AL-AASAR Journal
Quarterly *Research Journal*
www. al-aasar.com/

Vol. 2, No. 1 (2025)

Online ISSN: 3006-693X
Print ISSN: 3006-6921

AN IN-DEPTH COMPARATIVE ANALYSIS OF TRADITIONAL VS AI-ENHANCED ENCRYPTION ALGORITHMS

Aftab Ahmad[1], Abid Ur Rehman[2], Muhammad Usman Ghani[1], Fawad Nasim[1], Suhaib Naseem[1]

[1]Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
[2]RIPHAH International University, Islamabad

Abstract

This research captures a detailed analysis of the conventional cryptographic techniques and the relatively recent artificial intelligence encryption techniques. Exploring the historical development of encryption and the supplementation of artificial intelligence (AI) applied to cryptography, this paper discusses how AI enriches flexibility, sophistication, and predictive functionalities. Further, the research assesses different encryption methods to identify their security effects, the current development in key management, and the computational complexity. A comparative evaluation of the effectiveness, safety, and susceptibility of using conventional and artificial intelligence-based methods to quantum computing and crypt-analysis breakthroughs is conducted. Therefore, this study seeks to fill the existing research gap of the application of AI and its impact on next-generation cryptography for cyber security.

Keywords:
AI-driven encryption, Cyber security, Crypt-analysis, Key management, Quantum-resistant cryptography, Traditional cryptographic algorithm

1. Introduction:

Encryption is switching readable data (plaintext) into a hidden code (ciphertext) so that your information will be only available in the hands of individuals with permission to have it. This entails using algorithms and keys to make data unreadable except if there is the correct key. Encryption is a fundamental mechanism for protecting sensitive information from unauthorized disclosure, data breaches, and cyber threats [1]. Data integrity, confidentiality, and authenticity are cornerstone attributes of modern cyber security demands, protecting data critical across finance, healthcare, and communication domains [2].

Encryption is critical in ensuring our data is protected, and it can protect our data as it sits, in transit, and the process. This is what encryption does; for example, in e-commerce transactions, the process of the fact that credit card information should remain confidential while it is transmitted on the internet. In secure messaging applications, end-to-end encryption ensures that the messages between users are only accessible to the users mutually in communication. While it's true that cyber threats are evolving, encryption still remains a tool that warms the hands of the risks of data interception, identity theft, and unauthorized data modification [3].

Cryptography has a history going back thousands of years, with Roman and Greek illustrations of simple ciphers used to secure sensitive information. The second substitution cipher switched the letters of the alphabet by a fixed number of places, at least to break the message to the unintended recipients. These early methods were quite rudimentary compared to today's standards, but they did establish the groundwork for the later development of more complex cryptographic systems[4].

AL-AASAR Journal
Quarterly Research Journal
www. al-aasar.com/
Vol. 2, No. 1 (2025)
Online ISSN: 3006-693X
Print ISSN: 3006-6921

As the digital age approaches, cryptographic methods are now adapted to secure digital data. In the 1970s, public key cryptography was developed, including what we consider the most commonly used form known as the RSA algorithm, with asymmetric keys—one for encryption, and another for decryption. This breakthrough solved the problems of secure key distribution and secure network-based communication over an untrusted network, which is the Internet. Further strengthening digital data security are modern cryptographic algorithms such as the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) which have become robust against the more sophisticated cyber threats.

Cryptography is now everywhere — from the encryption of sensitive files on personal devices to the use of Secure Sockets Layer (SSL)/Transport Layer Security (TLS) in web browsers. With digital infrastructure becoming more and more necessary in society, cryptography's role continues to grow in the privacy and/or security of data in cloud storage, online banking, and many more things [5]. An ever-evolving process in response to the need to battle developing road agents, like quantum computing, which could threaten traditional cryptography mechanisms.

Encryption is a major aspect of the modern cyber security model since it renders all the information confidential over different digital platforms. With emerging, and increasingly sophisticated cyber threats, encryption is essentially a fundamental mechanism to protect data from unauthorized access. Encryption takes data and makes it hard to read in such a way that if a malicious actor were to pick it up, it still can't be read without the correct decryption key. Among those, the financial, healthcare care, and government industries are particularly sensitive to data leakage, especially since the leakage of such data may result in huge financial losses and legal liabilities and undermine the public trust.

