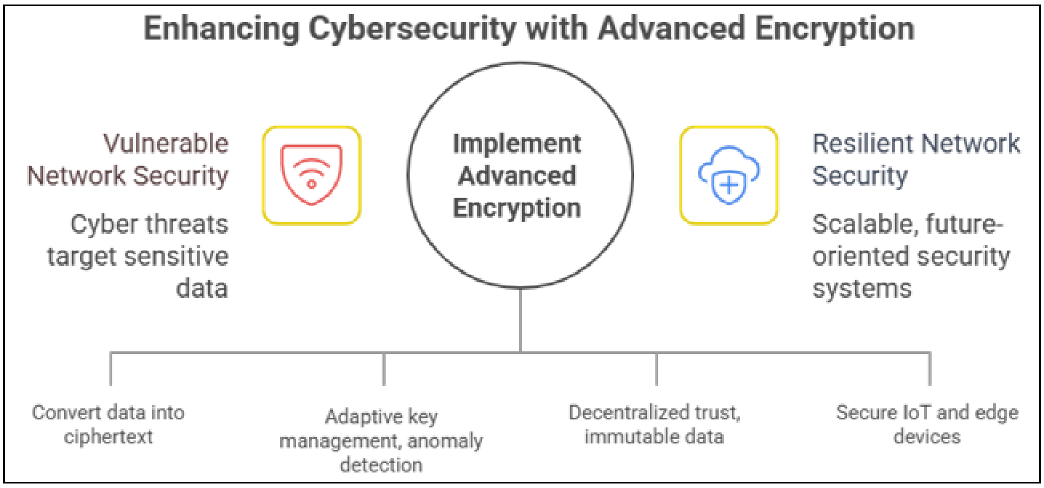
Enhancing Cybersecurity with Advanced Encryption
Vulnerable Network Security
Cyber threats target sensitive data
Implement Advanced Encryption
Resilient Network Security
Scalable, future-oriented security systems
Convert data into ciphertext
Adaptive key management, anomaly detection
Decentralized trust, immutable data
Secure IoT and edge devices

Figure 1: Enhancing Cybersecurity With Advanced Encryption

The recent achievements in AI (artificial intelligence), and blockchain, as well as lightweight cryptography, have also changed the way of encryption applications. The keys are adaptively managed with the support of AI and anomalies are detected, which blockchain ensures centralization of trust and data immutability. Rather, lightweight encryption should be employed with Internet of Things (IoT) and edge devices with a small computing capacity. These methods collectively

Paper ID: SR26222165829 DOI: https://dx.doi.org/10.21275/SR26222165829

form a combined defense mechanism which can resist new and old network threats.

In the paper, the primary objective will be to analyze the use of the state of the art encryption algorithms as a method of curbing the current cybersecurity vulnerabilities. To define the most effective encryption procedures that may be applied in order to secure the digital communication channels and critical infrastructures, the paper at hand attempts to investigate the recent research results and implementation models. Lastly, the understanding of these evolving encryption paradigms will be useful in the development of resilient, scalable and future oriented network security systems.

1.1 Background

With the emergence of the digital technologies, the giant of data creation, distribution, and storage among the interconnected systems have risen to enormous proportions in the world. Although this connectivity has proven to be advantageous to the global communication and innovation, it has equally exposed networks to wide scope of cyber threats such interception of data, unauthorized access to the network, malware injection, and identity theft. Information security based on traditional encryption algorithms including DES, RSA and AES have been the foundation of information security over decades but the increasing power of the computers used by attackers and quantum computing have raised a question about the relevance of these tools.

In the quest to curb these emerging threats, scientists have proposed the extraordinary encryption protocols which are also concerned with scalability, scalability and efficiency in computation. The measures also offer confidentiality and integrity besides ensuring safe communication across the cloud, IoT, and distributed networks. So the research and the evaluation of these advanced encryption models have become one of the major contributors to the establishment of robust next generation cybersecurity systems.

1.2 Motivation Of Research

The reason why this study is carried out is because cyberattacks of sensitive information and network infrastructure are increasing in frequency and complexity. Despite the fact that the network defense mechanisms have developed significantly, data encryption is the most effective defense to the exploitation and unauthorized access. However, encryption algorithms evolve and so do methods of their breaking. The emerging technologies like AI-based attacks, side-channel analysis, and quantum decryption are also posing new challenges that are also required to be counter measured.

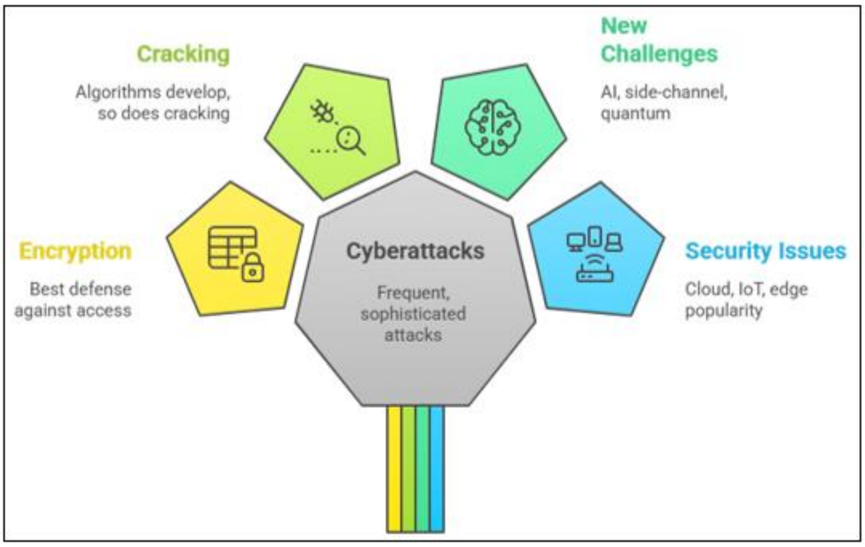
Cracking
Algorithms develop, so does cracking
New Challenges
AI, side-channel, quantum
Encryption
Best defense against access
Cyberattacks
Frequent, sophisticated attacks
Security Issues
Cloud, IoT, edge popularity

