algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography – A Comparative Analysis in AI Era

Naresh Kshetri[1], Mir Mehedi Rahman[2], Md Masud Rana[3], Omar Faruq Osama[4] and James Hutson[5]
Department of Cybersecurity, Rochester Institute of Technology, NY, USA[1]
School of Business and Technology, Emporia State University, KS, USA[2]
Department of Information Technology, San Juan College, NM, USA[3]
Dept. of System Science & Ind. Eng., Binghamton Univ., SUNY, NY, USA[4]
Department of Art History, AI & Visual Culture, Lindenwood University, MO, USA[5]

***Abstract*—The increasing integration of artificial intelligence (AI) within cybersecurity has necessitated stronger encryption methods to ensure data security. This paper presents a comparative analysis of symmetric (SE) and asymmetric encryption (AE) algorithms, focusing on their role in securing sensitive information in AI-driven environments. Through an in-depth study of various encryption algorithms such as AES, RSA, and others, this research evaluates the efficiency, complexity, and security of these algorithms within modern cybersecurity frameworks. Utilizing both qualitative and quantitative analysis, this research explores the historical evolution of encryption algorithms and their growing relevance in AI applications. The comparison of SE and AE algorithms focuses on key factors such as processing speed, scalability, and security resilience in the face of evolving threats. Special attention is given to how these algorithms are integrated into AI systems and how they manage the challenges posed by large-scale data processing in multi-agent environments. Our results highlight that while SE algorithms demonstrate high-speed performance and lower computational demands, AE algorithms provide superior security, particularly in scenarios requiring enhanced encryption for AI-based networks. The paper concludes by addressing the security concerns that encryption algorithms must tackle in the age of AI and outlines future research directions aimed at enhancing encryption techniques for cybersecurity.**

***Keywords*—Algorithms; analysis; artificial intelligence; asymmetric encryption; cryptography; cybersecurity; symmetric encryption**

I. Introduction

Algorithms are and were always the driving force behind cryptography and cybersecurity as we are marching towards the artificial intelligence (AI) and machine learning era. Several countermeasures, techniques, and cybersecurity practices are popular with the use of machine learning and deep learning algorithms apart from AI algorithms [1-2]. As we know cybersecurity combines information security and network security, the annual number of data breaches is growing every year. Loss of private information, malware attacks, use of smart gadgets, growing number of internet population, and several others are upcoming challenges for cryptography algorithms.

Vulnerabilities and attacks on ciphers, private keys, and algorithms are increasing as we are considering "Security for AI" and vise-versa [3-4]. New and unexpected attacks, development of several frameworks and tools are going on as we discuss various encryption algorithms. From the initial use of symmetric algorithms like Data Encryption Standard (DES), and their several weaknesses we tend to know that hackers are exploiting the powerful algorithms (like SHA3, MD5, up to CRYSTALS) today. The use of "secret key" in symmetric algorithms (although asymmetric works a little better as compared to symmetric) is no longer secret as attackers have successfully compromised the key in both symmetric and asymmetric algorithms.

The emergence of AI has revolutionized cybersecurity, providing adaptive and dynamic encryption techniques to combat swiftly changing cyber threats [1]. AI-driven methodologies have enhanced encryption systems' resilience, facilitating real-time identification of anomalies and threats that conventional methods find challenging to spot [2]. The use of AI, especially via machine learning (ML) and deep learning (DL) algorithms, has markedly improved the efficacy of encryption methods, rendering them more adept at managing the increasing complexity and volume of contemporary data environments.

AI is becoming more and more integrated into cybersecurity and encryption as technology advances. AI is essential for protecting AI systems from complex cyberattacks, in addition to fortifying encryption procedures by streamlining key generation and data security techniques [3]. In an increasingly linked and insecure digital world, the synergy between AI and encryption is essential because it allows more effective, scalable, and proactive security measures, guaranteeing the security of both data and AI systems [4].

This paper is structured as follows to explore the comparative analysis of encryption algorithms and their relevance in modern cybersecurity, particularly in the AI era. Section II provides a background study, outlining the historical evolution and challenges of cryptographic algorithms, and establishing the role of AI in enhancing these methods. Section

III examines the technical aspects of various encryption algorithms, focusing on their contributions to safeguarding sensitive data in complex systems. Section IV offers a comparative analysis of symmetric encryption (SE) and asymmetric encryption (AE), highlighting key differences in terms of efficiency, security, and scalability. Section V discusses the role of AI in transforming encryption practices, focusing on how AI enhances real-time adaptability, tackles emerging threats, and enables personalized encryption strategies. Section VI focuses on the security challenges encryption faces in modern society, particularly against emerging cyber threats. Section VII presents the discussion and conclusions, summarizing the insights gained from the comparative analysis and suggesting improvements for existing encryption techniques. Lastly, Section VIII outlines the future scope of research, discussing potential advancements in encryption algorithms and their application in AI-driven cybersecurity solutions.

II. Background Study

The foundation of contemporary encryption methodologies is well-examined in the literature, providing critical insights into their application in AI-driven contexts. Kapoor and Thakur [5] offer a thorough comparative analysis of symmetric and asymmetric key algorithms, underscoring the growing importance of encryption in safeguarding digital information in an increasingly networked environment. Their analysis highlights the superiority of asymmetric encryption, which employs two keys to enhance security through mathematical complexity. For symmetric algorithms, they emphasize the adaptability and efficiency of the Advanced Encryption Standard (AES), particularly its resilience against common attacks and its rapid execution speed. In contrast, the authors identify Elliptic Curve Cryptography (ECC) as the most secure asymmetric technique, noting its reliance on the algebraic properties of elliptic curves and finite fields. This detailed examination is a vital reference for algoTRIC, as it informs the optimization of AES and ECC within its architecture for large-scale, multi-agent systems. By focusing on trade-offs between speed and security resilience, the paper addresses critical challenges in mitigating emerging cyber threats.

Building on this foundation, Soomro et al. [6] conduct a comprehensive analysis of both symmetric and asymmetric cryptographic algorithms, focusing on their role in strengthening cybersecurity across diverse contexts. Their work identifies key cryptographic objectives—secrecy, integrity, authenticity, and non-repudiation—as essential for secure communication and data protection. They emphasize the speed and efficiency of symmetric algorithms, such as AES, making them suitable for high-throughput applications. Conversely, they highlight the robustness of asymmetric algorithms, notably RSA, for contexts requiring secure key management. This review contributes significantly to algoTRIC by elucidating how cryptographic strategies can be adapted to address the unique challenges of AI-driven systems. By balancing performance, scalability, and security resilience, this work helps frame the escalating need for robust data protection in modern cybersecurity frameworks.

Furthering these insights, Ustun et al. [7] introduce a machine learning-based intrusion detection system designed to address cybersecurity vulnerabilities in smart grids. Their approach leverages IEC 61850 Sampled Value (SV) messages to identify cyberattacks, particularly false data injection (FDI), within contemporary power system communication frameworks. By utilizing machine learning to distinguish between normal operations and cyberattacks, their system demonstrates high accuracy in identifying symmetrical and asymmetrical faults as well as FDI attacks. These findings are particularly relevant to algoTRIC's efforts to incorporate advanced intrusion detection algorithms in AI-driven environments. Specifically, their approach underscores the importance of integrating encryption techniques, such as AES and ECC, to secure communication streams while ensuring real-time intrusion detection in complex, multi-agent systems.

Similarly, Arora [8] examines the critical role of cryptographic methods in cybersecurity, emphasizing the importance of encryption and decryption for protecting digital data. The study underscores the efficiency of symmetric encryption techniques, such as AES, for managing large-scale data, alongside the superior security of asymmetric algorithms, like RSA, for secure key management. By addressing the fundamental principles of cryptography—confidentiality, integrity, and authenticity—Arora provides essential guidance for incorporating encryption into AI-driven systems. This analysis highlights the trade-offs between the high performance of symmetric encryption and the enhanced security of asymmetric approaches, offering a roadmap for optimizing encryption methods in AI systems that must balance computational demands with robust data protection.

Finally, Henriques and Vernekar [9] focus on the integration of symmetric and asymmetric cryptography to secure communication in Internet of Things (IoT) networks. They address the unique challenges posed by IoT systems, where sensitive data transmitted between devices demands heightened protection against cyberattacks. Their methodology combines the speed and efficiency of symmetric encryption, exemplified by AES, with the secure key management capabilities of asymmetric cryptography, such as RSA. This dual approach mitigates prevalent IoT vulnerabilities, including insecure network services and weak authentication mechanisms. Their work is particularly relevant to algoTRIC, as it explores how combining encryption algorithms can balance speed, scalability, and security in complex, large-scale AI-driven systems.