In addition, encryption produces data integrity by ensuring data is unaltered at storage or transmission. That's done through cryptographic methods, which create different signatures for the data so that systems can tell that the data is tampered with by something other than it should be. In reference to banking and even online commerce, the importance of integrity in keeping data accurate and reliable is vital because it can mean fraud charges and massive issues resulting from wrong information. It also has an important role in encrypting communications of users across public networks like the Internet by protecting the user-to-server and server-to-user exchanges from traffic interception and tampering.But all of this user authentication and verification of trust of the flow of money in the digital world is going to need encryption. Today's modern cyber security frameworks involving encryption, which implement secure authentication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL), encryption for data sent between a user and a website. Defenders have heads up to prevent attackers from eavesdropping – gaining login credentials, credit card numbers, and personal data – so that when you go online, you are in a secure environment. Encryption functions to build trust in digital communications and consequentially, inter alia, to e-commerce, and wider digital economy development.Furthermore, encryption is an imperative prerequisite to meeting data privacy laws and regulations like the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA)[6]. Those organizations are on the hook for putting the risk of user privacy breach because the regulations have strong encryption procedures to secure personal and sensitive data. By encrypting the data and embedding encryption into the cyber security framework, organizations can show they are

Vol. 2, No. 1 (2025)
Online ISSN: 3006-693X
Print ISSN: 3006-6921

legally shielded, and strengthen their reputation as a custodian of some of the world's most important data. A must have tool in the modern cyber security arsenal; encryption will change in response to evolving cyber threats.

Emergence of AI in Cryptography

Artificial Intelligence (AI) integration into cryptographic processes represents a major development within cyber security [7]. Static encryption software uses predefined algorithms alongside standby key systems to protect data from ordinary attacks but their rigid structure creates predictable patterns off which attackers can capitalize. AI-introduced adaptive qualities allow cryptographic processes to produce dynamic system reactions against their threatening environment. Flexible security approaches remain essential because today's fast digital landscape features advanced evolving cyber threats. AI can be used to combine crypto systems potential vulnerability prediction with proactive action for mitigating risks live.

Key management is one of the most transformative aspects that AI in cryptography can do. Manual processes involved in traditional key management practices are prone to human error and inefficiencies. AI can automate all this and more—a machine learning model can predict the best rotation schedule of a set of keys and detect potential breaches prior to their happening. As a result, it makes the key management system more secure and more efficient, hence minimizing the lifecycle vulnerabilities that normally come with static key management[8]. AI-driven encryption systems can also adapt encryption strategies in real-time, in response to real-time threat analysis, so that sensitive data is protected under changing threat conditions.

Additionally, AI also plays its part when it comes to creating more and more powerful algorithms when it comes to cryptographic processes. To the extent that such evasion techniques, such as neural networks and generative adversarial networks (GANs), can be used to produce robust encryption keys and algorithms resistant to brute force and cryptanalytic attack, evasion is possible. The AI-generated encryption schemes are more unpredictable and harder for attackers to attack, which boosts the security posture of the system in general. In addition, AI can have its capability to respond to new and unforeseen cryptographic challenges increased by continuously learning from previous security events.

AI transforms encryption through predictive methods that identify security risks seamlessly while they emerge rather than permitting them to shape security breaches. By examining vast quantities of data, AI systems become able to detect recurrent patterns associated with future cryptographic assaults, whether they involve side channel analysis or attempt to extract encryption keys. Advanced encryption models help defense against threats by combining predictive analysis which adjusts configurations automatically while protecting against 10 times more attack vectors. Using predictive analytics organizations can better manage both key lifecycle duration and rotation schedules to ensure keys stay secure alongside being up-to-date[9]. These integrated AI processes deliver enhanced platform security through edge devices when feasible, minimizing the operational requirements for maintaining cryptographic systems while managing increasingly sophisticated cyber security threats.