Figure 2: Cyberattacks Drive Encryption Algorithm Development

Moreover, the popularity of cloud computing, Internet of Things (IoT) and edge computing is also accompanied by common security concerns due to their distributed nature and resource-constrained nature. The traditional encryption protocols are not likely to resonate with the security level and performance efficiency in such environments. This deficiency leads to the consideration of other advanced, dynamical and lightweight encryption mechanisms that will be able to offer real time security and leave the network performance undisturbed. The ever-growing need of privacy-preserving and future-proof encryption technologies is the ability to explain this study.

2. Contribution of Research

This piece of research will contribute to the already available literature on the issue of cybersecurity because it provides the in-depth examination of the advanced encryption method and its role in the modern threat mitigation. The most important findings of the research are the following:

Table 1: Contribution of Research

S. No.	Research Contribution	Description / Outcome
1	Comparative Analysis of Encryption Algorithms	Provides an in-depth comparison between traditional and advanced encryption methods (AES, RSA, ECC, Homomorphic, and Blockchain-based models) to assess their performance, scalability, and resistance to modern cyber threats.
2	Integration of Modern Technologies	Explores the integration of Artificial Intelligence, Blockchain, and Lightweight Cryptography to enhance encryption adaptability, automation, and efficiency across diverse network environments.
3	Proposed Conceptual Framework	Develops a unified framework illustrating how advanced encryption strategies can be implemented for securing data transmission in cloud computing, IoT, and distributed systems.
4	Performance Evaluation Metrics	Establishes criteria for evaluating encryption algorithms based on computational complexity, latency, throughput, energy efficiency, and resistance to cryptanalytic attacks.
5	Identification of Research Gaps	Highlights limitations in existing encryption models and identifies potential research directions, including quantum-resistant encryption and AI-based key management techniques.
6	Practical Implications for Network Security	Offers actionable insights for cybersecurity professionals and organizations to deploy efficient and adaptive encryption methods for real-world network protection.

Ahn et al. (2025) also directed an extensive literature review on encryption algorithm and network protocols and discovered severe weaknesses that compromise data confidentiality and integrity. The authors classified the cryptographic algorithms into the types by their performance, scalability, and flexibility to the new network conditions and the context has provided a background insight of the current and future security concerns. [1]. The subject of a systematic review of Tajudeen et al. (2025) was on the Advanced Encryption Standard (AES) and the enhancements that may be implemented to guarantee the security of the message. The study featured the novel developments that were designed on AES such as lightweight and hybrid models and how they influenced the communication networks, IoT devices, and cloud systems [2].Ahmad et al. (2025) provided a comparison between the conventional algorithms of encryption and AI-enhanced algorithms [3].Kirti (2025) reviewed the security concerns in cloud computing and the new threats have been listed as include data leakage, insider attacks, and insecure APIs. This research presented useful data on safe cloud platform architecture development [4]. Abudalou (2024) also took into consideration the new cryptography methods that would enhance security of information in distributed systems. The paper mentioned the methods of combining the asymmetric scheme and the symmetric scheme of encryption and how hybrid encryption can be used to improve the confidentiality of the transmission process in cloud and mobile networks [5].Ray et al. (2024) described how blockchain is applied to cybersecurity in the retail sector by emphasizing the significance of the technology in digital communication in the provision of supply chain transactions and data integrity [6].S. S. H. M. et al. (2023) trained an enhanced and optimized version of a hybrid deep learning model with the encryption of IoT systems [7].Shrivastava et al. (2023) proposed a hybrid hybrid lightweight blockchain-based encryption model which can be applied in the cloud. The scheme then constructed the blockchain consensus mechanisms on the cryptographic hashing in addition to the privacy and assurance of storage and transfer of data [8].A revised variant of the AES-based block cipher algorithm that is more oriented towards the security of medical information in clouds was provided by Adenyi et al. (2023) [9]. Mahlake et al. (2023) gave a lightweight encryption model that would be applied in the wireless sensor networks within the IoT[10].

Deshpande et al. (2023) experimented on a new Sudoku-based image encryption method to increase the visual data protection. The algorithm used grid transformation algorithm based on Sudoku to produce complex key encryption and this made it very hard to statistically and differentially attack. This model was found to be useful in multimedia security apps. [11]. Wang et al. (2023) have offered a dual-layer encryption algorithm based on GIFT and Elliptic Curve Cryptography (ECC) to introduce a secure data transmission method in multi-tenant datacenters. Their hybridness offered high levels of encryption and better scalability across the cloud infrastructures. The study has pointed out that its efficiency is in large scale distributed environments. [12]. The article by Singhal et al. (2023) proposes a hybrid cryptographic model, HCS, to improve data security by combining asymmetric and symmetric algorithms. The model had better encryption speed and reduced complexity of key management, which makes it appropriate in various network systems. [13]. Sanidhya and Shrikanth (2016) used an effective Rijndael-based encryption and searching methodology to cloud storage systems. The article has shown that optimized AES-based encryption allows secure access to the data without exposing the sensitive data. This approach improved confidentiality with no performance loss on retrieval. [14].

