AI-Based Cryptography: A Comprehensive Review of Adaptive Encryption, Neural Cryptanalysis, and Post-Quantum Resilience

Mohammed A. Abdewi
Mathematics and Computer Science Department, Faculty of Science, Al-Azhar University, Nasr City, Cairo, Egypt
mohammed.alsatori82@gmail.com (corresponding author)

Farouk A. Emara
Mathematics and Computer Science Department, Faculty of Science, Al-Azhar University, Nasr City, Cairo, Egypt
aly_emara86@azhar.edu.eg

Ashraf A. Gouda
Mathematics and Computer Science Department, Faculty of Science, Al-Azhar University, Nasr City, Cairo, Egypt
gouda@azhar.edu.eg

Mohammed A. Razek
Mathematics and Computer Science Department, Faculty of Science, Al-Azhar University, Nasr City, Cairo, Egypt
abdelram@azhar.edu.eg

Received: 25 November 2025 | Revised: 28 January 2026 | Accepted: 14 February 2026

 DOI: https://doi.org/10.48084/etasr.16510

ABSTRACT

Nowadays, protecting information is paramount. With the rapid evolution of cyber threats and the growing potential of quantum computing to compromise classical encryption methods, the integration of Artificial Intelligence (AI) into cryptography has become a promising area for exploration. This review outlines recent advances in AI-based encryption techniques, such as dynamic key generation, adversarial neural cryptography, and AI-enhanced cryptanalysis. It compares AI-based approaches to traditional cryptographic systems in terms of adaptability, security strength, and quantum resistance. This paper also summarizes key research contributions and highlights the benefits and current challenges of deploying AI-based cryptography, including computational overhead and the absence of formal security guarantees. The review aims to offer an introductory overview of how AI is reshaping the future of encryption and to identify areas that require further research and validation.

Keywords-artificial intelligence; AI-based encryption; cryptography; quantum resistance; adversarial neural networks; dynamic key generation; adaptive encryption

I. INTRODUCTION

Encryption is the process of converting data from a readable format (plaintext) into an encoded format (ciphertext), protecting it from unauthorized access and ensuring its confidentiality, integrity, and authenticity. As digital technology has evolved, encryption has become an indispensable tool in protecting sensitive data across various domains, from personal communications to financial transactions and national security systems. Historically, encryption solutions have relied primarily on mathematical complexities and algorithmic rigidity to maintain data security. These classical cryptographic techniques are broadly categorized into two main types: symmetric and asymmetric encryption. Symmetric encryption utilizes a single secret key for both encryption and decryption, with well-established algorithms such as the Advanced Encryption Standard (AES) offering efficient protection. On the other hand, asymmetric encryption (public key cryptography) employs a pair of keys, a public key for encryption and a private one for decryption.

Prominent algorithms in this category include Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), both of which depend on complex mathematical problems such as integer factorization and discrete logarithms. Classical encryption methods have served as foundational components of digital security infrastructure for decades, but their static and mathematically deterministic nature makes them increasingly vulnerable to sophisticated cyberattacks. Today's cybersecurity landscape is characterized by advanced brute-force attacks powered by rapid computational advances, as well as sophisticated side-channel attacks that exploit indirect leakages of information such as timing, power consumption, or electromagnetic emissions [1, 2]. Furthermore, the emergence and rapid progression of quantum computing technologies significantly challenge the security assurances provided by classical encryption algorithms. Specifically, Sho's algorithm, capable of efficiently factoring large integers, undermines the foundations of widely used cryptographic techniques like RSA and ECC. Such vulnerabilities have exposed the critical limitations inherent in classical cryptographic systems, highlighting their insufficient adaptability to modern threats and raising an urgent demand for innovative encryption solutions that are both dynamic and resilient.

In response to these challenges, AI has emerged as a transformative approach, reshaping cryptographic paradigms by introducing adaptive, learning-driven encryption methods. AI-based encryption solutions leverage Machine Learning (ML), neural networks, and adversarial learning to dynamically adjust encryption strategies in response to evolving threats [3, 4]. Unlike classical encryption methods, AI-based approaches can autonomously detect emerging attack patterns and proactively adjust their encryption strategies, significantly enhancing security in real-time. A key innovation offered by AI is adversarial learning, which employs competing neural network models to identify and correct vulnerabilities autonomously, thus continuously reinforcing encryption strength [5]. Furthermore, AI-based solutions demonstrate substantial promise in resisting quantum-computing-based cryptographic threats. Unlike traditional cryptographic techniques that are fundamentally reliant on static mathematical assumptions vulnerable to quantum algorithms (such as Shor's algorithm), AI-based methods offer a dynamic and potentially quantum-resilient alternative due to their adaptability and continuous learning capabilities.