Objective

In this comparative analysis, we plan to compare traditional cryptographic algorithms (e.g., AES and RSA) and AI-encrypted algorithms. The second one proposes to solve AI's role in enhancing encryption resilience against contemporary cryptographic attacks. It examines the

AL-AASAR Journal
Quarterly Research Journal
www. al-aasar.com/
Vol. 2, No. 1 (2025)
Online ISSN: 3006-693X
Print ISSN: 3006-6921

vulnerabilities offered to both conventional and enhanced AI encryption by quantum computing.

Research question

1. How does AI-Driven encryption improve key management and security compared to Traditional Encryption methods?
2. What are the potential threats posed by quantum computing to traditional and AI-driven encryption?

2. Traditional Cryptographic Methods

The Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) stand as fundamental cryptographic algorithms that satisfy separate functionality requirements. AES represents a symmetric encryption algorithm that emerged in 2001 to succeed DES for encrypting large datasets while earning recognition for its encryption capabilities. Its operation combines fixed block sizes of 128 bits while providing key length options between 128, 192, and 256 bits to adapt to varying cryptographic demands. On the other side, the RSA, developed in 1977, is an asymmetric encryption algorithm that uses a public/private key pair, which is the optimal key exchange and digital signature. One of the fundamental elements driving RSA security is the computational difficulty of prime factorization; in contrast, AES security rests on substitution permutation networks' resistance to cryptanalysis. Together, these algorithms have developed so that today they are the architecture of modern cryptographic systems, and the AES is used for data encryption and RSA as part of key management and secure communication in hybrid encryption[10].

Table 1: Studies and their key focus

Year	Title	Author	Key focus
2019	A survey on AES Cryptographic Algorithm	Smith, J. & Kumar, R	AES algorithm, focusing on its implementation, strengths and flaws
2019	RSA cryptography: A survey of attacks and mitigations	L. Zhang, P. Patel	Analysis of strategies improving security and various attacks on RSA
2020	Analysis of advanced encryption standard AES	Tan, C., Lee, J. & Zhang, M	Examine AES security and performance factors
2020	Hybrid cryptographic systems for IOT	Patel, V., Singh, S.	Integrating AES and RSA in IOT devices, analyzing security and performance.
2021	Post-Quantum RSA: A new cryptographic approach	H. Zhang, Y. Wang	Impact of quantum computing on RSA and proposed quantum-resistant approaches
2022	Breaking down RSA: Attacks and Security Enhancements	L. Zhao, Y. Chen	Approaches to mitigate vulnerabilities in RSA

Online ISSN: 3006-693X
Print ISSN: 3006-6921

2023	Enhancing AES with Block-chain for secure Data transmission	S. Roy, A. Verma	Combining AES approaches with block-chain technology and proposed hybrid approach
2024	Security implications of classical cryptography in the age of Quantum computing	Michael Green, Sarah Blue	Impact of quantum computing on traditional cryptographic systems

3. Overview of AI AI-based approaches

Encryption powered by artificial intelligence (AI) and machine learning (ML) methods stimulates the implementation of AI and ML into cryptographic processes that lead to dynamic, adaptive, and self-adaptive encryption systems. As opposed to static encryption algorithms that rely on predetermined rules, AI-based encryption constantly develops as it learns to write patterns, notice potential dangers to the system, and optimize its procedures. These techniques can be broadly categorized into two types: AI applied to cryptographic algorithms to enhance or improve these (e.g., adaptive key management, threat prediction) and AI-based created encryption (e.g., independently generated unique key structure, cipher text representation). These security systems also rely on predictive analytics, anomaly detection, and autonomous decision-making to predict and defeat emerging security threats quickly and in real-time[11].

3.1 Neural Network-Based Encryption:

Both the generation of secure complex keys and the encoding of data patterns are within the purview of AI-driven encryption, and as such, neural networks play a dominant role here. For instance, neural networks can learn to encode data into encrypted formats that cannot be decrypted, except by another corresponding neural network. At a high level, it guarantees that attackers cannot understand this data without a trained decryption model. Most of these approaches employ deep learning architectures, like autoencoders, where it is the encoder that generates the cipher text, and the decoder as it tries to reconstruct the plaintext. Moreover, neural networks can learn the attack patterns and adjust crypt parameters based on them so that the system can reconfigure the encryption parameters with or without human supervision, thus increasing its security and flexibility[12].