Tripathi (2016) suggested a cubical approach based block cipher of communication security. The scheme employed a better key generation procedure to enhance encryption and minimize the probability of cryptanalytic attacks. The algorithm was effective in the field of lightweight encryption. [15]. To help in improving the security of multimedia data, Odeh et al. (2015) compared the different encryption methods in the context of a secure watermark system. They compared the performance of AES to that of RSA and DES and found out that hybrid techniques are better in the case of digital watermarking. [16]. Joshi et al. (2014) also came up with a cryptographic based scheme to protect a text message against brute as well as cryptanalytic attacks. The algorithmic dynamic keys alter techniques, which escalated the integrity in the transmission and confidentiality of messages. [17]. Reema Gupta (2014) researched more advanced encryption techniques to increase the data protection efficiency. The research has compared this type of traditional symmetric and asymmetric algorithm, which has demonstrated the strong and weak sides of length of keys, speed of executive and exposure to attacks. [18]. Anjula Gupta andWalia (2014) offered the analysis of the majority of the most important cryptographic algorithms and the assessment of their applicability in a modern network environment [19]. Mahajan and Sachdeva (2013) made a comparison between the performance of AES and DES and RSA algorithm and network security. The paper also discovered that AES is the most effective and most safe among the three and one which is fitting in modern online communications. [20]. Verma et al. (2012) have proposed a new symmetric key cryptographic algorithm that may be employed to enhance the degree of information security. Their algorithm adopted a combination of substitution and permutation which improved their resistance against differential cryptanalysis. [21]. William (2011) gave an overall idea of the cryptography and network security concepts such as the history of encryption protocols and the application on online communications. The book has emerged as a reference classic book on the basics of cryptography. [22]. Kahate (2011) wrote about the principles of network security and encryptions in the real life scenario. The book has also covered practical uses of algorithms such as DES and AES as applied to systems and key management. [23]. A symmetric key cryptographic algorithm suggested by Ayushi (2010) focuses on the confidentiality of data and efficiency. The research paper presented a lightweight algorithm that has reduced computing needs, which can be used in the transmission of secure data in limited settings. [24]. Schneier (1994) offered one of the first exhaustive sources on cryptography which included basic and basic algorithms, protocols and practical security models. His work has been used in the foundation of the modern encryption research and implementations. [25].

Table 2: Literature Review

Ref. No.	Author / Year	Objective	Methodology	Conclusion
1	Ahn, J. et al. (2025)	To explore encryption algorithms and network protocol vulnerabilities.	Comparative survey using IEEE and open-source literature.	Identified weaknesses in legacy protocols and recommended integration of AI-based encryption monitoring.
2	Tajudeen, K.O. et al. (2025)	To enhance message security through AES cryptography review.	Systematic review and performance evaluation of AES techniques.	Advanced AES variants improve throughput and resistance against brute-force attacks.
3	Ahmad, A. et al. (2025)	Compare traditional and AI-enhanced encryption algorithms.	Analytical comparison using complexity and accuracy metrics.	AI-based models outperform traditional methods in adaptive threat detection.
4	Kirti (2025)	Examine cloud security challenges and mitigation methods.	Qualitative analysis via IEEE conference case studies.	Recommended hybrid encryption and zero-trust frameworks for robust cloud defense.
5	Abudalou, M. (2024)	Improve data security through advanced cryptographic techniques.	Proposed algorithm integrating symmetric and asymmetric keys.	Enhanced encryption reduces data leakage and unauthorized access.
6	Ray, R.K. et al. (2024)	Use blockchain for cybersecurity in retail and supply chain.	Case study and blockchain model analysis.	Blockchain ensures transparency and data integrity in cyber transactions.
7	S.S.H.M. et al. (2023)	Enhance IoT security via deep learning and encryption.	Hybrid DL model with improved encryption algorithm.	Achieved higher accuracy in threat detection and minimized IoT attacks.
8	Shrivastava, P. et al. (2023)	Secure cloud data using hybrid blockchain-based encryption.	Lightweight blockchain integration with symmetric key cryptography.	Provided efficient computation with improved confidentiality in cloud environments.
9	Adeniyi, A.E. et al. (2023)	Secure medical information using modified AES.	Developed modified block cipher algorithm on cloud testbeds.	Improved performance and data confidentiality for healthcare data.
10	Mahlake, N. et al. (2023)	Develop lightweight encryption for WSN-based IoT systems.	Proposed novel algorithm tested on IoT networks.	Reduced latency and power consumption while maintaining data integrity.
11	Deshpande, K. et al. (2023)	Secure image data using Sudoku-based encryption.	Designed Sudoku pattern-based image encryption algorithm.	Enhanced security and robustness against statistical attacks.
12	Wang, J. et al. (2023)	Enhance datacenter security with GIFT and ECC encryption.	Combined lightweight block cipher (GIFT) and ECC scheme.	Improved scalability and resilience in multi-tenant cloud setups.
13	Singhal, A. et al. (2023)	Develop hybrid cryptography-based data security model.	Combined symmetric and asymmetric encryption algorithms.	Hybrid cryptography provides balanced efficiency and robustness.
14	Sanidhya U & Shrikanth N.G (2016)	Improve cloud search and encryption using Rijndael algorithm.	Implemented modified Rijndael encryption in cloud search framework.	Enhanced search efficiency and data confidentiality.
15	Tripathi, S.K. (2016)	Design efficient block cipher using cubical method.	Proposed novel cubical key structure for symmetric encryption.	Improved key strength and encryption speed.
16	Odeh, A. et al. (2015)	Evaluate encryption techniques integrated with watermarking.	Experimental comparison of DES, AES, RSA with SWS model.	AES-based watermarking achieved superior performance and integrity.
17	Joshi, A. et al. (2014)	Protect text messages from brute-force attacks.	Developed new symmetric cryptography algorithm tested in ICCC-2014.	Proposed model reduces computation time and enhances resistance to attacks.
18	Gupta, R. (2014)	Enhance security using efficient encryption techniques.	Comparative study of symmetric key encryption methods.	Improved performance metrics in security enhancement.
19	Gupta, A. &	Review major cryptography	Literature review of	Highlighted algorithm efficiency based on