III. Encryption Algorithms for Cybersecurity

Building on the foundational insights from prior studies on the comparative strengths and applications of symmetric and asymmetric encryption algorithms, the next section delves into the practical implementation of these techniques within contemporary cybersecurity solutions. Encryption techniques and complex algorithms with respect to privacy preserving, wireless sensor networks (WSN), and AI are rapidly used in several system applications and solutions [10-11]. Applications like healthcare monitoring, smart cities, advertising, logistics with analysis of energy, overhead, speed are used for several AI-powered business models. Financial transactions (may consist of hash, public key, private key, and digital signature) today require high level security using Secure Hashing Algorithms

(SHA) and Message Digest (MD) algorithms used by distributed ledgers and blockchain technology (Table I).

Compressed sampling on encrypted images with a combined random Gaussian measurement matrix can also be used for AI based image encryption [12]. To resist several kinds of cyberattacks (primarily as primage attacks, collision attacks) that can pass plaintext sensitivity tests for successful communications. On the other hand, network security or endpoint security (of or partial of cryptography and/or cybersecurity), is fully achieved through data encryption using artificial intelligence [13]. Improving encryption speed, wireless sensors security, integrity of data proposed a proactive solution with remarkable performance as compared to static encryption methods.

Homomorphic encryption has arisen as a formidable method to bolster data security in AI-driven applications, facilitating computations on encrypted data without necessitating decryption. This capacity is essential for preserving data privacy in sensitive domains such as healthcare, banking, and smart city infrastructures, where AI is extensively employed for decision-making and data analysis. Homomorphic encryption encompasses several varieties, including fully homomorphic encryption (FHE), slightly homomorphic encryption (SWHE), and substantially homomorphic encryption (PHE), each presenting distinct trade-offs regarding computational complexity and efficiency [14]. Although Fully Homomorphic Encryption (FHE) permits infinite operations on encrypted data, its practical application is frequently constrained by substantial computing expenses and reduced processing velocities. Conversely, SWHE and PHE provide more efficient options by facilitating a limited range of actions, rendering them more appropriate for situations that emphasize performance while maintaining data security. In AI-driven contexts, including these encryption methods into machine learning models not only protects data during training and inference but also mitigates risks associated with emerging vulnerabilities such as data leakage and unauthorized access. As AI progresses, enhancing these encryption techniques will be essential for guaranteeing strong and scalable cybersecurity solutions.

Furthermore, the computational complexity of cryptographic algorithms emerges as a central concern, influencing not only the feasibility of deploying large-scale encryption solutions but also the security posture of data processing pipelines. Evaluations of complexity commonly employ Big-O notation, time-to-encrypt metrics, key-size scaling factors, and throughput measurements, all of which help determine the practical utility of a given cryptographic method. For symmetric encryption algorithms such as the Advanced Encryption Standard (AES), computational efficiency often proves to be one of their distinguishing strengths, as the complexity scales linearly with data input size, resulting in O(n) operations and predictable performance outcomes even as datasets grow larger. In contrast, asymmetric algorithms like RSA exhibit more pronounced complexity, commonly represented as $O(n^3)$ or higher when operations on large integers are involved, reflecting the significant computational overhead associated with public-key cryptography.

Moreover, the integration of AI-based threat detection and encryption acceleration further complicates these estimates, as machine learning heuristics and hardware-assisted optimizations can alter the baseline complexity by dynamically adjusting key distribution strategies, refining block-cipher rounds, or adopting hybrid encryption approaches. Evaluating complexity also demands close attention to scalability parameters in distributed environments, since multi-agent systems often require concurrent encryption-decryption operations across decentralized nodes, thereby magnifying the importance of parallelizable algorithms. Within this context, assessing complexity involves quantifying performance differentials over heterogeneous architectures, analyzing latency contributions from memory access patterns and cache line misses, and simulating the behavior of algorithms under diverse workload distributions.

As such, the integration of AI approaches with conventional encryption algorithms such as AES has demonstrated effectiveness in augmenting data security, especially in volatile threat landscapes. Recent research indicates that the integration of machine learning models, such as k-Nearest Neighbors (k-NN), with AES encryption markedly enhances the identification and mitigation of anomalies, facilitating real-time responses to new cyber threats. The k-NN's pattern recognition capabilities enhance the encryption process, adapting to emerging attack vectors and bolstering AES's resilience against advanced attacks [15]. This method enhances secure data transmission and bolsters the integrity of secret data storage. With the increasing volume and complexity of data in AI-driven systems, integrating machine learning with encryption methods such as AES is crucial for adopting a proactive approach to cybersecurity.

Chaotic algorithms have arisen as an effective solution for image encryption in AI-driven networking systems, owing to its intrinsic characteristics such as sensitive dependence on beginning conditions, topological mixing, and long-term unpredictability [16]. These qualities are utilized to generate intricate encryption patterns, where even minor alterations in the original settings result in completely distinct encrypted outputs, hence substantially improving data security. Recent implementations indicate that chaotic algorithms, along with sophisticated encryption techniques, can provide non-linear transformations that effectively rearrange and disperse pixel positions, rendering the image data into a highly randomized state. This method guarantees that the encryption process emulates a dynamical system, rendering the reversal of the process without precise system parameters computationally impractical [16]. Through the application of repeated chaotic functions, these encryption methodologies guarantee elevated entropy in the encrypted data, so successfully countering brute-force assaults and enhancing resilience against cryptographic scrutiny. In AI-driven environments, where data security is imperative against advanced threats, the amalgamation of chaotic systems with encryption enhances the security framework while preserving computational performance by reducing processing overhead.

TABLE I. INTUITIONS (UP TO THREE) OF SOME COMMON ADVANCED ENCRYPTION ALGORITHMS FOR SECURITY AND CRYPTOGRAPHY IN THE ARTIFICIAL INTELLIGENCE (AI)-DRIVEN SOCIETY

Ref	Encryption Type	Intuition I	Intuition II	Intuition III
[10]	Partial Homomorphic	Enables privacy-preserving computations on encrypted blockchain data	Mitigates risks from collision, preimage, and wallet attacks	Optimizes computational overhead for AI-integrated blockchain environments
[11]	AI-Driven Data Solutions	Adapts encryption parameters dynamically based on real-time network conditions	Integrates anomaly detection to proactively adjust encryption settings against threats	Optimizes computational and energy resources while maintaining high security levels
[12]	AI Image	Utilizes hyperchaotic sequences for robust pixel scrambling and diffusion	Enhances resistance against differential and brute-force attacks	Achieves high randomness and compression efficiency with compressed sensing
[13)	Innovative Data for WSANs	Adapts encryption parameters dynamically using AI for real-time threat response	Leverages LSTM networks to optimize encryption based on sequential data analysis	Employs Isolation Forests to enhance anomaly detection and network resilience
[14]	AI-based Homomorphic	Enables privacy-preserving computations on encrypted data without decryption	Mitigates data exposure risks in untrusted environments like cloud computing	Supports collaborative AI tasks with multi-key encryption across multiple parties
[15]	AI and AES	Combines AES's robust encryption with AI for adaptive threat detection	Utilizes AI-driven k-NN for real-time anomaly analysis in encrypted data	Enhances encryption efficiency through AI-optimized parameter selection
[16]	Image Transmission	Leverages chaotic mapping for high sensitivity and complex key generation	Enhances image confidentiality through pixel-level scrambling and diffusion	Mitigates brute-force attacks via topological chaos and statistical uniformity

IV. COMPARISONS OF ALGORITHMS W.R.T. SE AND AE

As encryption techniques continue to evolve, their applications in various domains underscore the need for a nuanced understanding of their operational strengths and limitations. The exploration of how these algorithms integrate into modern cybersecurity frameworks provides a foundation for deeper analysis. Thus, a focused comparison follows between symmetric encryption (SE) and asymmetric encryption (AE) will elucidate the key distinctions that influence their use. By examining differences in key management, scalability, performance, and reliability, this analysis aims to identify the most suitable encryption methods for specific applications and highlight the critical trade-offs involved in their deployment within contemporary cryptographic systems.

To evaluate the cryptographic algorithms, it is significant to contrast symmetric encryption algorithms with asymmetric encryption algorithms as modern cryptography is designed based on symmetric and asymmetric encryption which are two fundamental categories of encryption algorithms (Table II). The main purposes of both types of encryption are the same, that is to safeguard the data security and integrity over the diverse applications. Although their purposes are the same, they have significant differences based on the way of managing encryption keys, evaluating performance and functionality requirements. To identify the most effective encryption method for a particular scenario, it is essential to distinguish the strength, weakness, functionalities and other features of both types of encryption methods. This section of the paper distinguishes the fundamental types of encryption algorithm based on key management, scalability, swiftness and reliability.