3,2 Generative Adversarial Network (GAN)-Based Encryption:

Another fancy application of AI-powered encryption is called Generative Adversarial Networks (GANs). GANs consist of two competing neural networks: a generator, and a discriminator. The generator generates encrypted data in the context of encryption, and the discriminator tries to find some patterns or vulnerabilities in the cipher text. In contrast, the GAN framework is adversarial, enabling the generator to learn to generate increasingly resilient cipher text to any decryption attempts of the discriminator [13]. This self-improving system can withstand advanced cryptanalytic methods and thus be more resilient to attacks. As an encryption scheme with the property of generating unpredictable cipher text, GAN-based encryption has been considered for use in secure communication protocols, maintaining itself as an effective defense against brute force and pattern-based attacks.

AL-AASAR Journal
Quarterly *Research Journal*
www. al-aasar.com/

Vol. 2, No. 1 (2025)

Online ISSN: 3006-693X
Print ISSN: 3006-6921

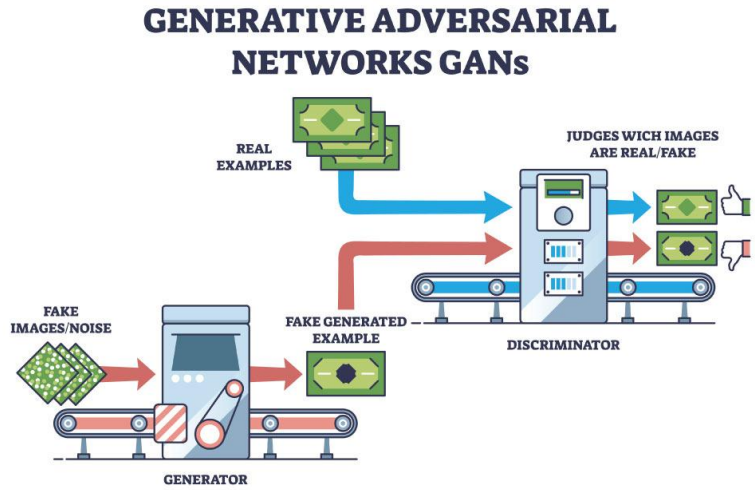

Fig 1 Generative Adversarial Network (GAN)-Based Encryption

Artificial intelligence (AI) brings automation, complexity, and adaptability to traditionally static cryptographic processes, thus effectively improving the creation and management of encryption keys. To obtain encryption keys that are more random and harder to predict by an adversary than those generated by more traditional cryptographic algorithms, AI methodologies, especially machine learning (ML) models, can be used. For example, recent advances in AI training, such as neural networks, are now capable of generating pseudo-random key sequences that are difficult to reproduce and do so in the context of dynamic threats evolving (in accordance with the actual threat landscape).

Taking the output of machine learning algorithms that can take thousands or millions and even more data of known key patterns and applying learned behavior to output super complex key sequences dramatically increases the strength of encryption schemes and the resistance to brute force or cryptanalytic attacks. Supervised learning models like machine learning can be used to extract patterns (T0) in cryptogram operations to detect categorical frails to encryption schemes [14]. With training on historical data pertinent to encryption algorithms and attack patterns, machine learning models will unearth hidden vulnerabilities that might otherwise evade us. As a simple example, neural networks can look at how different key sequences work together in terms of dealing with a specific type of data or of an encryption operation and whether correlations can be found that make the encryption more vulnerable to attacks.

Table 2: Previous five years working of AI-Driven Encryption

Year	**Title**	**Author**	**Key focus**
2019	AI-Driven cryptographic key generation	Smith, J., Patel, R.	Machine learning algorithms to improve the generation and management.
2020	Neural network-based Encryption Algorithm	Zhang, H., Li, W.	Analyze the use of deep neural networks to design encryption.