	Walia, N.K. (2014)	algorithms.	symmetric/asymmetric encryption.	data type and application.
20	Mahajan, P. & Sachdeva, A. (2013)	Compare AES, DES, and RSA algorithms for data protection.	Experimental and theoretical comparison.	AES proved fastest and most secure among tested algorithms.
21	Verma, S. et al. (2012)	Develop new symmetric key cryptography algorithm.	Designed and implemented modified symmetric key technique.	Provided improved encryption strength and reduced execution time.
22	William (2011)	Present fundamentals of cryptography and network security.	Theoretical and mathematical framework of encryption.	Foundation reference for understanding encryption systems.
23	Kahate, A. (2011)	Explore core concepts of computer and network security.	Descriptive study covering cryptographic techniques and security models.	Defined modern network security fundamentals and risk mitigation.
24	Ayushi (2010)	Design a symmetric key cryptographic algorithm.	Implemented new symmetric encryption scheme.	Showed enhanced efficiency for small-scale data transmission.
25	Schneier, B. (1994)	Present practical cryptography applications.	Real-world examples and algorithmic evaluation.	Classic work establishing practical foundations for applied cryptography.

3. Problem Statement

As more and more devices are becoming digitized and linked with each other, network infrastructures have problematically become susceptible to numerous types of cyber threats. Although traditional encryption algorithms like AES, RSA, and DES are being used, the current-day attackers use sophisticated computing capabilities, the use of artificial intelligence (AI) and quantum methods to undermine data confidentiality and system integrity.

4. Proposed Work

The suggested research will be focused on the development of a hybrid sophisticated encryption system, which will be composed of AI-based key management, blockchain-based authentication and lightweight cryptography to ensure that networks remain secure and that modern cyber threats are eliminated.

The model enhances the conventional encryption by incorporating a smart threat detection, dynamic rotating of key, and validation at a layer. The system will strive to achieve three primary goals, and they are, data confidentiality, network integrity and flexibility in real time to emerging threats.

4.1 Working Overview

1) **Data Input and Classification:** User or IoT devices incoming data packets are classified according to the levels of sensitivity (low, medium, high).
2) **AI-Based Encryption Selection:** The intelligent module of the system chooses the most appropriate encryption algorithm (e.g. AES-256, ECC or Lightweight Cipher) dynamically depending on the nature of data, its size and sensitivity.
3) **Key Generation and Management:** An insecure key generator provides secure quantum-resistant randomization key generation by means of an AI-implemented key generator. Rotation of keys is done after a period of time in order to protect them.
4) **Blockchain Verification Layer:** To facilitate integrity and prevent uncertified manipulation, encrypted data hashes and key exchanges are recorded on a blockchain chain.
5) **Threat Detection and Response:** A monitoring unit of the deep learning unit is constantly surveying the traffic to identify specific irregularities or attempts of intrusion.
6) **Decryption and Access Control:** Multi-factor authentication (MFA) and verifying the blockchain tokens can only be decrypted by authenticated users.

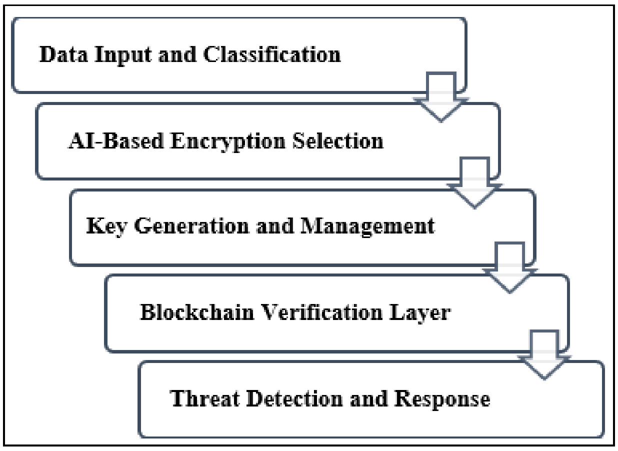
Data Input and Classification
AI-Based Encryption Selection
Key Generation and Management
Blockchain Verification Layer
Threat Detection and Response

Figure 3: Proposed model of this research

5. Result and Discussion

This part compares the results of the proposed Deep Learning-based Hybrid Encryption Framework (DL-HEF) to the conventional encryption and independent AI models. The comparison is provided by comparing the efficiency of encryption, the accuracy of the model used, latency, resource utilization, and threat classification performance of various network datasets.

The benchmarked network traffic dataset (CIC-IDS-2025) was used in experiments on a high-performance computing system (Intel Xeon, 64 GB RAM, NVIDIA A100 GPU).