One of the main differences of symmetric and asymmetric encryption is the number of keys used in the encryption process. There are two types of keys used in encryption and decryption processes which are known as public key and private key. In a symmetric algorithm, a private key is used alone to encrypt and decrypt data [17]. On the other hand, an asymmetric algorithm uses both the public key and private key where the public key is used to encrypt data and private key is used to decrypt data. Public key encryption is designed based on intensive computational mathematical functions; therefore, asymmetric algorithms are not very suitable or efficient for minor devices.

The second important term of differences between symmetric and asymmetric encryption is reliability. The encryption process of the symmetric method is simpler than the asymmetric method, however, in symmetric method both the sender and receiver share the common private key to encrypt and decrypt data which is a major concern about data security as eavesdropping can be conducted by attacker anytime in the channel of data exchange. Alternatively, in asymmetric encryption, the public key is used to encrypt the data while the private key is used to decrypt the data [18]. As the private key is secret and only the receiver knows the private key, it becomes very difficult for the attacker to decrypt the original data. As a result, asymmetric encryption is considered more reliable in comparison to symmetric encryption in case of data exchange.

Swiftness of encryption and decryption is also a very powerful component that can be considered to differentiate symmetric and asymmetric encryption. Al-Shabi, in his paper, conducted an analysis to compare the performance for identifying the strengths and weaknesses of different types of

symmetric and asymmetric encryption based on various factors such as battery consumption, block size, structure, time consumption and types of attacks. His result shows that based on real-time encryption, a symmetric algorithm is much faster than asymmetric encryption [18]. Similar kind of study was conducted by Panda in 2010. Her paper indicates that a symmetric algorithm is almost 1000 times faster than an asymmetric algorithm as an asymmetric algorithm needs more powerful computational resources. To compare different types of algorithm, 3 types of file such as text, image and binary were used in her analysis where the performance factors were decided considering Encryption Time, Decryption Time and Throughout. The result of her study found better performance from the AES algorithm, a subcategory of symmetric encryption, in comparison to other encryption algorithms based on Encryption Time, Decryption Time and Throughout [19].

Use of blocks is also a considerable component that can be used to distinguish between symmetric and asymmetric algorithms. There are mainly two important components considered in symmetric encryption known as block cipher and stream cipher, which are significantly crucial for confidentiality of data and integrity of cryptography [21]. AES, a subcategory of symmetric encryption, is operated on plaintext where the size of the block is 128 bits. This block cipher can also utilize different key lengths such as 128 bits, 192 bits or 256 bits of cipher secret [20]. On the other hand, asymmetric encryption does not require block size to encrypt data, rather this method leverages the idea of chunk data processing that is correspondent to the key size.

In the field of AI-driven cybersecurity, selecting between symmetric encryption (SE) and asymmetric encryption (AE) involves a thorough evaluation of performance, scalability, and security requirements. SE algorithms, such as AES, excel in real-time AI applications due to their high-speed encryption and low computational demands, which highlights as essential for AI tasks requiring rapid data processing [19]. However, AE algorithms like RSA provide enhanced security by leveraging public-private key pairs, a feature that underscores as crucial for maintaining confidentiality in sensitive data exchanges [18]. While SE is ideal for resource-constrained AI environments, such as IoT, due to its lower energy consumption, AE's computational intensity makes it better suited for secure initial key exchanges in distributed AI systems [20]. This difference in resource demands directly impacts scalability; SE supports continuous, high-throughput data streams often required in AI workflows, while AE's structure enables secure data sharing across complex, multi-agent networks through recent advances in secure communication protocols [21]. Effective cybersecurity in AI ultimately requires balancing SE's efficiency and AE's strong data protection, particularly in applications where threats to data integrity and confidentiality are significant [17].

TABLE II. COMPARISON OF SYMMETRIC ENCRYPTION AND ASYMMETRIC ENCRYPTION IN AI-DRIVEN CYBERSECURITY

Aspect	Symmetric Encryption (SE)	Asymmetric Encryption (AE)	Ref.
Integration with AI	SE algorithms like AES and Blowfish are efficient for real-time AI-driven data processing, supporting rapid encryption for high data volumes in AI workflows.	AE algorithms such as RSA and ECC are suitable for securely establishing initial connections in AI systems, though slower for real-time processing.	[19]
Data Throughput	High throughput makes SE ideal for handling large data in AI tasks (e.g., image processing or continuous data flows in AI-based IoT).	Lower throughput is better for secure, one-time exchanges rather than sustained high-speed AI-driven processing.	[21]
Resource Optimization	Low computational demands allow SE to support AI applications in resource-constrained environments, like mobile AI/IoT.	Higher resource needs make AE less suitable for low-power AI applications, though ideal for secure initial setup in complex AI networks.	[20]
Real-Time Efficiency	SE provides rapid encryption/decryption, enhancing real-time AI functions like anomaly detection in cybersecurity.	Slower speed limits AE in real-time AI scenarios; however, it provides robust security for secure data onboarding in AI systems.	[18]
Scalability in AI Systems	SE scales well within high-speed AI environments, enabling quick encryption across multi-agent or large data environments.	AE scales better for secure AI communications in distributed or cloud-based systems, especially for sensitive exchanges.	[21]
Battery and Power Use	Low power consumption suits AI-based mobile or IoT cybersecurity applications, allowing efficient continuous data encryption.	Higher power demand limits AE's suitability for battery-dependent AI devices, though it's viable for centralized secure key exchanges.	[20]
Security Strength	SE algorithms are faster but require secure key management in AI-driven environments to prevent compromise.	AE's public-private key pair provides greater security in AI-based networks with high confidentiality needs, particularly when securing data exchanges.	[18]
Complexity	Simpler structures in SE make it easier to embed into AI cybersecurity models needing rapid, low-latency responses.	AE's complexity is suitable for initial secure connections but can slow down ongoing high-volume AI data processing.	[19]
Use in AI Applications	Frequently applied in AI-driven real-time applications like intrusion detection, anomaly detection, and real-time threat monitoring.	Used to establish secure connections for sensitive AI operations, such as secure federated learning or distributed AI models.	[17]

V. Algorithms in the AI Era

The comparative analysis of symmetric and asymmetric encryption algorithms reveals critical insights into their respective strengths and limitations, offering a clear framework for selecting appropriate methods based on specific requirements. However, as the cybersecurity landscape continues to evolve, traditional encryption approaches must adapt to emerging challenges. The next section explores how AI is evolving encryption by introducing adaptive and dynamic capabilities. Through the integration of ML and DL models, encryption techniques are becoming more resilient, enabling real-time detection of threats and enhancement of key generation processes.

AI is increasingly integrated into encryption techniques, offering adaptive and dynamic solutions to address evolving cybersecurity threats. ML models play a pivotal role by analyzing large datasets to detect anomalies, making encryption protocols more resilient to cyberattacks [22] (Fig. 1). In recent years, there has been a surge in the application of deep learning to enhance cryptographic algorithms, particularly through convolutional neural networks (CNNs). These models help to create more robust key generation processes, as demonstrated in recent studies where CNNs were applied to Advanced Encryption Standard (AES) algorithms to improve encryption performance and security resilience [23]. Such AI-driven encryption systems are capable of continuously evolving, adapting to new security challenges, and countering sophisticated hacking attempts in real-time [24].

In addition to improving encryption processes, AI also aids in the proactive detection and mitigation of cyber threats. As Rangaraju [25] notes, through leveraging ML models, particularly deep learning algorithms, cybersecurity systems can predict potential vulnerabilities and strengthen encryption methods. These techniques not only enhance the overall security infrastructure but also allow for the development of intelligent, self-updating systems that can respond to newly emerging cyber threats. The real-time adaptability of AI in encryption is crucial, especially as traditional cryptography methods, such as RSA, become increasingly vulnerable to advanced cyberattacks [26]. This integration of AI into cryptography sets the stage for more secure communication and data protection in the AI era [27].