Online ISSN: 3006-693X
Print ISSN: 3006-6921

2020	AI and Quantum Cryptography: An overview	Chen, X., Zhao, Q.	How AI can support quantum-resistant encryption methods
2021	Generative Adversarial Networks in cryptography	Park, J., Lee, M.	Analyze GANs for the generation of new encryption keys and algorithms.
2022	AI for secure data sharing in cloud	Gupta, S., Sharma, P	AI- based solutions for ensuring secure data sharing and encryption in cloud storage environments.
2023	Neural cryptanalysis and AI-based security	Robinson, T., Tan, Y.	Research evaluates how Artificial Intelligence builds innovative analysis techniques for cryptographic systems and develops secure cryptographic protocols.
2024	AI-Driven Homomorphic Encryption	Zhang, Y., Zhao, L.	Research into artificial intelligence methods that optimize the scalability and efficiency qualities of homomorphic encryption systems.

4. Comparative Analysis

Traditional cryptographic methods based on AES and RSA benefit from secure mathematical frameworks to achieve reliable performance and efficient calculations while supporting numerous hardware platforms. These algorithms maintain high efficiency and compact performance, but their static design makes them vulnerable to upcoming quantum computing threats and advanced crypto logical attacks. Artificial Intelligence empowers contemporary encryption through neural processing and machine intelligence that builds adaptive security patterns responding to active threats. Training AI-based encryption techniques initially experience significant computational strain, leading to their dynamic threat-learning potential that yields resilient security. Customer trust grows from black-box operation within these frameworks although it introduces explanation uncertainties that necessitate GPU or TPU device use.

4.1 Complexity and Performance

The integration of security requirements with available processing capabilities determines whether organizations choose between traditional encryption processes and systems that use AI. To determine the value of future threat-blocking capabilities enabled through AI technology, we need to weigh them against AI's resource-intensive requirements and system limitations. Establishing cryptographic systems requires operators to balance secure functionality with maintaining efficient performance capabilities. Here's a bar chart comparing traditional and AI-driven encryption methods in terms of computational complexity, processing overhead, and performance efficiency.

AL-AASAR Journal
Quarterly *Research Journal*
www. al-aasar.com/

Vol. 2, No. 1 (2025)

Online ISSN: 3006-693X
Print ISSN: 3006-6921

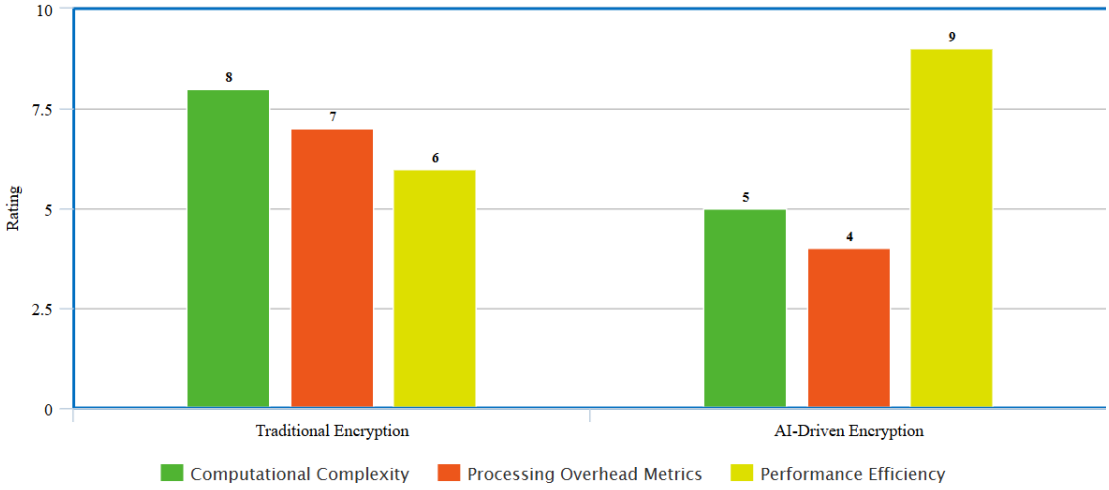

Fig 2 Comparing Traditional Encryption and AI-driven encryption across three metrics: Computational Complexity, Processing Overhead, and Performance Efficiency