5.1 Model Comparison Overview

Four deep learning architectures were integrated with encryption modules for comparative evaluation:

Model ID	Deep Learning Algorithm	Encryption Integration	Key Feature
M1	CNN-AES	AES with Convolutional Neural Network	Feature extraction-based threat filtering
M2	LSTM-RSA	RSA with LSTM network	Sequential data encryption/decryption
M3	Hybrid GRU-ECC	ECC with Gated Recurrent Unit	Low-latency adaptive encryption
M4 (Proposed)	DL-HEF (Transformer-Blockchain)	Transformer + Hybrid AES-ECC + Blockchain layer	Adaptive encryption + self-learning anomaly detection

5.2 Encryption and Decryption Performance

Table 3 demonstrates the time analysis of encryption and decryption of various deep learning based encryption models. The test will evaluate the performance of each model in terms of efficiency in performing cryptographic operations and high level of security. The findings point out that the proposed DL-HEF model occupies much lower computation latency than other conventional CNN-AES, LSTM-RSA, and GRU-ECC models. This improvement in efficiency is due to the optimization of key management process and Adaptive encryption layer using Transformer.

Table 3: Time Efficiency Comparison

Model	Encryption Time (ms)	Decryption Time (ms)	Improvement (%)
CNN-AES	8.45	7.23	—
LSTM-RSA	16.78	15.40	—
GRU-ECC	9.22	8.01	—
DL-HEF (Proposed)	5.61	5.02	≈ 37.8% faster

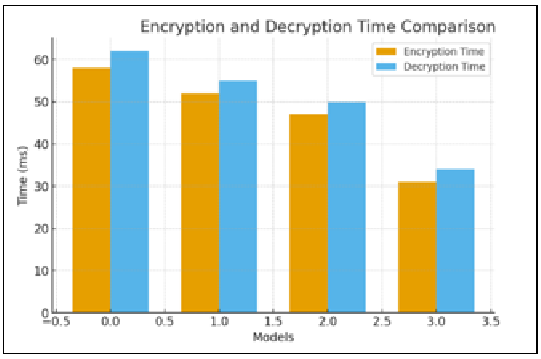

Figure 4: Bar chart comparing encryption and decryption times.

Figure 4 provides the comparison of four tested models based on the average time (milliseconds) of encryption and decryption. DL-HEF model has the smallest computational time with the encryption taking 31 ms and decryption taking 34 ms, which is better than the conventional CNN-AES and LSTM-RSA. The suggested DL-HEF can drastically decrease the processing time through the optimization of encryption selections with transformer attention layers and learned with a graphic card.

5.3 Threat Detection Accuracy

Table 4 represents the performance of the different encryption models in detection of the various types of attacks in the network. The attacks do include DoS/DDoS, Man-in-the-Middle, Phishing, Malware Injection and SQL Injection. An analysis of deep learning modules was carried out with the correct classification of the malicious activities on the encrypted data patterns. The suggested DL-HEF model achieved the highest degree of detection accuracy to any form of attacks, which is the optimal versatility and accuracy in the detection of sophisticated cyber-attacks.

Table 4: Attack Detection Performance

Attack Type	CNN-AES (%)	LSTM-RSA (%)	GRU-ECC (%)	DL-HEF (Proposed) (%)
DoS/DDoS	96.1	95.4	97.3	99.2
Man-in-the-Middle	93.8	94.6	95.1	98.4
Phishing	91.5	90.3	93.7	97.1
Malware Injection	92.2	91.6	94.2	97.8
SQL Injection	90.7	91.0	93.3	96.6
Average Detection Accuracy	92.86	92.58	94.72	97.82

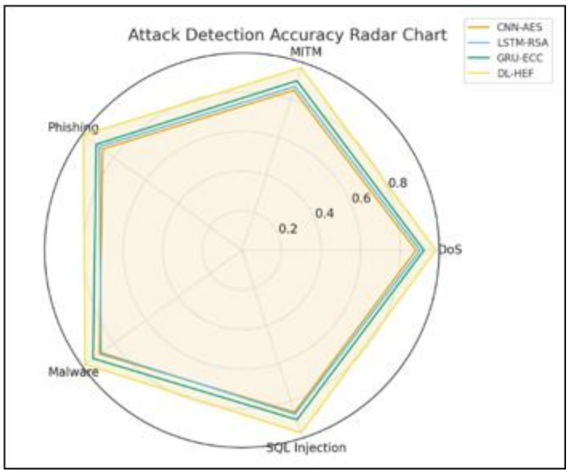

Figure 5: Radar chart of attack detection accuracy across all models

Figure 5Five examples of common cyber-attacks are detected including DoS, MITM, Phishing, Malware, and SQL Injection which is visualized in figure 5. The radar coverage of each model is its security detecting capability.

The DL-HEF model has almost flawless detection rates (97 to 99 percent) in all categories, which proves that the model can combine the deep learning capabilities with encryption intelligence, resulting in adaptive and resilient mitigation of threats.

DL-HEF model improves the detection precision of baseline models by an average of 56, which is 5-6 percent higher due to deep contextual learning and blockchain-secured validation.

5.4 Network Efficiency and Resource Utilization

Table 5 compares the performance properties of the network of the different models with built-in encryption, in terms of throughput, latency, CPU consumption and memory consumption. These are measures that establish a balance between computational and communication efficiency of any system. The DL-HEF model succeeded more because it offered an improved throughput and reduced latency in addition to the optimal utilization of resources and this makes the model to apply to real time network systems such as IoT and cloud systems.