Although the emergence of quantum computing poses an existential threat to classical algorithms, the shift toward AI-based encryption is fundamentally driven by the need to overcome the static and mathematically deterministic nature of traditional cryptographic systems. Classical methods, such as RSA and ECC, rely on fixed mathematical problems that lack the adaptability required to respond to novel, real-time adversarial behaviors without manual intervention. AI-based solutions address these systemic weaknesses by introducing learning-driven paradigms that facilitate dynamic key generation, where neural networks process large datasets to produce unpredictable data-adaptive keys that mitigate traditional key management challenges. Furthermore, through techniques like adversarial neural cryptography, AI systems can autonomously identify and rectify vulnerabilities through a self-improving loop, offering a level of proactive threat detection and resilience that static classical models cannot achieve. By moving away from rigid algorithmic structures, AI provides an adaptive framework that not only complements post-quantum primitives but also ensures that cryptographic defenses can evolve in real-time alongside increasingly sophisticated non-quantum cyber threats.

Despite the significant advantages offered by AI-based encryption, it is important to recognize and address several challenges inherent in these innovative approaches. Notably, AI-based encryption methods often require substantial computational resources, particularly when training DL models or conducting real-time cryptanalysis. This computational overhead can limit their scalability and applicability in resource-constrained environments such as Internet of Things (IoT) devices. Moreover, AI-based cryptographic systems currently lack formal security proofs equivalent to those available for classical cryptographic schemes, raising concerns about their reliability and robustness against sophisticated adversaries. Additionally, while AI methods offer promise in quantum resistance, their practical effectiveness against quantum-powered attacks remains an ongoing research area, necessitating rigorous analysis and validation.

This review aims to comprehensively explore these emerging AI-based cryptographic solutions, examining their fundamental techniques, capabilities, potential for post-quantum resilience, and challenges in practical deployment. Various AI-enhanced cryptographic methodologies, including AI-based key management, adversarial neural cryptography, real-time adaptive encryption protocols, and AI-based cryptanalysis, are reviewed. By evaluating their effectiveness against traditional methods, this review seeks to illuminate how AI-based solutions can significantly enhance data security in an evolving threat landscape, ultimately paving the way for future-proof cryptographic practices.

II. CLASSICAL CRYPTOGRAPHY AND ITS LIMITATIONS

Cryptography has long served as the foundation for securing digital communications by ensuring the confidentiality, integrity, and authenticity of data. Classical cryptographic systems fall into two primary categories: symmetric encryption and asymmetric encryption, both of which rely heavily on well-established mathematical principles. In symmetric encryption, a single secret key is used for both encryption and decryption processes. Widely adopted algorithms in this category include AES, which provides efficient encryption but suffers from key distribution challenges. In contrast, asymmetric encryption, also known as public key cryptography, employs a pair of keys consisting of a public key for encryption and a private key for decryption. Notable algorithms include RSA and ECC, both of which derive their security from hard mathematical problems such as integer factorization and discrete logarithms. Although these classical methods have underpinned secure communications for decades, they face increasing limitations in today's complex threat landscape. One significant challenge is their static nature, which makes them poorly suited for dynamically evolving cyber threats. For example, brute-force attacks have become

more feasible due to modern computing power, and side-channel attacks now exploit indirect information leakage such as timing or electromagnetic emissions [1, 2]. A particularly critical vulnerability is the emerging threat of quantum computing. Algorithms like Shor's algorithm can solve the integer factorization and discrete logarithm problems in polynomial time, thus undermining the core assumptions behind RSA and ECC. This advancement poses an existential risk to many classical cryptographic protocols, which are not designed to resist quantum attacks. Additionally, classical cryptographic methods often rely on fixed encryption schemes and lack adaptability in real time, as they cannot autonomously detect novel threats or respond to adversarial behavior without human intervention. As a result, their static design makes them increasingly vulnerable in environments that require dynamic and intelligent responses. These growing challenges necessitate the exploration of alternative adaptive cryptographic paradigms, such as those enabled by AI. AI-based cryptographic systems aim to address these limitations by introducing self-learning capabilities, dynamic key generation, and real-time threat adaptation, offering a promising direction to secure sensitive information in the face of emerging threats [3, 4].

III. CORE AI-BASED ENCRYPTION TECHNIQUES

The integration of AI into the field of cryptography represents a paradigm shift from static, mathematically predefined systems to dynamic, adaptive models capable of learning from evolving threats. AI-based encryption takes advantage of the capabilities of ML, DL, and neural networks to enhance the flexibility, security, and efficiency of cryptographic protocols. To evaluate the relative strengths and weaknesses of classical and AI-based encryption methods, it is essential to assess them across four critical criteria: adaptability, security strength, computational cost, and quantum resistance. These dimensions reflect not only the technical performance of an encryption method but also its suitability in addressing evolving cybersecurity challenges.