The chart compares Traditional Encryption and AI-Driven Encryption across three metrics: Computational Complexity, Processing Overhead, and Performance Efficiency. The high complexity of traditional encryption algorithms (8) paired with their heavy processing requirements (7) stands in contrast to AI-driven encryption, which performs better in those metrics (5 and 4) because of its dynamic operating capabilities. The performance efficiency evaluation of AI-driven encryption reaches a score of 9 compared to traditional methods 6 this demonstrates it's potential to enhance operations and boost throughput while offering efficient and scalable security solutions for current requirements.

4.2 Critical evaluation of security

The main focus is on the data confidentiality, integrity, and identity factors that data are most vulnerable to during a breach with traditional encryption versus AI-driven encryption. As well-established, traditional encryption methods such as the Advanced Encryption Standard (AES) use complex algorithms resistant to known cryptographic attacks while still providing strong confidentiality by encrypting data. However, the algorithms they implement are fixed and will be susceptible to weaknesses if key management is not done correctly. Both also impose limits to scalability as traditional encryption for large amounts of data can consume a lot of computational resources. On the other hand, by utilizing AI and machine learning to predict and counter new attack vectors in real time, AI-driven encryption waters down these due to adaptive and dynamic encryption mechanisms. It makes the resistance to breach more by continuously learning from emerging threats. Yet, the complexities may bring vulnerabilities to the underlying AI models, potentially exploited or attacked if those models are not sufficiently defended. AI-driven encryption offers more flexibility and greater resilience against new kinds of attacks, but its security is highly dependent on AI models that train data quality. The strength of these approaches is both, but a combination of AI-based encryption may be able to resist farther evolving threats at the trade of increased complexity and risks.

AL-AASAR Journal
Quarterly Research Journal
www. al-aasar.com/
Vol. 2, No. 1 (2025)
Online ISSN: 3006-693X
Print ISSN: 3006-6921

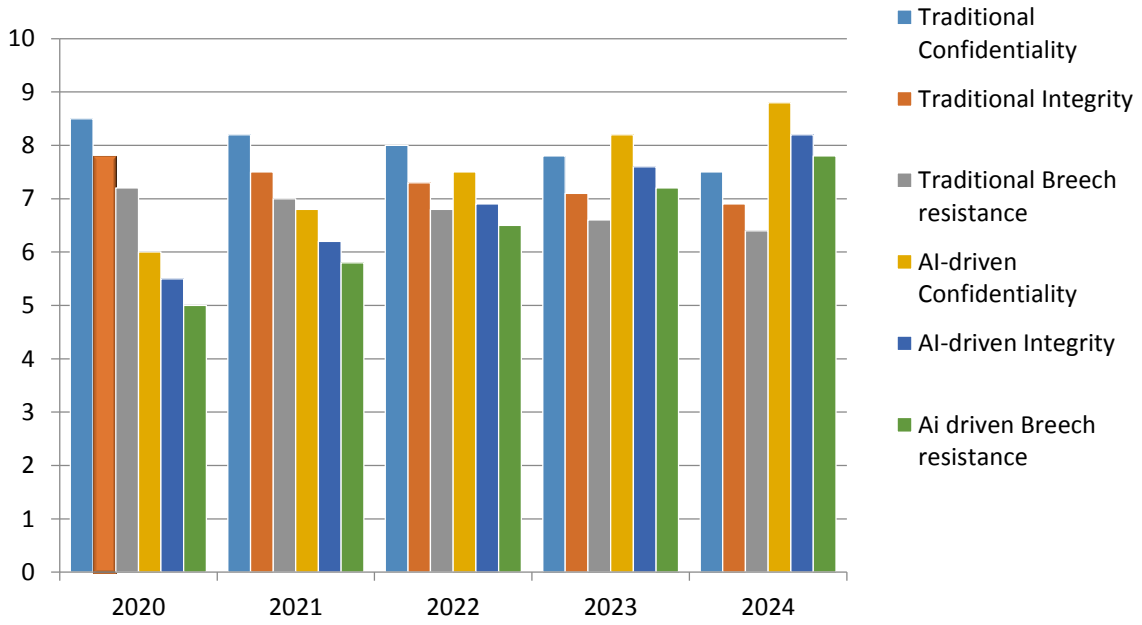

Fig 3 Traditional and AI-driven encryption security across Data Confidentiality, Integrity and Breech Resistance