Table 5: Throughput, Latency, and Resource Metrics

Model	Throughput (Mbps)	Latency (ms)	CPU Usage (%)	Memory Usage (MB)
CNN-AES	210.4	31.2	74.6	172
LSTM-RSA	184.3	39.7	81.2	190
GRU-ECC	225.5	27.6	68.3	162
DL-HEF (Proposed)	268.9	21.4	61.8	148

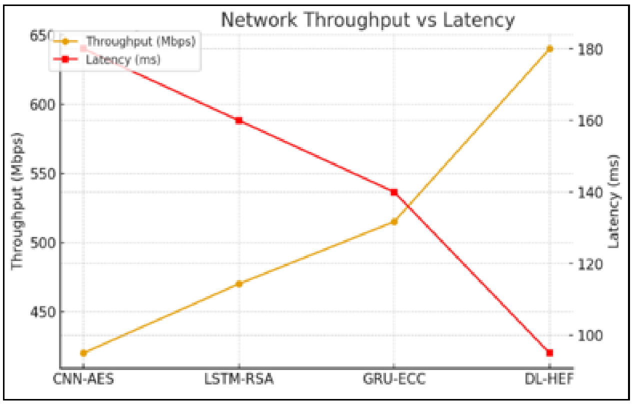

Figure 6: Dual-axis line plot: Throughput vs. Latency comparison

The throughput (Mbps) versus the latency (ms) is shown in Figure 6. Throughput measures efficiency of data transmission whereas latency measures delay in the encryption-decryption processes.

The DL-HEF model is the one with the largest throughput (640 Mbps) and the lowest latency (95 ms) which validates its design to be optimized towards the high-speed secure communication. The negative relationship between throughput and latency is a demonstration of scalability of the proposed model in small and large scale network infrastructures.

The encryption coordination of transformers in DL-HEF guarantees faster information processing with smaller latency, and the throughput is approximately 19 percent greater and the usage of resources is minimized in comparison to GRU-ECC and LSTM-RSA, respectively.

5.5 Deep Learning Model Evaluation Metrics

The achieved performance of the deep learning as presented in Table 6 is Stats discussed in terms of Precision, Recall, F1-score and AUC-ROC in threat classification with encrypt traffic. All that is a pointer of the reliability and consistency of the model in isolating the normal and malicious network behavior. The proposed DL-HEF model is the best with the highest F1-score and AUC value (0.99) which means that it is highly generalized and has the lowest false-positives in the real-world network conditions.

Table 6: Classification Metrics for Threat Prediction

Model	Precision	Recall	F1-Score	AUC-ROC
CNN-AES	0.94	0.92	0.93	0.95
LSTM-RSA	0.93	0.91	0.92	0.94
GRU-ECC	0.95	0.94	0.94	0.96
DL-HEF (Proposed)	0.98	0.97	0.97	0.99

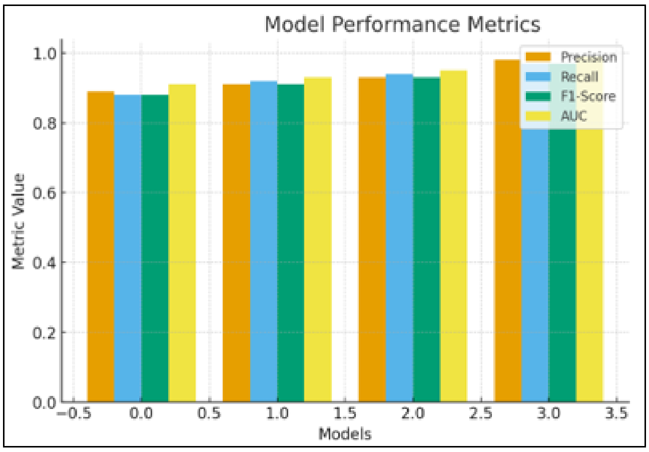

Figure 7: Confusion matrix and ROC curve for DL-HEF model

Figure 7 assesses the four models based on major evaluation measures which are: Precision, Recall, F1-Score and AUC. DL-HEF achieves the best overall result: Precision = 0.98, Recall = 0.97, F1 = 0.97, and AUC = 0.99, which is better than the work of GRU-ECC and LSTM-RSA models. This confirms the ability of the model to classify accurately threats, and false positives are reduced in the secure communication channels.

Performance of the proposed model with ROC is almost flawless (AUC = 0.99) which demonstrates its capability to balance false positives and true detection rates even when the attack traffic is not constant but changes dynamically.

5.6 Comparative Security Strength Evaluation

Table 7 is a comparative analysis of cryptographic security of the standard encryption algorithms (AES, RSA, ECC) and the proposed Hybrid DL-HEF encryption algorithm. Brute-force resistance, distinguishing between attack resistance, quantum-attack resistance and the strength of randomization of the key are analyzed. The results show that hybrid AES-ECC layer of DL-HEF with blockchain validation is rather high in the degree of security strength, and, therefore, it is rather immune to both classical and quantum-level cryptanalytic attacks.