With the newly found ability to detect and mitigate cybersecurity threats, AI assists in offering advanced solutions that traditional encryption methods struggle to match. These solutions include CNNs, as noted, but also long short-term memory (LSTM), AI-driven systems that can analyze vast amounts of data in real-time, identifying patterns that signal potential threats. These AI-enhanced systems use data profiling techniques to categorize security events, enabling more accurate discrimination between legitimate threats and false positives [28]. For example, a study employing AI-based security information and event management (SIEM) demonstrated improved accuracy in detecting network intrusions by combining event profiling with various neural networks, outperforming traditional machine learning approaches [29] [30]. The ability to adapt to complex and evolving attack patterns makes these new technologies an essential tool for modern cybersecurity.

Such capacity to adapt and learn from emerging threats is critical as cybercriminals continuously develop more sophisticated attack methods. Deep learning models, especially when applied to real-time cybersecurity monitoring, can detect anomalies much faster than traditional methods, providing organizations with the agility to respond to cyberattacks proactively [31]. Recent advancements in deep learning-based intrusion detection systems (IDS) have shown promising results in identifying zero-day attacks, reducing detection time, and improving overall system security [32]. This proactive approach allows for not only quicker detection but also the anticipation of future attacks, helping organizations stay one step ahead of cybercriminals.

On the other hand, although integrating AI into encryption processes provides significant advancements and benefits, there are also numerous challenges and ethical concerns. One of the primary issues is the risk of over-reliance on AI-based systems, which could lead to complacency in monitoring and updating security protocols [33]. The dynamic nature of these tools can make encryption systems highly efficient, but this reliance also increases the risk that undetected vulnerabilities could be exploited by adversaries using AI for malicious purposes [34]. Furthermore, as AI-driven encryption systems become more widespread, the sheer volume of data processed raises concerns about privacy violations. AI models often require vast amounts of personal or sensitive information to function optimally, which can lead to unintended privacy breaches if not managed properly [35].

Another ethical concern involves the dual-use nature of AI technologies in encryption. While AI enhances security, it also opens avenues for adversaries to exploit AI systems to breach encrypted communications. AI-based algorithms could potentially be reverse-engineered or manipulated to bypass security protocols, creating a new type of cyber threat [36]. The sophistication of AI tools allows attackers to uncover hidden patterns or weaknesses in encryption systems, potentially leading to large-scale data breaches. This highlights the need for comprehensive governance frameworks that address not only the technical challenges but also the ethical risks associated with deploying AI in encryption and cybersecurity [37].

Looking ahead, ever-advancing AI tools are expected to play an increasingly central role in the future of encryption, evolving alongside the cyber threat landscape. The adaptability of AI to real-time data allows for personalized encryption solutions tailored to the behaviors and preferences of individuals, making it more difficult for cybercriminals to execute successful attacks [38]. Through learning from patterns in network traffic and user behavior, AI can continuously optimize encryption protocols, ensuring that they remain effective against emerging threats [39]. This ability to adapt to new challenges positions the technology as a vital tool in maintaining robust cybersecurity defenses in the coming years.

Moreover, integration into encryption technologies opens possibilities for more seamless and efficient security solutions. The use of AI to automate encryption processes could lead to faster, real-time encryption adjustments without human intervention. This is particularly valuable in dynamic environments, such as the Internet of Things (IoT), where

devices continuously communicate and exchange data [40]. The ability to monitor and respond to security threats in real-time ensures that encryption methods are always up to date, thus reducing the risk of breaches [41]. However, these advancements must be balanced with considerations for ethical use and the prevention of potential misuse of AI in malicious hacking activities.

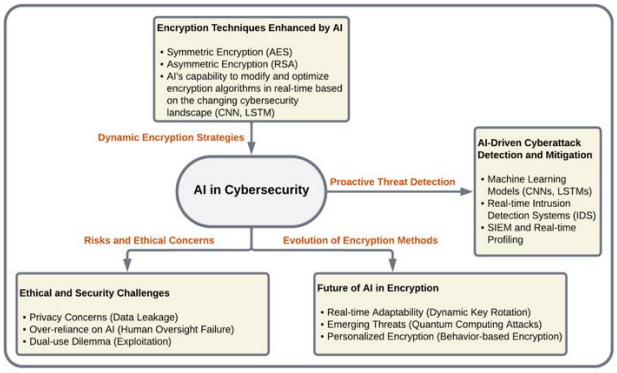

Fig. 1. AI-driven enhancements in encryption (including symmetric and asymmetric) and cybersecurity.

In the era of rapid technological progress, artificial intelligence has emerged as a revolutionary influence across several domains, including cybersecurity. As AI systems advance, the algorithms utilized for data protection as well as encryption must adapt to the intricacies of contemporary threats. The convergence of AI and encryption offers prospects for bolstering cybersecurity resilience via real-time monitoring, adaptive response strategies, and intelligent automation.

A. *Artificial Intelligence-Enhanced Encryption for Improved Cybersecurity*

As AI increasingly integrates with encryption, its transformative impact on cybersecurity becomes evident. The prior discussion outlined the potential of AI-driven methodologies in enhancing traditional encryption systems, offering adaptive and dynamic capabilities. This section delves deeper into the specific mechanisms by which AI enhances both symmetric and asymmetric encryption techniques, focusing on how AI-driven solutions address emerging cybersecurity threats through improved key generation, anomaly detection, and real-time responsiveness.

Conventional encryption techniques, such as the Advanced Encryption Standard (AES) in symmetric encryption and RSA in asymmetric encryption, have been significantly augmented by AI to boost their security and efficiency. AI's capacity to analyze vast datasets, identify trends, and adapt to evolving threats positions it as an ideal collaborator for cryptographic systems.

In symmetric encryption, AI-driven optimization strategies dynamically create, and update AES encryption keys based on real-time threat assessments. Machine learning (ML) algorithms now anticipate vulnerabilities and pre-empt brute-force attacks by identifying anomalous patterns across encrypted data. This dynamic methodology transforms AES into a more adaptable and resilient system, capable of addressing diverse threats without compromising operational speed [32].

For asymmetric encryption, RSA benefits from AI's ability to refine the key generation process. Genetic algorithms, a subset of AI methodologies, enhance the selection of prime numbers, ensuring that encryption keys are robust and less vulnerable to attacks [23]. These advancements reduce computational demands for both encryption and decryption processes while maintaining high levels of security, particularly in environments requiring secure communications.

Deep learning methodologies further expand the potential of AI-enhanced encryption. Techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are now integrated into cryptographic frameworks to monitor encrypted communications in real-time. These algorithms detect irregularities in data streams, identify potential breaches, and enable pre-emptive responses to system intrusions [33]. By adding this layer of real-time detection, AI provides an additional safeguard that static encryption technologies cannot match.

Moreover, the incorporation of AI into cryptographic processes enhances both efficiency and effectiveness. For instance, CNNs within AES key generation operations not only improve security but also lower computational costs [28]. In resource-limited environments such as the Internet of Things (IoT), asymmetric cryptographic methods like RSA leverage AI-driven approaches to optimize encryption and decryption processes, ensuring secure communication without overburdening system resources [29].

B. *Homomorphic Encryption and Privacy-Enhancing Artificial Intelligence Methodologies*

The integration of AI into conventional encryption techniques highlights its transformative potential to enhance security, efficiency, and adaptability. While these advancements address many existing challenges, the need for encryption methods that maintain data confidentiality during processing is paramount, particularly in fields requiring large-scale data analysis. As such, one of the most exciting advancements in AI-driven encryption involves the progression of homomorphic encryption. Homomorphic encryption enables calculations upon encrypted data without necessitating decryption, so safeguarding sensitive information during processing. This is especially beneficial in AI applications requiring the analysis of large data sets, such as in finance, healthcare as well as cloud computing. Also, AI is significantly enhancing the efficiency and scalability of homomorphic encryption techniques. Utilizing AI methodologies might enhance the efficacy of homomorphic encryption by reducing the noise typically accumulated during calculations, hence making these techniques more appropriate for practical use [35].

This advancement is particularly significant for privacy-preserving AI applications, in which sensitive data, such as health-related records and financial information, must be safeguarded throughout the analytical process [22]. Homomorphic encryption, in conjunction with AI, allows businesses to cooperate upon encrypted data without disclosing the underlying knowledge. This privacy-preserving methodology has considerable ramifications for sectors such as healthcare, where patient information may be safely exchanged

and evaluated across institutions without jeopardizing privacy or regulatory adherence [39].