A. Adaptability

Traditional cryptographic systems are inherently static. Once an algorithm such as AES, RSA, or ECC is defined, its operation remains unchanged unless explicitly reconfigured. Although such algorithms are designed for broad reliability, they do not respond dynamically to novel threats or changes in attack patterns. Updates or improvements often require manual intervention, system reconfiguration, or a complete cryptographic transition. In contrast, AI-based encryption introduces adaptive capabilities. ML models, particularly DL and reinforcement learning techniques, can analyze new attack vectors, detect anomalies in encrypted traffic, and autonomously adjust encryption strategies in real time. This self-improving nature allows AI systems to evolve alongside threats, offering a dynamic defense mechanism that static algorithms cannot match [3, 4].

B. Security Strength

The security of classical encryption is based on hard mathematical problems such as integer factorization (RSA) or discrete logarithms (ECC). These problems have been studied extensively and, under current computational assumptions, are difficult to solve. As a result, classical cryptosystems offer strong security when correctly implemented. However, once a vulnerability is discovered (e.g., a flaw in key management or implementation), the entire system may become compromised. AI-based systems offer potentially higher resilience by introducing randomness, pattern recognition, and real-time learning. Through adversarial training, such as Generative Adversarial Networks (GANs), AI models can iteratively improve encryption protocols to withstand simulated attacks [5-8]. Nonetheless, the lack of formal security proofs in most AI-based models makes their theoretical robustness less well-established than that of classical methods. However, their practical security strength may outperform classical systems in environments where adaptability is critical.

C. Computational Cost

Established algorithms such as AES are computationally efficient, especially when implemented with hardware acceleration. However, some public-key systems, such as RSA and ECC, involve complex operations (e.g., modular exponentiation) that become computationally expensive at high key sizes, particularly in constrained environments like the IoT. AI models, especially those involving deep neural networks or adversarial training, often require significant computational resources for training and inference. Real-time applications of AI encryption can impose high memory and processing demands, limiting their feasibility in resource-constrained settings. Techniques such as lightweight neural architectures and model compression are under research to address this limitation.

D. Quantum Resistance

Most classical public-key algorithms are vulnerable to quantum attacks, particularly Shor's algorithm, which can efficiently solve integer factorization and discrete logarithms. This makes RSA and ECC especially susceptible in the presence of large-scale quantum computers. AI-based cryptography does not rely on the mathematical hardness assumptions targeted by quantum algorithms. Instead, it depends on the data-driven behavior of neural networks and adversarial processes. This offers promising, though not yet fully validated, potential for quantum resistance. Moreover, AI techniques can be combined with post-quantum primitives (e.g., lattice-based encryption) to improve security in the post-quantum era [7].

The technical foundation of AI-based encryption is based on adversarial training loops and data-driven pattern recognition, moving beyond the static mathematical assumptions of classical ciphers. In adversarial neural cryptography, training involves a competitive process where a generator network creates encryption protocols while a rival adversary network attempts to decrypt them; the resulting feedback allows the generator to iteratively reinforce the system's security. For applications such as cryptanalysis,

Convolutional Neural Networks (CNNs) are trained on extensive datasets of ciphertext-plaintext pairs to autonomously learn differential characteristics, a method that has practically outperformed classical techniques in breaking the SPECK cipher. Practical scalability is currently being explored through Federated Learning for distributed key management in the Internet of Vehicles (IoV) and triple-layer neural networks for IoT security. Despite these advances, the transition to AI-based models introduces significant computational overhead and challenges in terms of training stability and hyperparameter tuning. To mitigate these trade-offs and improve performance in resource-constrained environments, recent research emphasizes the development of lightweight neural architectures and techniques such as model pruning and Tiny Machine Learning (TinyML).

IV. AI ENHANCEMENTS IN CRYPTOGRAPHY

The most significant contribution of AI to cryptography comes from its ability to enhance encryption through ML and DL models. These AI-based methods provide the following enhancements, shown in Figure 1.

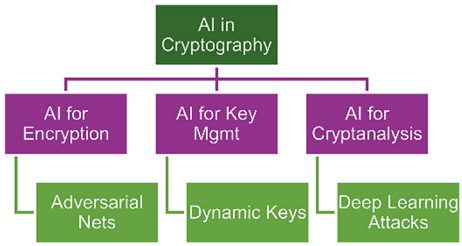

Fig. 1. Taxonomy of AI applications in cryptography.