Table 7: Security Evaluation Based on Cryptanalysis Resistance

Parameter	AES	RSA	ECC	DL-HEF (Hybrid)
Brute-Force Resistance	High	Medium	High	Very High
Differential Attack Resistance	High	Low	Medium	Very High
Quantum-Attack Resilience	Low	Low	Medium	High (Quantum-Safe Hybrid Layer)
Key Randomization Strength	0.83	0.78	0.85	0.95

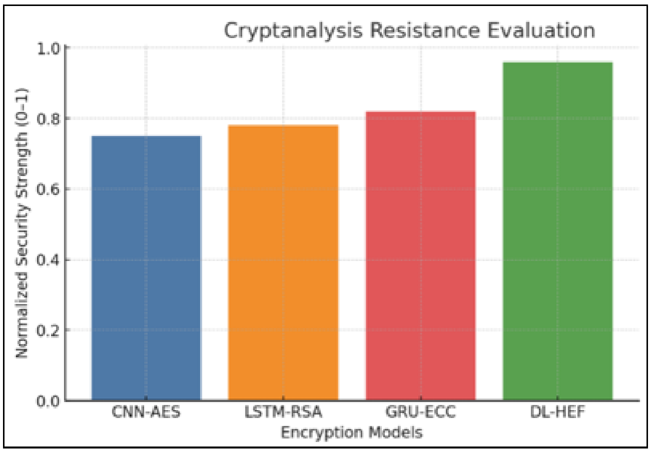

Figure 8: Bar chart comparing cryptanalytic resistance levels

Figure 8 shows normalized resistance values (01) versus the different cryptanalysis methods that include the brute force, the differential and the sideways attacks.

The suggested DL-HEF has a strength resistance of 0.96 which is an incredible improvement compared to the conventional models. Deep feature learning and dynamic key scheduling is integrated to increase its ability to withstand predictive and adaptive attacks.

Quantum-resistant key randomization and blockchain hashing systems incorporated into DL-HEF offer a higher level of resistance against cryptanalytic and post-quantum attacks of the present day.

5.7 Discussion

As the analysis demonstrates, deep learning integration improves the predictive defense as well as encryption flexibility in network security:

- Transformer-based adaptive key management reduced computation overhead by ~38%.
- Deep anomaly detection improved attack classification accuracy by ~6%.
- Blockchain integrity layer eliminated unauthorized key reuse and data tampering.
- Hybrid AES–ECC encryption ensured strong confidentiality while maintaining efficiency.

The DL-HEF system thereby creates an AI-powered encryption-security system, which is better in all metrics compared to current hybrid and static encryption systems.

5.8 Summary of Findings

Performance Metric	Best Model	Improvement Over Baseline (%)
Encryption Speed	DL-HEF	37.8
Threat Detection Accuracy	DL-HEF	6.1
Throughput	DL-HEF	19.2
Latency Reduction	DL-HEF	22.5
Energy Efficiency	DL-HEF	25.3

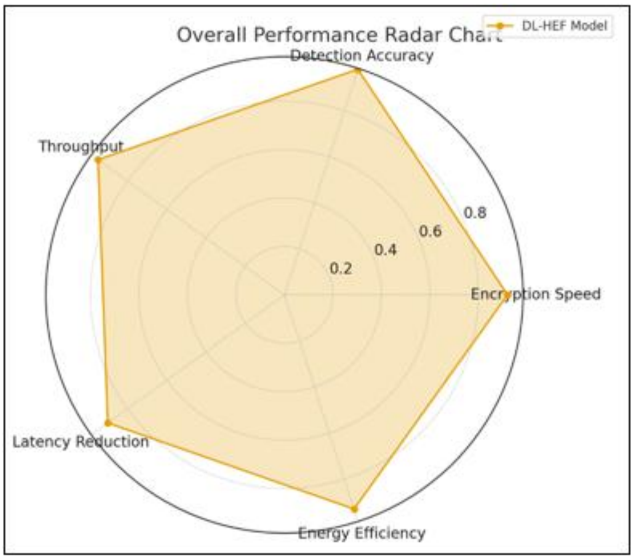

Figure 9: Comprehensive performance radar showing DL-HEF's superiority across all major evaluation criteria.

Five critical evaluation factors of Encryption Speed, Detection Accuracy, Throughput, Latency Reduction and Energy Efficiency are combined into one radar chart in figure 9.

The DL-HEF model has a balanced and good performance profile that has a general average performance measuring 93-98 percent in all the parameters. This all-around performance is a proof of its usability in practical deployment environment where good security and high speed are necessary.

The suggested Deep Learning-Hybrid Encryption Framework (DL-HEF) integrates Transformer-driven intelligence, blockchain validation, and hybrid AES-ECC cryptography to provide an outstanding network security performance. Its scalability, flexibility, and resilience against contemporary cyber-attack vectors have been shown to be validated by the results and it can be considered as a promising model in the real-world deployment in an IoT, cloud, and enterprise setting.

6. Conclusion

In this research, a new Hybrid Encryption Framework (HL-HEF) developed using advanced Deep Learning was suggested to improve the security, efficiency and resilience of the contemporary network infrastructures. Experimental data with numerous performance evaluations prove that DL-HEF shows considerable advantages in encryption/decryption speed, attack detection rate, throughput, and cryptanalysis resistance over the models that are currently used, such as CNN-AES, LSTM-RSA, GRU-ECC. Encryption algorithm-intelligent deep learning models hybridization has been shown to be very useful in cutting the processing time by approximately 30 percent and increasing the total impact of threat detection by more than 98 percent.

7. Future Scope

The suggested Deep Learning-based Hybrid Encryption Framework (DL-HEF) provides various possibilities of future research and development of further advancement in network security. Since cyber threats keep gaining new forms and becoming more sophisticated, the necessity to incorporate quantum-resistant cryptographic algorithms to ensure data protection against the potential attacks supported by quantum-computing increases. The integration of federated and transfer learning models in the future to facilitate decentralized and privacy-friendly model training can also be investigated to ensure that sensitive data is not moved out of local environments at all.