Moreover, AI-based methodologies have begun to influence the design, evaluation, and implementation of encryption algorithms, offering novel avenues for both enhancing and challenging traditional security paradigms. Such approaches incorporate machine learning-based techniques to identify patterns in cipher operations, anticipate potential vulnerabilities, and recommend key management strategies tailored to diverse computational contexts. By employing deep learning models trained on large-scale encryption datasets, researchers can detect subtle correlations in encrypted traffic and refine key scheduling protocols, leading to more resilient cryptographic schemes. In addition to bolstering algorithmic integrity, AI-driven methodologies assist in automating threat detection, as real-time analytics enable dynamic adjustments to key sizes, modes of operation, and encryption parameters based on evolving adversarial tactics. The infusion of AI elements further empowers hybrid encryption approaches where neural networks guide the selection between symmetric and asymmetric algorithms, optimizing both security and computational efficiency.

Lastly, reinforcement learning agents can adaptively determine when to apply advanced cryptographic primitives, such as fully homomorphic encryption, by weighing computational overhead against security gains. Beyond defensive capabilities, AI-based methodologies facilitate the detection and prevention of side-channel attacks, since carefully tuned machine learning classifiers recognize subtle anomalies in power consumption or electromagnetic emissions. Although these techniques hold immense promise, they also raise new ethical and regulatory questions regarding data privacy, algorithmic transparency, and model interpretability, necessitating continuous oversight and methodological rigor in future AI-cryptography research.

C. Blockchain and Artificial Intelligence: A Collaborative Strategy for Security

As homomorphic encryption exemplifies the potential of AI-driven methodologies for securing sensitive data during processing, the integration of AI with blockchain technology offers a complementary avenue for advancing cybersecurity. Blockchain, known for its decentralized and secure architecture, has emerged as a critical tool for safeguarding digital transactions across industries such as finance, healthcare, and supply chain management. However, the growing complexity of blockchain applications demands greater efficiency, scalability, and resilience. AI's integration with blockchain not only addresses these challenges but also enhances the foundational security and operational efficiency of blockchain networks.

Blockchain's inherent security lies in its decentralized structure, which distributes data across multiple nodes to prevent tampering and ensure transparency. When combined with AI, this architecture is further fortified by novel cryptographic techniques such as AI-driven homomorphic encryption. These advanced methods secure data transmission across blockchain networks, even as the volume and complexity of transactions increase. The incorporation of AI enhances blockchain's ability to handle sophisticated encryption requirements, making it a more robust framework for industries that rely on secure, high-throughput digital transactions.

AI also revolutionizes blockchain's consensus mechanisms, which are essential for verifying transactions and maintaining data integrity. Traditional methods like proof-of-work (PoW) and proof-of-stake (PoS) are often criticized for their high energy consumption and computational inefficiencies. AI-augmented consensus algorithms address these limitations by streamlining the validation process, significantly increasing transaction speed while reducing energy demands [40]. This optimization makes blockchain networks more sustainable and scalable, enabling their adoption in diverse and resource-intensive applications without compromising security.

Beyond efficiency, AI contributes to blockchain's real-time security capabilities by identifying and mitigating threats as they arise. Machine learning and anomaly detection algorithms enable blockchain networks to detect irregular transaction patterns, prevent unauthorized access, and counter distributed denial-of-service (DDoS) attacks. These proactive measures ensure that blockchain remains a reliable and resilient platform for secure digital transactions [37]. The fusion of AI's adaptive intelligence with blockchain's decentralized infrastructure not only addresses existing challenges but also sets new benchmarks for trust, scalability, and security in an evolving digital ecosystem.

D. Artificial Intelligence and Quantum-Resistant Cryptography

The integration of AI with blockchain technologies demonstrates its potential to address contemporary cybersecurity challenges, but the emergence of quantum computing introduces a new frontier of threats. Quantum computers, with their unparalleled ability to solve complex mathematical problems, threaten to undermine traditional cryptographic methods such as RSA and elliptic curve cryptography (ECC). As this technological shift looms, AI is playing a pivotal role in developing quantum-resistant cryptographic methods to ensure the continued security of digital communications.

One of the most promising approaches to quantum-resistant cryptography involves lattice-based algorithms, which rely on the computational difficulty of solving lattice problems—a complexity that remains formidable even for quantum computers. AI methodologies enhance the development and evaluation of these post-quantum cryptographic algorithms by identifying potential weaknesses and optimizing their implementation in practical systems [30]. By leveraging AI-driven simulations and predictive modelling, researchers can refine lattice-based encryption techniques to ensure their resilience against both theoretical and practical quantum attacks.

In addition to fortifying cryptographic algorithms, AI also contributes to preparing for the broader implications of quantum computing. Through the simulation of quantum assaults, AI enables the rigorous testing of existing encryption methods under quantum conditions. This proactive approach not only helps to identify vulnerabilities but also informs the creation of robust cryptographic standards designed to safeguard sensitive information in the quantum age [27]. Moreover, AI models are

used to predict the pace and direction of quantum computing advancements, enabling the development of encryption methods that stay ahead of potential threats [26]. The synergy between AI and quantum-resistant cryptography exemplifies the forward-thinking strategies required to navigate this impending technological shift. As quantum computing capabilities grow, the collaboration of AI and cryptography will be instrumental in ensuring that encryption techniques evolve to meet new challenges.

E. Ethical Implications in AI-Enhanced Cryptography

As advancements in AI-driven encryption and quantum-resistant cryptography push the boundaries of cybersecurity, they also introduce complex ethical considerations. The deployment of such powerful technologies raises critical questions about transparency, accountability, and equitable access, necessitating a careful examination of the broader societal implications of AI-enhanced cryptography. The incorporation of AI within encryption systems presents significant ethical dilemmas. As AI algorithms increase in complexity, the need for openness and accountability in their decision-making processes, especially in encryption and cybersecurity, is intensifying. It is essential to design AI-driven cryptography systems with ethical concerns to foster confidence and avoid abuse.

A primary worry is the dual-use characteristic of AI technology. Although AI may improve encryption as well as cybersecurity, it may also be utilized by nefarious individuals to develop more advanced assaults or to avoid detection. Developing AI-driven encryption systems with strong ethical standards is crucial to avoid their misuse for bad reasons [36]. Furthermore, as AI along with encryption technologies proliferate, it is essential to guarantee their accessibility and equity. It includes tackling the digital divide including guaranteeing that modern encryption technologies are accessible to all societal sectors, not just to those with the means to use them [24].

To get farther into the AI age, encryption algorithms must advance to match the increasing sophistication of cyber threats. Artificial intelligence is significantly transforming both asymmetric and symmetrical encryption systems, which renders them more adaptable, effective, and safe. The integration of AI in key generation and real-time threat detection is transforming cybersecurity methodologies. Nonetheless, the prospect of AI-driven cryptography has concerns as well. It is essential for these systems to be morally robust, transparent, and resilient against new dangers, including those from quantum computing, to ensure their success. Advancing and perfecting AI-driven encryption methods will enable the establishment of an increased secure digital future which safeguards sensitive information while promoting innovation.

VI. Algorithm Security in Modern Society

Encryption algorithms are essential tools in maintaining the confidentiality and integrity of digital communications in modern society (Fig. 2). With the increasing reliance on digital platforms for both personal and professional interactions, ensuring secure communication has become a priority [42]. Algorithms such as the AES and RSA are widely adopted to protect sensitive data, including emails, financial transactions, and other online communications. AES, a symmetric key algorithm, is favored for its speed and efficiency in encrypting large volumes of data, making it suitable for applications where rapid data processing is critical [43]. In contrast, RSA, an asymmetric key algorithm, is often used for secure key exchanges and digital signatures due to its robust security features, although it operates at a slower speed [44]. Together, these algorithms form the foundation of secure digital communications, providing the first line of defense against unauthorized access and cyberattacks.

As society becomes more dependent on digital communication, the application of encryption algorithms continues to expand. For instance, hybrid encryption schemes that combine the strengths of both AES and RSA are becoming more popular. These hybrid systems leverage the efficiency of AES in data encryption and the strength of RSA in secure key management, ensuring that both the data and the encryption keys are protected during transmission [45]. Such combined approaches offer enhanced security, particularly in environments where large volumes of sensitive information are frequently exchanged, such as in e-commerce or financial institutions [46]. As encryption technologies evolve, they continue to play a vital role in safeguarding digital communication, adapting to new threats and ensuring that sensitive information remains confidential and secure [47]. Thus, actionable risk assessment methodologies are particularly valuable for organizations that rely heavily on algorithms for their security, as they provide a clear framework to assess vulnerabilities, adapt to evolving threats, and reduce reliance on external vendors [48].