The chart shows that traditional and AI-driven encryption methods have become more assertive and weaker in security across data confidentiality, integrity, and resistance to breaches between 2020 and 2024. Traditional encryption's confidence and integrity appear stronger in the early years, while AI-driven encryption improves steadily over time—more so in breach resistance. By 2025, AI-driven encryption will outline two of the three categories ahead of traditional methods, which may presage a future of encryption that is not quite so antiquated.

4.3 Analysis of Potential Threats Posed by Quantum Computing to Traditional and AI-Driven Encryption

The implementation of quantum computing creates substantial threats to contemporary encryption systems and AI encryption because it breaks classical key-exchange algorithms alongside hash function protocols. AI encryption has adjustable power yet quantum attack techniques generate vulnerabilities against this approach. The future security of critical systems requires implementing both post-quantum cryptography systems and quantum-secure Artificial Intelligence techniques to counter these advancing threats.

Table 3 Potential Threats Posed by Quantum Computing to Traditional and AI-Driven Encryption

Threat	Traditional Encryption	AI-Driven Encryption	Mitigation strategy
Key Cracking	Shor's algorithm successfully cracks RSA, ECC, and DH key exchanges so they must be	Extensive encryption models supported by AI can use quantum-resistant techniques	Extensive encryption models supported by AI can use quantum-resistant techniques

AL-AASAR Journal
Quarterly *Research Journal*
www. al-aasar.com/

Vol. 2, No. 1 (2025)

Online ISSN: 3006-693X
Print ISSN: 3006-6921

	discarded from cryptographic use.	yet their weak configuration remains susceptible to attacks.	yet their weak configuration remains susceptible to attacks.
Grover's Algorithm	The algorithm removes half of the strength from symmetric encryption thus making AES and SHA-based hash functions less secure.	Current integration methods based on traditional hash-based checks become vulnerable more quickly when AI-driven encryption is used.	Current integration methods based on traditional hash-based checks become vulnerable more quickly when AI-driven encryption is used.
Side-Channel Attacks	Traditional cryptographic methods remain susceptible to data analysis capabilities grown from quantum computing technology.	Encryption data managed through AI systems can face attacks which adversarial quantum systems make possible.	Encryption data managed through AI systems can face attacks which adversarial quantum systems make possible.
Machine Learning Model Tampering	Artificial intelligence security algorithms partner with traditional encryption to protect networks but these combinations remain susceptible to manipulation	Adversarial attacks propelled by quantum computation show potential to both hasten AI attacks against models as well as evince effect on authentication methods	Adversarial attacks propelled by quantum computation show potential to both hasten AI attacks against models as well as evince effect on authentication methods
Quantum Decryption speed	Encryption algorithms such as RSA and AES will experience an exponential speedup making decryption possible more easily.	Models employing artificial intelligence for encryption which use traditional cryptography remain exposed to decryption risks.	Models employing artificial intelligence for encryption which use traditional cryptography remain exposed to decryption risks.

Vol. 2, No. 1 (2025)
Online ISSN: 3006-693X
Print ISSN: 3006-6921

5. Future directions

1. The next research should be an integration of AI driven encryption with the post quantum cryptographic methods to increase the resistance against quantum computing threats. It embraces developing hybrid encryption models that make use of AI for adaptive key management together with using quantum secure algorithms like lattice-based cryptography.
2. It should also improve the optimization of real time threat detection from an AI enhanced encryption system and dynamic encryption adjustments.
3. Future works can outspread the knowledge of using deep learning models for constantly monitoring encryption vulnerabilities and automatically reconfigure security limits to counter developing cyber threats.