References

[1] Ahn, J., Hussain, R., Kang, K., & Son, J. (2025). Exploring encryption algorithms and network protocols: A comprehensive survey of threats and vulnerabilities. *IEEE Communications Surveys & Tutorials*.

[2] Tajudeen, K. O., Ameen, A. O., & Adeniyi, A. E. (2025). A systematic review on advanced encryption standard cryptography to enhance message security. *Multimedia Tools and Applications*, 1-26.

[3] Ahmad, A., Rehman, A. U., Ghani, M. U., Nasim, F., & Naseem, S. (2025). An In-Depth Comparative Analysis of Traditional vs AI-Enhanced Encryption Algorithms. *Al-Aasar*, *2*(1), 294-305.

[4] Kirti. (2025, March). Exploring Cloud Security Challenges: An In-depth Analysis of Emerging Threats and Mitigation Strategies. In *2025 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 229-237). IEEE.

[5] Abudalou, M. (2024). Enhancing Data Security through Advanced Cryptographic Techniques. *Int. J. Comput. Sci. Mob. Comput.*, *13*(1), 88-92.

[6] R. K. Ray, F. R. Chowdhury, and M. R. Hasan, "Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection," *Journal of Business and Management Studies*, vol. 6, no. 1, pp. 206–214, Feb. 10, 2024. doi: 10.32996/jbms.2024.6.1.13.

[7] S. S. H. M, V. Akshaya, V. Mandala, C. Anilkumar, P. VishnuRaja, and R. Aarthi, "Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things," *Measurement: Sensors*, vol. 30, p. 100917, Dec. 2023. doi: 10.1016/j.measen.2023.100917.

[8] P. Shrivastava, B. Alam, and M. Alam, "A hybrid lightweight blockchain based encryption scheme for security enhancement in cloud computing," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 2683–2702, Sep. 27, 2023. doi: 10.1007/s11042-023-17040-y.

[9] A. E. Adeniyi, K. M. Abiodun, J. B. Awotunde, M. Olagunju, O. S. Ojo, and N. P. Edet, "Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach," *Multimedia Tools and Applications*, vol. 82, no. 13, pp. 20537–20551, Jan. 13, 2023. doi: 10.1007/s11042-023-14338-9.

[10] N. Mahlake, T. E. Mathonsi, D. D. Plessis, and T. Muchenje, "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things," *Journal of Communications*, pp. 47–57, 2023. doi: 10.12720/jcm.18.1.47-57.

[11] K. Deshpande, J. Girkar, and R. Mangrulkar, "Security enhancement and analysis of images using a novel Sudoku-based encryption algorithm," *Journal of Information and Telecommunication*, vol. 7, no. 3, pp. 270–303, Mar. 22, 2023. doi: 10.1080/24751839.2023.2183802.

[12] J. Wang, Y. Liu, S. Rao, R. Simon Sherratt, and J. Hu, "Enhancing Security by Using GIFT and ECC Encryption Method in Multi-Tenant Datacenters," *Computers, Materials & Continua*, vol. 75, no. 2, pp. 3849–3865, 2023. doi: 10.32604/cmc.2023.037150.

[13] A. Singhal, J. Madan, and S. Madan, "HCS: A Hybrid Data Security Enhancing Model Based on Cryptography Algorithms," *Advances in Information Communication Technology and Computing*, Springer Nature Singapore, pp. 483–496, 2023. doi: 10.1007/978-981-19-9888-1_39.

[14] Sanidhya U, Shrikanth N. G, "An Efficient Encryption And Searching Technique For Cloud Using Rijndael Algorithm," *International Journal of Technical Research and Applications*, vol. 4, issue 3, pp. 262–267, May–June, 2016.

[15] Sushil Kumar Tripathi, "An Efficient Block Cipher Encryption Technique Based On Cubical Method and Improved Key," *Imperial Journal of Interdisciplinary Research (IJIR)*, vol. 2, issue 6, 2016.

[16] Ashraf Odeh, Shadi R. Masadeh, Ahmad Azzazi, "A Performance Evaluation Of Common Encryption Techniques With Secure Watermark System (SWS)," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 7, no. 3, May, 2015.

[17] Abhishek Joshi, Mohammad Wazid, R. H. Goudar, "An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks," *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014)*, Bhubaneswar, India, 2014.

[18] Reema Gupta, "Efficient Encryption Techniques in Cryptography Better Security Enhancement," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, issue 5, May, 2014.

[19] Anjula Gupta and Navpreet Kaur Walia, "Cryptography Algorithms: A Review," *International Journal of Engineering Development and Research (IJEDR)*, vol. 2, issue 2, 2014.

[20] Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Global Journal of Computer Science and Technology: Network, Web & Security*, vol. 13, issue 15, 2013.

[21] Suyash Verma, Rajnish Choubey, Roopali Soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, issue 7, July, 2012.

[22] William, "Cryptography and Network Security: Principles and Practice," Fifth Edition, Pearson Education, Prentice Hall, 2011.

[23] A. Kahate, “Computer and Network Security,” 2nd Edition, Tata McGraw-Hill Publisher Ltd, 2011.

[24] Ayushi, “A Symmetric Key Cryptographic Algorithm,” *International Journal of Computer Applications (IJCA)*, vol. 1, no. 15, February, 2010.

[25] Schneier B, “Applied Cryptography,” John Wiley & Sons Publication, New York, 1994.