Yet, as noted, the rapid adoption of IoT devices and cloud computing has created new vulnerabilities in cybersecurity systems, particularly due to the limited computing capabilities of many IoT devices [34]. Many of these devices rely on lightweight encryption algorithms, such as the Data Encryption Standard (DES) or AES, which are efficient but may be more susceptible to attacks due to their reduced complexity [49]. Additionally, IoT devices often lack regular security updates, making them easy targets for cybercriminals. Cloud computing environments further complicate the situation, as data in transit and at rest in the cloud are vulnerable to interception, especially during migration between different cloud platforms [49]. This growing complexity necessitates the development of more robust encryption techniques tailored to the needs of both IoT and cloud environments [51].

Furthermore, the rise of supply chain attacks, where third-party software or hardware components are compromised, presents another significant challenge. As Hammi Zeadally and Nebhen (2023) point out, since many organizations rely on cloud services that integrate multiple external vendors, ensuring the security of every component is increasingly difficult [52]. In such environments, traditional encryption methods may not provide sufficient protection against sophisticated attacks. Emerging encryption models, such as lattice-based cryptography and hybrid encryption schemes, have been proposed as solutions to strengthen security, especially in resource-constrained IoT devices and cloud platforms [53]. As IoT and cloud ecosystems continue to expand, the demand for

an advanced encryption methods that can effectively address these new vulnerabilities [50] will only increase [54]. Also, the escalating sophistication of cryptojacking and ransomware highlights the importance of robust encryption algorithms to safeguard against unauthorized access and financial disruptions who are using blockchain technology for their security [55].

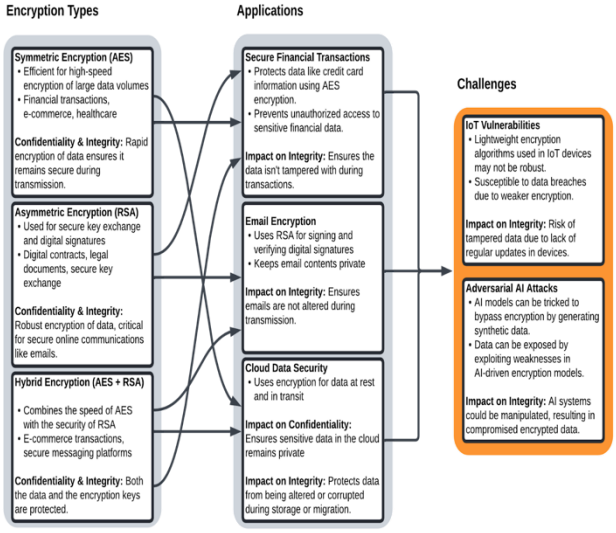

Fig. 2. Encryption algorithms (symmetric, asymmetric, and hybrid) securing digital communications.

While these tools can enhance encryption and cybersecurity, it also introduces new vulnerabilities, particularly through adversarial AI attacks. These attacks exploit the weaknesses in AI models by introducing adversarial inputs, causing the system to make incorrect decisions. In the context of encryption, adversaries can manipulate these models designed to detect anomalies in encrypted communications or tamper with ML algorithms that generate encryption keys [56]. For example, recent studies have shown that adversarial ML techniques can be used to bypass AI-driven encryption models by generating synthetic data that mimics normal traffic patterns, thereby fooling detection systems [57].

Moreover, adversarial attacks can target not just encryption algorithms but the entire AI-based cybersecurity framework. These attacks can render AI-based defenses ineffective by exploiting weaknesses in neural networks used for real-time threat detection [58]. For instance, Generative Adversarial Networks (GANs) have been employed to create realistic attack scenarios that deceive AI systems, making it harder for traditional encryption methods to safeguard data [59]. The increasing sophistication of adversarial AI raises the stakes for maintaining secure systems, requiring not only advancements in encryption but also in AI model robustness [60]. As these threats evolve, the integration of more secure AI models into encryption protocols will be vital for protecting sensitive information in the digital age.

Moreover, the widespread use of encryption technologies in sectors such as finance, healthcare, and national security brings with it significant ethical and legal challenges. Governments and regulatory bodies face the difficult task of balancing individual privacy rights with the need for surveillance to prevent criminal activities [61]. Encryption ensures that sensitive data remains confidential, but it also makes it harder for law enforcement agencies to access potentially crucial information [63]. As a result, there has been ongoing debate about the implementation of encryption backdoors, which would allow authorized entities to decrypt data under specific circumstances. However, these backdoors present a serious ethical dilemma, as they could be exploited by malicious actors if not properly secured [63]. As encryption continues to play a critical role in modern society, it will be essential for policymakers to develop clear, globally consistent frameworks that address both the ethical and legal challenges posed by these technologies [37]. In addition to the ethical concerns, encryption technologies also raise legal questions regarding jurisdiction and data ownership. As data crosses international borders, determining which country's laws apply to encrypted information becomes increasingly complicated [64]. For instance, different nations have varying regulations regarding data privacy and encryption standards, which can lead to conflicts when encrypted data is stored in one country but accessed or processed in another [65].

As encryption continues to play a critical role in modern society, it will be essential for policymakers to develop clear, globally consistent frameworks that address both the ethical and legal challenges posed by these technologies [37]. In addition to the ethical concerns, encryption technologies also raise legal questions regarding jurisdiction and data ownership. As data crosses international borders, determining which country's laws apply to encrypted information becomes increasingly complicated [62]. For instance, different nations have varying regulations regarding data privacy and encryption standards, which can lead to conflicts when encrypted data is stored in one country but accessed or processed in another [63].

VII. Discussion and Limitations

The integration of AI with encryption signifies a pivotal change in cybersecurity, offering both prospects and complex obstacles. The significance of AI in encryption has led to significant progress constantly in real-time threat detection as well as flexible security mechanisms, which are more vital in the contemporary linked and susceptible digital environment. This capacity allows encryption systems to promptly address abnormalities and emerging attack patterns, hence providing resilience unattainable by conventional static encryption approaches. Nonetheless, this progress entails an increasing dependence on machine learning as well as deep learning models, that, whilst augmenting encryption capabilities, can present weaknesses like adversarial assaults. These assaults target vulnerabilities in AI models using misleading inputs, compromising the precision and resilience of systems intended to identify and counter cyber threats. Thus, the dual-use characteristic of AI technology requires a measured and attentive strategy, especially in vital sectors such as healthcare, banking, and national security, wherein AI-driven encryption plays a crucial role in safeguarding extremely sensitive information.

Nonetheless, this progress is not without limitations. First, the over-reliance on AI systems for encryption may create blind spots, wherein undetected vulnerabilities can be exploited by

adversaries leveraging AI for malicious purposes. Second, the ethical and legal challenges surrounding AI-driven encryption, such as potential breaches of data privacy [62] and concerns about surveillance misuse, demand robust governance frameworks. These frameworks must include clear ethical guidelines and enforceable regulations to prevent the unintended misuse of AI-enhanced encryption technologies.

Additionally, accessibility disparities pose significant challenges. AI-driven encryption technologies, while offering scalable solutions, often require substantial technological resources and compliance capabilities. This raises questions about equity, as organizations with limited resources may struggle to implement these advanced systems effectively. Addressing such disparities is vital to ensuring the widespread and fair adoption of AI-powered encryption.

As such, the following validation approach should be used in future studies. In evaluating the proposed cryptographic solutions, employing a rigorous validation process establishes a credible foundation for comparative analysis and subsequent knowledge generation. This process begins with controlled laboratory testing, where encryption algorithms undergo quantitative benchmarking against standardized datasets, fixed key lengths, and pre-defined plaintext-ciphertext pairs to ensure reproducibility. By comparing time-to-encrypt, CPU utilization, memory usage, and latency across multiple cryptographic methods, researchers gain insights into both efficiency and scalability. The application of formal verification techniques, such as model checking and theorem proving, bolsters confidence in algorithmic correctness, ensuring that keys, modes of operation, and cipher primitives function as intended under a range of computational scenarios.

Beyond laboratory environments, field testing in distributed AI-driven systems delivers validation grounded in practical contexts, as real-time data streams reveal how well the chosen cryptographic methods withstand dynamic adversarial tactics. For comprehensive comparative analysis, conducting multi-criteria decision-making (MCDM) evaluations allows researchers to weigh performance metrics, security robustness, and resource overhead against one another. Statistical tests, including ANOVA or Wilcoxon signed-rank tests, further enhance credibility by confirming that observed differences in performance are significant and not attributable to random variation. Iterative refinement informed by validation feedback cycles contributes to continual improvement, bridging the gap between theoretical design and practical deployment. Through meticulous validation and comparison, the resulting cryptographic frameworks achieve a higher degree of reliability, fostering trust among stakeholders and ensuring that deployed solutions fulfill the intended security objectives in increasingly complex AI ecosystems.