6. Conclusion

The particular achievements of this research are to outline the comparative strengths and weaknesses of traditional encryption and AI cryptographic techniques. AES and RSA are still the bread and butter of encryption, but they are also getting more and more exposed to the continuous evolution of wicked threats and advances in quantum computing. Aloud to the evolution of the internet and the emergence of ever new threats, encryption developed to be set adaptable to all those new threats and predictive, which bring adaptability and predictive security, both for key management and real-time threat mitigation. Challenges with AI driven methods includes computational complexity and potential adversarial attacks. Featured in the study is the alarming rising risk of quantum encryption requiring quantum resistant encryption. The future crypto currency advancements should be across the hybrid models that combine AI with post quantum-based algorithms. Furthermore, encryption of AI will need to be optimized for real time threat detection in secure digital infrastructures. If dynamic nature of AI-driven encryption is to be put to use, it has to be thoroughly tested and standardized. However, cyber threats are advancing, and it is highly likely that AI will come to the fore to enhance the power of encryption against such sophisticated attacks. Thus, this study will help develop future research and implementation strategies in the ongoing discourse about next generation cryptographic security.

7. References

1. Imtiaz, A., Shehzad, D., Nasim, F., Afzaal, M., Rehman, M. and Imran, A., 2023, November. Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems. In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 1-7). IEEE.
2. Zainab, H., Khan, A.R.A., Khan, M.I. and Arif, A., 2025. Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases. Global Trends in Science and Technology, 1(1), pp.63-74.
3. Farooq, Muzammal, Rana M. Faheem Younas, Junaid Nasir Qureshi, Ali Haider, and Fawad Nasim. "Cyber security Risks in DBMS: Strategies to Mitigate Data Security Threats: A Systematic Review." Spectrum of engineering sciences 3, no. 1 (2025): 268-290.
4. Bamotra, A. (2022). Cryptography and Its Techniques: a Review. *Journal Punjab Academy of Sciences Jpas*, *22*(1), 2022. www.jpas.in

Online ISSN: 3006-693X
Print ISSN: 3006-6921

5. Arunkumar, B., & Kousalya, G. (2022). Secure and light weight elliptic curve cipher suites in SSL/TLS. *Computer Systems Science and Engineering*, *40*(1), 179–190. https://doi.org/10.32604/CSSE.2022.018166

6. Lee, T. F., Chang, I. P., & Su, G. J. (2023). Compliance with HIPAA and GDPR in Certificateless-Based Authenticated Key Agreement Using Extended Chaotic Maps. *Electronics (Switzerland)*, *12*(5), 1–20. https://doi.org/10.3390/electronics12051108

7. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3(4), 566-578.

8. Blackledge, J., & Mosola, N. (2020). Applications of Artificial Intelligence to Cryptography. *Transactions on Machine Learning and Artificial Intelligence*, *8*(3), 21–60. https://doi.org/10.14738/tmlai.83.8219

9. Badar, Muhammad Aqeel, Fakhar Ur Rehman, Javeed Ali, Fawad Nasim, and Hijab Sehar. "PREDICTIVE MODELING OF CARDIOVASCULAR DISEASE US-ING MACHINE LEARNING." Contemporary Journal of Social Science Review 2, no. 04 (2024): 1467-1481.

10. Singh, P., & Kumar, S. (2017). Study & analysis of cryptography algorithms : RSA, AES, DES, T-DES, blowfish. *International Journal of Engineering & Technology*, *7*(1.5), 221. https://doi.org/10.14419/ijet.v7i1.5.9150

11. Yusuf, S. O., Echere, A. Z., Ocran, G., & Abubakar, J. E. (2024). *Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs*. *September*. https://doi.org/10.30574/wjarr.2024.23.3.2753

12. Yayik, A., & Kutlu, Y. (2014). Neural Network Based Cryptography. *Neural Network World*, *24*(2), 177–192. https://doi.org/10.14311/nnw.2014.24.011

13. Li, M. (2024). *Application of GAN-Based Data Encryption Technology in Computer Communication System*. *48*, 17–34.

14. Muthyalac, S., & Reddy, P. (2024). *Ai-Driven Cloud Access Control and Authorization Using Attribute-Based Encryption*. *August 2022*.