- Dynamic Key Generation: In classical encryption, keys are static and vulnerable to brute force or advanced cryptographic attacks. AI, however, can dynamically generate cryptographic keys using ML algorithms, making it harder for attackers to predict or break the encryption. DL models, such as neural networks, can process large datasets, generating encryption keys that adapt based on the data being encrypted, which increases the unpredictability and security of the system.
- Adversarial Neural Cryptography: AI also facilitates the development of adversarial neural networks, where two networks (the generator and adversary) compete to enhance encryption techniques. These networks continuously learn from each other. For instance, one network generates encryption protocols while the other attempts to break them, forcing both systems to adapt and improve autonomously. This technique mimics GANs and strengthens encryption against real-world adversarial threats. The adversarial process is visually represented in Figure 2, where the generator produces encrypted data and the adversary analyzes vulnerabilities, feeding back information to iteratively improve encryption. This self-improving loop is the cornerstone of Adversarial Neural Cryptography. An example of how GANs are used in cryptography can be found in [6].

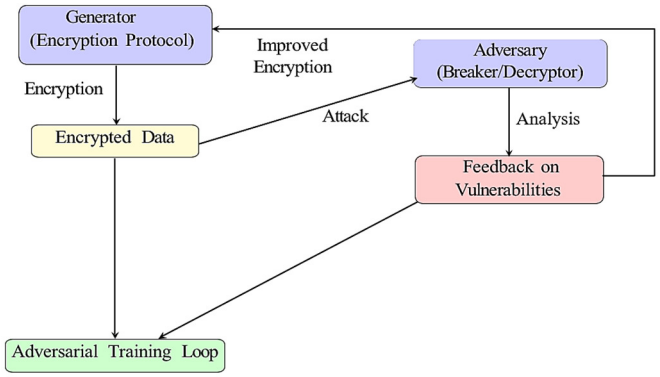

Fig. 2. Adversarial Neural Cryptography: The generator creates encrypted data, while the adversary analyzes it for vulnerabilities, providing feedback that improves encryption in a self-reinforcing adversarial training loop.

- Real-Time Threat Detection and Adaptation: One of AI's strongest attributes in encryption is its ability to detect and respond to threats in real time. ML models can monitor encrypted traffic, detect anomalies, and adapt encryption protocols based on detected attack patterns. This continuous learning process allows AI to keep pace with the rapidly evolving nature of cyber threats, providing a level of security that classical methods cannot.
- Post-Quantum Encryption Potential: With quantum computing posing a significant threat to classical cryptographic algorithms like RSA and ECC, AI-based encryption offers potential quantum-resistant solutions.

By moving away from fixed mathematical problems and adopting flexible data-driven models, AI-based systems [7] can provide more robust defense mechanisms against quantum-powered cryptographic attacks. The transition from classical to AI-based encryption marks a revolutionary step in securing sensitive information. As the digital landscape evolves, so do the methods we use to protect data. AI-based encryption provides a more adaptive and resilient approach to safeguarding information, with the added potential to withstand the quantum computing threats on the horizon. By incorporating ML, adversarial networks, and DL models, AI significantly enhances both the security and efficiency of modern cryptographic systems.

V. PROS AND CONS OF AI-BASED CRYPTOGRAPHY

The field of AI-based cryptography has advanced significantly, leveraging adversarial neural networks and ML models. In [5], novel asymmetric encryption methods were explored, highlighting scalability, post-quantum potential, and the need for computational resources and hyperparameter tuning. In [8], symmetric encryption was improved using adversarial networks, demonstrating adaptability but facing training stability and real-world resistance challenges. In [9], Tree Parity Machines were explored for quantum-resistant cryptography, optimizing synchronization time but encountering entropy degradation and computational costs. Although these approaches demonstrate the transformative potential of AI in cryptography, challenges such as scalability and robustness remain.