Furthermore, the widespread use of AI-driven encryption systems raises urgent accessibility and ethical issues. Even while these technologies provide scalable solutions, their use in a variety of international businesses raises concerns about transparency and equality, particularly when firms have varying levels of technological resources as well as regulatory compliance skills. The fair distribution of these cutting-edge technologies must be given equal weight with technological resilience in the advancement of AI-powered encryption. These technologies also raise significant ethical and legal issues, including surveillance, data privacy, and the possible abuse of AI-enhanced encryption to provide vulnerabilities for illegal data access. To prevent AI-encrypted systems from unintentionally jeopardizing the same security and confidentiality they are meant to safeguard, strict governance structures and ethical standards must be established. Therefore, this open conversation covers both the enormous possibilities and the serious threats of AI-driven encryption, necessitating a thorough, interdisciplinary response to responsibly influence cybersecurity's future.

To sum up, the combination of encryption and artificial intelligence has brought about a new age in cybersecurity that offers increased resistance to a wide range of online dangers. AI-driven encryption is essential in today's fast-paced, data-intensive digital environment because of its adaptable, real-time features, which provide major benefits over conventional encryption methods. Homomorphic encryption and AI-enhanced algorithms are only two examples of the encryption techniques that have advanced because of this integration, strengthening data security and enabling sophisticated calculations on encrypted data. AI algorithms provide a strong defense against complex cyberattacks as they become better at managing the complexities of threat detection including adaptive encryption key management. However, this development raises fresh moral and legal issues. The ethical conundrums around privacy, transparency, and equality, together with the dual-purpose possibilities for AI technology, highlight the need for a concerted effort from all parties involved. To create moral guidelines including legal frameworks that encompass both the technical aspects of AI-enhanced encryption and its wider social ramifications, cooperation between government, business, and academia is crucial.

In the future, establishing a safe and flexible cybersecurity framework will require a proactive approach to the creation and management of AI-driven encryption systems. To reduce new dangers and protect sensitive data in a variety of industries, further research in fields like adversarial resilience, quantum-resistant encryption, and ethical AI will be essential. Through adopting this forward-thinking viewpoint, the cybersecurity industry can capitalize on AI's ability to develop encryption technologies while additionally making certain that those solutions are just, ethically appropriate, as well as resilient to the constantly changing cyberthreat scenario. In this sense, incorporating AI into encryption seems not just a technological development but also a step toward a digital future that is safe, sustainable, as well as considerate of privacy.

Although there are several issues in algorithms for both encryption and decryption, some of the major ones (in symmetric encryption and asymmetric encryption) are shown in Fig. 3 below. The challenges in algorithm generation, algorithm writing, and algorithm difficulty continues as the use of various language models including Artificial Intelligence (AI), Deep Learning (DL), and Machine Learning (ML) keeps growing.

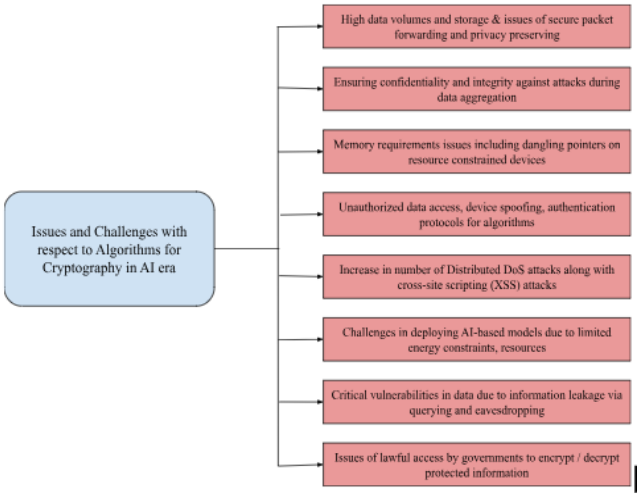

Fig. 3. Encryption algorithms (symmetric, asymmetric, and hybrid) securing digital communications.

VIII. Conclusion and Future Scope

We provided an in-depth study focusing on securing sensitive information with comparative analysis for symmetric encryption and asymmetric encryption algorithms for cryptography. The comparison on the study focuses on key factors like security resilience, scalability, speed in the light of evolving cyber threats. We have addressed the security concerns tackled by encryption algorithms in the Artificial Intelligence (AI) and Large Language Models (LLMs) age along with research directions to enhance overall cybersecurity and cryptography. The aspect comparison between symmetric encryption and asymmetric comparison allows us to decide the environments used including AI environments, key-pairs leveraging via secure key exchanges, and/or decision in secure protocols for secure data sharing.

Future scope of algorithms whether it be symmetric encryption and asymmetric encryption algorithms, largely rely upon use of AI models, reliability, scalability, and key management. Enabling machines to learn is always a future challenge that may require human intelligence in the next step for decision-making. As we progress into several AI algorithms in the future, all three types of learning (supervised learning, unsupervised learning, and reinforcement learning) we must be more intuitive in the future on how we process data and information.

References

[1] Thiyagarajan, P. (2020). A review on cyber security mechanisms using machine and deep learning algorithms. *Handbook of research on machine and deep learning applications for cyber security*, 23-41.

[2] Terumalasetti, S., & Reeja, S. R. (2022, August). A comprehensive study on review of AI techniques to provide security in the digital world. In *2022 third international conference on intelligent computing instrumentation and control technologies (ICICICT)* (pp. 407-416). IEEE.

[3] Al-Arjan, A., Rasmi, M., & AlZu'bi, S. (2021, July). Intelligent security in the era of AI: The key vulnerability of RC4 algorithm. In *2021 International Conference on Information Technology (ICIT)* (pp. 691-694). IEEE.

[4] Bertino, E., Kantarcioglu, M., Akcora, C. G., Samtani, S., Mittal, S., & Gupta, M. (2021, April). AI for Security and Security for AI. In *Proceedings of the Eleventh ACM Conf on Data and Appn Security and Privacy* (pp. 333-334).

[5] Kapoor, J., & Thakur, D. (2022). Analysis of symmetric and asymmetric key algorithms. In *ICT analysis and applications* (pp. 133-143). Springer.

[6] Soomro, S., Belgaum, M. R., Alansari, Z., & Jain, R. (2019, August). Review and open issues of cryptographic algorithms in cyber security. In *2019 Int Conf on Comp, Elect & Comm Engineering (iCCECE)* (pp. 158-162). IEEE.

[7] Ustun, T. S., Hussain, S. S., Yavuz, L., & Onen, A. (2021). Artificial intelligence-based intrusion detection system for IEC 61850 sampled values under symmetric and asymmetric faults. *Ieee Access*, *9*, 56486-56495.

[8] Arora, S. (2022). A review on various methods of cryptography for cyber security. *Journal of Algebraic Statistics*, *13*(3), 5016-5024.

[9] Henriques, M. S., & Vernekar, N. K. (2017, May). Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In *2017 International Conf on IoT and Application (ICIOT)* (pp. 1-4). IEEE.

[10] Yaji, S., Bangera, K., & Neelima, B. (2018, December). Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications. *25th Int Conf on HPC Workshops (HiPCW)* (pp. 81-85). IEEE.

[11] Arulmurugan, L., Thakur, S., Dayana, R., Thenappan, S., Nagesh, B., & Sri, R. K. (2024, May). Advancing Security: Exploring AI-driven Data Encryption Solutions for Wireless Sensor Networks. In *2024 Int Conf on Advances in Comp, Comm and Applied Informatics (ACCAI)* (pp. 1-6). IEEE.

[12] Xu, D., Li, G., Xu, W., & Wei, C. (2023). Design of artificial intelligence image encryption algorithm based on hyperchaos. *Ain Shams Engineering Journal*, *14*(3), 101891.

[13] Dharmateja, M., Rama, P. K., Asha, N., Nithya, P., Lalitha, S., & Manojkumar, P. (2024, March). Innovative Data Encryption Techniques using AI for Wireless Sensor Actuator Network Security. In *2024 Int Conf on Distributed Comp and Optimization Techniques (ICDCOT)* (pp. 1-6). IEEE.

[14] Hamza, R. (2023, October). Homomorphic Encryption for AI-Based Applications: Challenges and Opportunities. In *2023 15th International Conference on Knowledge and Systems Engineering (KSE)* (pp. 1-6). IEEE.

[15] Budhewar, A., Bhumgara, S., Tekavade, A., Nandkar, J., & Zanwar, A. (2024, April). Enhancing Data Security through the Synergy of AI and AES Encryption: A Comprehensive Study and Implementation. In *2024 MIT Art, Design and Tech Sch of Comp Int Conf (MITADTSoCiCon)* (pp. 1-5). IEEE.