TABLE I. OVERVIEW OF AI TECHNIQUES APPLIED IN CRYPTOGRAPHIC CONTEXTS

Ref.	Year	Encryption type	AI technique	Contribution	Limitation
[2]	2016	Secure inference	Encrypted DL (CryptoNets)	Enabled neural inference on encrypted data using homomorphic encryption	Limited to linear layers; slow inference
[8]	2016	Symmetric	Adversarial neural networks (GAN)	Introduced adversarial training for symmetric encryption using neural networks	Unstable training; lacks scalability; no formal proof
[10]	2019	Symmetric (SPECK cipher)	CNN	First use of deep learning for differential cryptanalysis; surpassed classical methods	Focused on reduced-round ciphers; needs large datasets
[11]	2020	Distributed ledger	AI + Blockchain	Explored the convergence of AI and blockchain for secure distributed systems	Lacks empirical validation; theoretical framework
[12]	2021	Cryptanalysis	DL (CNN)	Evaluated the effectiveness of DL for cryptanalysis in EURO- CRYPT study	Effective only on lightweight ciphers; not for RSA/ECC
[1]	2021	Traffic encryption	Hybrid DL	Detected anomalies in encrypted internet traffic	False positives; does not encrypt/decrypt
[13]	2024	Hybrid	GAN + XOR	Developed a hybrid encryption system combining GAN and XOR for enhanced security	Scalability and performance on larger datasets need exploration
[14]	2022	Privacy-preserving ML	Fully Homomorphic Encryption (FHE)	Implemented privacy-preserving ML using FHE for deep neural networks	Limited to simple models; performance overhead
[15]	2021	Blockchain security	AI Techniques	Reviewed the integration of AI and blockchain for enhanced security	Broad scope; lacks specific implementation details
[16]	2023	Symmetric	Triple Layer Vector-Valued Neural Network (TLVVNN)	Proposed a symmetric neural cryptographic key generation scheme for IoT security	Requires further validation in diverse IoT scenarios
[5]	2023	Asymmetric	GAN	Neural key exchange without pre-shared secrets; potential post-quantum resilience	Requires high computational power and hyperparameter tuning
[9]	2023	Asymmetric	Tree Parity Machines (TPMs)	Efficient synchronization for key generation; tested in insecure environments	Vulnerable to improper parameter choice; limited entropy
[3]	2023	Key management	Federated Learning	AI-based distributed key generation in IoV; preserves privacy	Dependent on data distribution; coordination overhead
[4]	2023	Symmetric image encryption	Hyperchaotic+ DL	Designed hybrid encryption for multimedia using chaotic maps and AI	Application-specific; lacks generalizability
[7]	2023	Intrusion detection	Multi-ML ensemble	Reviewed AI- powered IDS for encrypted environments	Did not propose an encryption algorithm
[6]	2024	Symmetric (GAN-based)	GAN with optimized activation	Studied GAN activation functions to improve encryption quality	No real-world integration or performance benchmark
[17]	2024	Traffic classification	ML (SVM, RF)	Classified encrypted traffic using AI models	Focuses on classification, not encryption
[18]	2024	Comparative analysis	AI era cryptography	Analyzed symmetric and asymmetric encryption algorithms in the context of AI	Needs empirical data; theoretical analysis
[19]	2021	Business intelligence	Steganography+ Cryptography	Enhanced business intelligence security using combined techniques	Applicability to other domains needs assessment
[20]	2022	Big data security	AI-enhanced models	Evaluated security threats and defense strategies in big data environments	Requires real-world deployment for validation
[21]	2024	National security	Cryptographic Security Models	Emphasized AIs' role in mitigating cyber threats at the national level	Policy implications need further exploration
[22]	2022	Healthcare security	AIoT Cryptographic Protocols	Addressed privacy and integrity concerns in AIoT healthcare systems	Implementation challenges in diverse healthcare settings
[23]	2022	Secure communication	Quantum Cryptography	Compared classic vs. quantum cryptographic techniques for secure communication	Quantum infrastructure requirements
[24]	2025	AI security	Various cryptographic techniques	Conducted a bibliometric review of cryptographic techniques in AI security	Broad overview; lacks in-depth analysis of individual techniques
[25]	2024	AES-128 chosen-plaintext cryptanalysis + topic modeling	CNN, Bi-LSTM, Bi-GRU	First DL framework to classify ciphertext topics without decryption	Fixed ciphertext size; limited datasets

To better understand the advancements and challenges in AI-enhanced cryptography, Table I presents a comparative summary of prominent studies in this field. The papers are classified based on encryption type, the applied AI technique, their main contributions, and known limitations.

VI. AI-BASED CRYPTANALYSIS

When it comes to cryptanalysis, the art of breaking cryptographic AI has proven to be a game-changer [12], and several related studies can be found in [26, 27]. Traditional cryptanalysis techniques, such as brute force, differential cryptanalysis, and linear cryptanalysis, often require deep mathematical insight and extensive manual effort. However, ML models, especially DL, have significantly accelerated this process by automating complex calculations, recognizing patterns, and detecting vulnerabilities that might escape traditional methods.

A. ML in Cryptanalysis

The most remarkable breakthrough in AI-based cryptanalysis comes from the application of DL to break lightweight block ciphers like SPECK [10]. The use of CNNs

for cryptanalysis revolutionized how cryptographic weaknesses are identified. By training CNNs to differentiate between real ciphertext pairs and random data, the model can learn the underlying differential characteristics of the cipher, allowing it to predict the correct encryption key. In [10], a CNN-based approach surpassed classical cryptanalysis in both speed and accuracy. Classical techniques, like differential cryptanalysis, often require human expertise to analyze how input differences affect the ciphertext. In contrast, AI models can automatically detect these differences and refine their approach as they are exposed to more data. This allows AI-based cryptanalysis to scale faster and identify patterns with greater precision.

B. Key Contributions of AI to Cryptanalysis

AI-based cryptanalysis offers several clear advantages over traditional methods:

1. Automation and Speed: AI models can process large datasets rapidly, automating tasks that previously required manual effort. For example, CNNs have been able to quickly break down reduced-round versions of SPECK [10], a task that would have been prohibitively time-consuming using traditional methods.
2. Pattern Recognition: ML, particularly DL, excels at detecting complex patterns that may not be obvious through classical techniques. These patterns are crucial for identifying weaknesses in encryption schemes. AI models can learn adaptively from ciphertext-plaintext pairs, as demonstrated in recent studies [10].
3. Adapting to New Cryptographic Systems: ML models can be retrained as new encryption systems emerge, ensuring that cryptanalysis tools stay relevant in a rapidly evolving landscape. This adaptability is a significant advantage over traditional static methods.

C. Challenges and Future Directions

Although AI has shown promise in breaking lightweight encryption systems, such as SPECK, several challenges remain, particularly when dealing with more complex encryption algorithms such as RSA and ECC [5]. AI models, although effective against block ciphers, may struggle with the computational complexity of public-key systems, where the problem space is much larger.

Another concern is the reliance on large datasets for training AI models. For AI-based cryptanalysis to be effective, models require extensive ciphertext-plaintext pairs to learn from, which may not always be available. Additionally, as quantum computing advances, many current cryptographic systems, including those targeted by AI, are likely to be rendered vulnerable, emphasizing the need for post-quantum cryptographic research.

AI-based cryptanalysis has already demonstrated its ability to outperform traditional methods in certain cases, such as recent work on block ciphers [10]. However, future advances must focus on addressing the challenges posed by more complex cryptographic systems and preparing for the advent of quantum computing.

VII. OPEN RESEARCH QUESTIONS AND FUTURE DIRECTIONS

AI-based encryption presents numerous promising avenues, but several critical research challenges remain unresolved. First, unlike classical cryptographic algorithms that are grounded in rigorous mathematical proofs, AI-based encryption systems currently lack formal security guarantees, raising the question of how provable security frameworks can be developed for neural cryptographic models under real-world adversarial conditions. Additionally, the high computational demands of training and deploying DL models hinder their deployment in resource-constrained environments such as IoT; thus, there is a need for lightweight solutions through techniques like model pruning, quantization, or Tiny Machine Learning (TinyML). Moreover, these systems remain susceptible to adversarial ML threats, including adversarial examples and model poisoning, necessitating the development of robust defense mechanisms to prevent key extraction or encryption bypass. Another significant gap is the absence of standardized datasets and evaluation benchmarks, making it difficult to consistently compare AI-based cryptographic methods; thus, establishing reproducible metrics for robustness, entropy, speed, and resistance to attacks is essential. Finally, with the looming threat of quantum computing, integrating AI with post-quantum cryptographic primitives such as lattice-based or hash-based systems is vital, and research must focus on how to optimally structure such hybrid approaches to combine adaptability with quantum resistance.

VIII. CONCLUSION

As cyber threats grow in frequency and sophistication, the limitations of traditional cryptographic methods become increasingly evident. Classical encryption, although foundational to modern security practices, struggles to keep up with the dynamic and evolving nature of attacks, particularly with the looming threat of quantum computing. In this landscape, AI-based encryption solutions represent a transformative advancement, offering adaptability, real-time threat detection, and continuous learning capabilities that classical systems lack. This review has highlighted several key strengths of AI in cryptography:

1. Enhanced Security Through Learning: AI models, especially DL networks, improve encryption by recognizing patterns and detecting vulnerabilities that classical methods might overlook. For example, CNNs have outperformed traditional cryptanalysis methods by identifying weaknesses more efficiently, such as through adversarial neural networks, which continuously evolve encryption strategies to stay ahead of attackers.
2. Dynamic Adaptation: AI-based systems adapt autonomously to emerging threats.
3. Potential for Quantum Resistance: As quantum computing becomes a viable threat, AI-based approaches provide potential post-quantum solutions that can adapt to quantum-based attacks, unlike static, mathematically-based traditional encryption systems.