[16] Tian, H., Yuan, Z., Zhou, J., & He, R. (2024). Application of Image Security Transmission Encryption Algorithm Based on Chaos Algorithm in Networking Systems of Artificial Intelligence. In *Image Processing, Electronics and Computers* (pp. 21-31). IOS Press.

[17] Abd Elminaam, D. S., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating the performance of symmetric encryption algorithms. *Int. J. Netw. Secur.*, *10*(3), 216-222.

[18] Al-Shabi, M. A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), 576-589.

[19] Panda, M. (2016, October). Performance analysis of encryption algorithms for security. In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (pp. 278-284). IEEE.

[20] Hintaw, A. J., Manickam, S., Karuppayah, S., Aladaileh, M. A., Aboalmaaly, M. F., & Laghari, S. U. A. (2023). A robust security scheme based on enhanced symmetric algorithm for MQTT in the Internet of Things. *IEEE Access*, *11*, 43019-43040.

[21] Kuznetsov, O., Poluyanenko, N., Frontoni, E., & Kandiy, S. (2024). Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography. *Cryptography*, *8*(2), 17.

[22] Halewa, A. S. (2024). Encrypted AI for Cyber security Threat Detection. *International Journal of Research and Review Techniques*, *3*(1), 104-111.

[23] Negabi, I., El Asri, S. A., El Adib, S., & Raissouni, N. (2023). Convolutional neural network based key generation for security of data through encryption with advanced encryption standard. *International Journal of Electrical & Computer Engineering* (2088-8708), 13(3).

[24] Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS)* ISSN: 3006-4023, 1(1), 132-151.

[25] Rangaraju, S. (2023). Ai sentry: Reinventing cybersecurity through intelligent threat detection. *EPH-International Journal of Science And Engineering*, *9*(3), 30-35.

[26] Saha, A., Pathak, C., & Saha, S. (2021). A Study of Machine Learning Techniques in Cryptography for Cybersecurity. *American Journal of Electronics & Communication*, *1*(4), 22-26.

[27] Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Eng Technologies and Innovations*, *1*(01), 294-319.

[28] Feisheng, L. (2024, April). Systematic Review of Sentiment Analysis: Insights Through CNN-LSTM Networks. In *2024 5th Int Conference on Industrial Engineering and Artificial Intelligence (IEAI)* (pp. 102-109). IEEE.

[29] Pacheco, J., Benitez, V. H., Felix-Herran, L. C., & Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. *IEEE Access*, *8*, 73907-73918.

[30] Tashfeen, M. T. A. (2024). Intrusion detection system using AI and machine learning algorithms. In *Cyber security for next-generation computing technologies* (pp. 120-140). CRC Press.

[31] Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69.

[32] Alionsi, D. D. D. (2023). AI-driven cybersecurity: Utilizing machine learning and deep learning techniques for real-time threat detection, analysis, and mitigation in complex IT networks. *Advances in Eng Innovation*, *3*, 27-31.

[33] Orner, C., & Chowdhury, M. M. (2024). AI and Cybersecurity: Collaborator or Confrontation. *Proceedings of 39th Int Confer*, *98*, 150-158.

[34] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *JAIGS*, ISSN: 3006-4023, 2(1), 129-171.

[35] Gupta, A., Wright, C., Ganapini, M. B., Sweidan, M., & Butalid, R. (2022). State of AI ethics report (vol 6, feb 2022). *arXiv preprint arXiv:2202.07435*.

[36] Riebe, T. (2023). Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion between Civilian and Defense R&D. In *Technology Assessment of Dual-Use ICTs: How to Assess Diffusion, Governance and Design* (pp. 93-110). Wiesbaden: Springer Fachmedien Wiesbaden.

[37] Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*.

[38] Evren, R., & Milson, S. (2024). The Cyber Threat Landscape: Understanding and Mitigating Risks. *Tech. rep. EasyChair*.

[39] Morley, J., & Floridi, L. (2020). An ethically mindful approach to AI for health care. *The Lancet*, *395*(10220), 254-255.

[40] Javadpour, A., Ja'fari, F., Taleb, T., Zhao, Y., Bin, Y., & Benzaïd, C. (2023). Encryption as a service for IoT: opportunities, challenges and solutions. *IEEE Internet of Things Journal*.

[41] Gupta, A., Royer, A., Heath, V., Wright, C., Lanteigne, C., Cohen, A., Ganapini, M., Fancy, M., Galinkin, E., Khurana, R., Akif, M., Butalid, R., Khan, F., Sweidan, M., (2020). The State of AI Ethics Report. *arXiv, abs/2011.02787*.

[42] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, *22*, 100759.

[43] Kuppuswamy, P., Al, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics*, *12*(2), 1148-1158.

[44] Pandey, P. K., Kansal, V., & Swaroop, A. (2023). Security challenges and solutions for next-generation VANETs: an exploratory study. In *Role of Data-Intensive Distributed Computing Systems in Designing Data Solutions* (pp. 183-201). Cham: Springer International Publishing.

[45] Akter, R. I. M. A., Khan, M. A. R., Rahman, F. A. R. D. O. W. S. I., Soheli, S. J., & Suha, N. J. (2023). RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. Int. J. Comp. *Appl. Math. Comput. Sci*, *3*, 60-71.

[46] Liu, Y., Gong, W., & Fan, W. (2018). Application of AES and RSA Hybrid Algorithm in E-mail. *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, 701-703. https://doi.org/10.1109/ICIS.2018.8466380.

[47] Subramanian, A., Donta, L. S., & Supraja, P. (2024, May). Assessing the Strength of Hybrid Cryptographic Algorithms: A Comparative Study. In *2024 Int Conf on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1-6). IEEE.

[48] Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and cybersecurity risk assessment. Journal of Information Security, 15(4), 564–588. https://doi.org/10.4236/jis.2024.154032

[49] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 1-18.

[50] Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures. *IEEE Int of Things Jou*, *10*(13), 11224-11239.

[51] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. (2017). Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, *55*, 26-33. https://doi.org/10.1109/MCOM.2017.1600363CM

[52] Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1-40.

[53] Bagla, P., Sharma, R., Mishra, A., Tripathi, N., Dumka, A., & Pandey, N. (2023). An Efficient Security Solution for IoT and Cloud Security Using Lattice-Based Cryptography. *Int Conf on Eme Trends in Net and Comp Comm (ETNCC)*, 82-87. https://doi.org/10.1109/ETNCC59188.2023.10284931.

[54] Ahmed, S., & Khan, M. (2023). Securing the Internet of Things (IoT): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the IoT ecosystem. *AI, IoT & the 4th Ind Rev Rev*, *13*(9), 1-17.

[55] Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2024). cryptoRAN: A review on cryptojacking and ransomware attacks w.r.t. banking industry - Threats, challenges, & problems. 2nd InCACCT (pp. 523–528). IEEE. https://doi.org/10.1109/InCACCT61598.2024.10550970

[56] Craighero, F., Angaroni, F., Stella, F., Damiani, C., Antoniotti, M., & Graudenzi, A. (2023). Unity is strength: Improving the detection of adversarial examples with ensemble approaches. *Neurocomputing*, *554*, 126576.

[57] Shroff, J., Walambe, R., Singh, S. K., & Kotecha, K. (2022). Enhanced security against volumetric DDoS attacks using adversarial machine learning. *Wireless Communications and Mobile Computing*, *2022*(1), 5757164.

[58] Sathupadi, K. (2023). Ai-based intrusion detection and ddos mitigation in fog computing: Addressing security threats in decentralized systems. *Sage Science Review of Applied Machine Learning*, *6*(11), 44-58.

[59] Zhang, C., Yu, S., Tian, Z., & Yu, J. J. (2023). Generative adversarial networks: A survey on attack and defense perspective. *ACM Computing Surveys*, *56*(4), 1-35.

[60] Fernando, P., & Wei-Kocsis, J. (2021). A Novel Data Encryption Method Inspired by Adversarial Attacks. *ArXiv, abs/2109.06634.*

[61] Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Iss in the Dig Age*, (2), 78-121.

[62] van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review, 49*, 105804.

[63] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, 1-4. https://doi.org/10.1038/s42256-019-0109-1.

[64] Lubin, A. (2023). The prohibition on extraterritorial enforcement jurisdiction in the datasphere. In *Research Handbook on Extraterritoriality in International Law* (pp. 339-355). Edward Elgar Publishing.

[65] Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *Int Jou of Int Auto & Comp*, *6*(5), 1-12.