However, AI-based encryption faces several challenges:

1. Computational Overhead: DL models, particularly those used in real-time encryption and cryptanalysis, require significant computational resources, which limits their deployment in resource-constrained environments like IoT.
2. Lack of Formal Security Proofs: Unlike classical cryptographic systems, AI-based models do not have the same level of provable security, making them vulnerable to adversarial attacks.
3. Quantum Threats: Although AI offers potential solutions, it still relies on current mathematical foundations that may be vulnerable to quantum computing attacks unless specifically integrated with post-quantum cryptographic techniques.

Looking ahead, AI-based encryption will undoubtedly play a pivotal role in the future of data security. Its combination of adaptability, continuous learning, and potential quantum resilience positions AI as a key tool in the next generation of cryptographic solutions. However, overcoming current limitations, particularly the need for formal security proofs and managing computational costs, will be essential for widespread adoption in critical security environments.

The future of cryptography lies in the integration of AI with emerging post-quantum frameworks, where dynamic, self-improving models can provide the robustness and security needed for the digital world's growing complexities.

REFERENCES

[1] T. Bakhshi and B. Ghita, "Anomaly Detection in Encrypted Internet Traffic Using Hybrid Deep Learning," *Security and Communication Networks*, vol. 2021, no. 1, 2021, Art. no. 5363750, https://doi.org/10.1155/2021/5363750.

[2] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy," in *Proceedings of The 33rd International Conference on Machine Learning*, June 2016, pp. 201–210.

[3] S. S. Chaeikar, A. Jolfaei, and N. Mohammad, "AI-Enabled Cryptographic Key Management Model for Secure Communications in the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 4589–4598, Apr. 2023, https://doi.org/10.1109/TITS.2022.3200250.

[4] D. Xu, G. Li, W. Xu, and C. Wei, "Design of artificial intelligence image encryption algorithm based on hyperchaos," *Ain Shams Engineering Journal*, vol. 14, no. 3, Apr. 2023, Art. no. 101891, https://doi.org/10.1016/j.asej.2022.101891.

[5] I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Learning asymmetric encryption using adversarial neural networks," *Engineering Applications of Artificial Intelligence*, vol. 123, Aug. 2023, Art. no. 106220, https://doi.org/10.1016/j.engappai.2023.106220.

[6] P. Singh, S. Dutta, and P. Pranav, "Optimizing GANs for Cryptography: The Role and Impact of Activation Functions in Neural Layers Assessing the Cryptographic Strength," *Applied Sciences*, vol. 14, no. 6, Mar. 2024, https://doi.org/10.3390/app14062379.

[7] T. Sowmya and E. A. M. Anita, "A comprehensive review of AI based intrusion detection system," *Measurement: Sensors*, vol. 28, Aug. 2023, Art. no. 100827, https://doi.org/10.1016/j.measen.2023.100827.

[8] M. Abadi and D. G. Andersen, "Learning to Protect Communications with Adversarial Neural Cryptography." arXiv, Oct. 21, 2016, https://doi.org/10.48550/arXiv.1610.06918.

[9] M. Stypiński and M. Niemiec, "Synchronization of Tree Parity Machines Using Nonbinary Input Vectors," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 1423–1429, Jan. 2024, https://doi.org/10.1109/TNNLS.2022.3180197.

[10] A. Gohr, "Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning," in *Advances in Cryptology – CRYPTO 2019*, 2019, pp. 150–179, https://doi.org/10.1007/978-3-030-26951-7_6.

[11] K. D. Pandl, S. Thiebes, M. Schmidt-Kraepelin, and A. Sunyaev, "On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda," *IEEE Access*, vol. 8, pp. 57075–57095, 2020, https://doi.org/10.1109/ACCESS.2020.2981447.

[12] A. Benamira, D. Gerault, T. Peyrin, and Q. Q. Tan, "A Deeper Look at Machine Learning-Based Cryptanalysis," in *Advances in Cryptology – EUROCRYPT 2021*, 2021, pp. 805–835, https://doi.org/10.1007/978-3-030-77870-5_28.

[13] I. Amir, H. Suhaimi, R. Mohamad, E. Abdullah, and C. H. Pu, "Hybrid encryption based on a generative adversarial network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 2, Aug. 2024, Art. no. 971, https://doi.org/10.11591/ijeecs.v35.i2.pp971-978.

[14] J. W. Lee *et al.*, "Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network," *IEEE Access*, vol. 10, pp. 30039–30054, 2022, https://doi.org/10.1109/ACCESS.2022.3159694.

[15] A. A. Hussain and F. Al-Turjman, "Artificial intelligence and blockchain: A review," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, Sept. 2021, Art. no. e4268, https://doi.org/10.1002/ett.4268.

[16] A. Sarkar, "A symmetric neural cryptographic key generation scheme for Iot security," *Applied Intelligence*, vol. 53, no. 8, pp. 9344–9367, Apr. 2023, https://doi.org/10.1007/s10489-022-03904-7.

[17] R. T. Elmaghraby, N. M. Abdel Aziem, M. A. Sobh, and A. M. Bahaa-Eldin, "Encrypted network traffic classification based on machine learning," *Ain Shams Engineering Journal*, vol. 15, no. 2, Feb. 2024, Art. no. 102361, https://doi.org/10.1016/j.asej.2023.102361.

[18] N. Kshetri, M. M. Rahman, M. M. Rana, O. F. Osama, and J. Hutson, "algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography – A Comparative Analysis in AI Era," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 12, 2024, https://doi.org/10.14569/IJACSA.2024.0151201.

[19] S. Pramanik *et al.*, "A Novel Approach Using Steganography and Cryptography in Business Intelligence:," in *Advances in Business Information Systems and Analytics*, A. Azevedo and M. F. Santos, Eds. IGI Global, 2021, pp. 192–217.

[20] D. Dai and S. Boroomand, "A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges," *Archives of Computational Methods in Engineering*, vol. 29, no. 2, pp. 1291–1309, Mar. 2022, https://doi.org/10.1007/s11831-021-09628-0.

[21] M. N. Al-Suqri and M. Gillani, "A Comparative Analysis of Information and Artificial Intelligence Toward National Security," *IEEE Access*, vol. 10, pp. 64420–64434, 2022, https://doi.org/10.1109/ACCESS.2022.3183642.

[22] A. A. Pise *et al.*, "Enabling Artificial Intelligence of Things (AIoT) Healthcare Architectures and Listing Security Issues," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–14, Aug. 2022, https://doi.org/10.1155/2022/8421434.

[23] S. B. Hegde, S. Srivastav, and N. B. Ks, "A Comparative study on state of art Cryptographic key distribution with quantum networks," in *2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT)*, Oct. 2022, pp. 1–7, https://doi.org/10.1109/GCAT55367.2022.9971870.

[24] H. Taherdoost, T. V. Le, and K. Slimani, "Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review," *Cryptography*, vol. 9, no. 1, Mar. 2025, Art. no. 17, https://doi.org/10.3390/cryptography9010017.

[25] K. Kumar, S. Tanwar, and S. Kumar, "Deep-Learning-based Cryptanalysis through Topic Modeling," *Engineering, Technology &*

Applied Science Research, vol. 14, no. 1, pp. 12524–12529, Feb. 2024, https://doi.org/10.48084/etasr.6515.

[26] A. Saini and R. Sehrawat, "An intelligent and efficient CNN-AES framework for image block encryption with a multi-key approach," *Engineering Research Express*, vol. 7, no. 1, Mar. 2025, Art. no. 015206, https://doi.org/10.1088/2631-8695/ada3af.

[27] U. Rawat, Abhishek, H. Singh, and A. Ur Rehman, "Cybersecurity Challenges and Risks in AGI Development and Deployment," in *Artificial General Intelligence (AGI) Security*, S. El Hajjami, K. Kaushik, and I. U. Khan, Eds. Springer Nature Singapore, 2025, pp. 291–314.

AUTHORS PROFILE

Mohammed A. Abdewi obtained his B.Sc. from AL-Anbar University and his M.Sc. from Alexandria University. He is currently a PhD researcher at Al-Azhar University, Faculty of Science.

Ali Farouk Emara received his B.Sc. in Pure Math and Computer Science from the Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt, in 2008. He received an M.Sc. in quality-of-service management in mobile cloud computing from the Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt, in 2016. In 2022, he received a Ph.D. in Efficient Schemes for Data and Resources Management in Mobile Cloud Computing from the Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt. He is currently working as an Assistant Professor in the Computer Science Department, Faculty of Science, Al-Azhar University, Cairo, Egypt.

Ashraf A. Gouda is an Assistant Professor in Computer Science at Al-Azhar University. He holds a Ph.D. in Computer Science from the Budapest University of Technology and Economics, Hungary (2005). His research interests include physics-informed neural networks, AI, IoT, quantum machine learning, quantum computing, and optimization techniques.

Mohammed Abdel Razek is a Professor in Computer Science at Al-Azhar University. He holds a Ph.D. in Computer Science and Artificial Intelligence from the University of Montreal, Canada (2004). His research focuses on AI techniques in e-learning, medicine, cybersecurity, and IoT. He has published more than 80 papers and served as an editor/reviewer for various journals and conferences.