Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 10, 2025

ENCRYPTION AND DECRYPTION IN COMPUTER SCIENCE: ALGORITHMS, APPLICATIONS, AND SECURITY CHALLENGES

Haider Abbas[*1], Dr. Malik Sikandar Hayat Khiyal[2], Dr. Muhammad Daud Awan[3]

[*1,2,3]*Preston University, Islamabad campus of Pakistan.*

[*1]haider7717@yahoo.com ,[2]drsikandarhayat@preston.edu.pk,[3]Drdaudawan@preston.edu.pk

DOI: https://doi.org/10.5281/zenodo.17491159

Keywords
Encryption, Decryption, Cryptography, Quantum Computing, AI-Driven Security, Blockchain, Post-Quantum Cryptography, Lightweight Cryptography, Data Integrity, Cybersecurity

Article History
Received: 12 September 2025
Accepted: 18 October 2025
Published: 31 October 2025

Corresponding Author: *
Haider Abbas

Abstract
Encryption and decryption are fundamental mechanisms in computer science that safeguard information confidentiality, integrity, and accessibility. This paper comprehensively reviews traditional and modern cryptographic techniques, including symmetric, asymmetric, and hybrid encryption algorithms, highlighting their mechanisms, advantages, and limitations. Core algorithms such as AES, DES, Blowfish, RSA, ECC, and Diffie Hellman are discussed with respect to their security performance, computational efficiency, and suitability for different digital environments. The study explores advanced developments such as homomorphic encryption, optical encryption, neural network-assisted cryptography, and blockchain-based key management systems, which offer enhanced privacy and efficiency in secure communications. Special attention is given to the emerging challenges posed by quantum computing, which threatens conventional encryption standards, and to the evolving field of post-quantum cryptography that aims to build quantum-resistant algorithms. Furthermore, the paper highlights the role of artificial intelligence and lightweight cryptography in securing IoT systems and resource-constrained devices. The review concludes that the continuous advancement of cryptographic systems, integration of AI-driven cybersecurity measures, and development of quantum-safe encryption standards are crucial for ensuring robust data protection in the rapidly evolving digital ecosystem.

1. INTRODUCTION

In computer science, encryption and decryption encode and safeguard information from prying eyes, guaranteeing confidentiality and access control. They transform useful data into a tangled mess that only authorized parties can access and revert to the original form. In this manner, sensitive information is secured from interception and unauthorized access, and unauthorized users' access is prevented, to ensure decryption and access control. In this environment, the most notable benefit is the confidentiality and privacy of the information. Decrypting the data without the key is impossible, making the data accessible only to parties that possess the key (Panda, 2016). This is of paramount importance in the healthcare industry, where encryption protects sensitive patient information, thereby ensuring privacy and compliance with HIPAA (Basha, 2024) and other similar legislations. Encryption confirms data integrity in addition to confidentiality. With homomorphic encryption, operations can be performed on encrypted data without compromising privacy (Othman et al.,

2014). This is invaluable in wireless sensor networks and other data-sensitive environments where data exposure is unethical and deceptive data processing is performed. with reference to communication texts, the corresponding encrypted images, with color modes used to encrypt the images, are protective of the encryption. The security is also increased with the reduction of possible adversary key breaches (Noor et al. 2022).

The security of encrypted information is fundamentally strengthened with the application of advanced cryptographic methods such as quantum cryptography. Under the principles of quantum mechanics, 'classical' encryption can be enhanced with quantum encryption to secure communication channels, which are fundamentally unbreachable, and create reliable protective structures for data (Basha 2024). The evolution of modern digital systems sparked the need to address the growing demands of data security, privacy, and efficient digital systems encryption and decryption. This is characterized by the strategic application of advanced and sophisticated cryptographic systems, the integration of new cutting-edge technologies neural networks, modern advancements in optical and image encryption, and the development of cryptographic systems.

Significant progress continues to be made in the area of symmetric and asymmetric encryption methods. RSA, DES, and AES remain critical algorithms in the encryption and protection of data communications. For instance, RSA encrypts the data along with other protective layers, such as multi-factor authentication and device fingerprinting, to protect a system used in online voting (Rahman et al., 2024). AES is also widely used because of its efficiency, as it rapidly encrypts and decrypts data, while also maintaining a high level of security (Yeow & Ng, 2023).

Optical encryption is the latest technology in encryption. It is presumed to offer fast, multi-dimensional processing at high speeds while consuming low power. Enhanced security is offered by techniques like meta-optics-empowered vector visual cryptography, which employs the several degrees of freedom of light and spatial dislocation as key parameters. Apart from high security, it also allows rapid decryption, thereby optimizing the processes (F. Zhang et al., 2023).

Neural networks having the potential for encryption is another mobile neural networks advanced development. The combination of neural network models with encryption algorithms poses potential neural networks protected data secure opportunities, the difficulties with the widespread practical use of neural networks remain (Yeow & Ng, 2023). Photonic ink based and time and temperature resolved coding and more recently, complex multi-channel information storage as well as anti-counterfeiting. This method, and the need for sensitive information to be handled with an appropriate tradeoff of convenience and security are addressed (D. Li et al., 2022). Even more, the frequent use of images in digital communication has attracted encryption of images. Chaotic systems and physical unclonable functions are new algorithms that ensure the theoretical security of an image is protected inversion and withstand a (Muhammad & Özkaynak, 2021) and rigorous mathematical proof technique. The developments in the protective digital systems encryption technologies, and information systems security order decryption systems provide for increasingly complex and compromised exchange systems. The need for development is highly relevant today and growing more significant.

Basic Concepts

The mechanisms of encryption and decryption work together to secure data and form an essential part of any cryptographic system. Algorithms that perform these operations work to protect data's confidentiality and security while trying to transform data from an intelligible form (plaintext) to an unintelligible form (ciphertext). The reversibility of the system allows data to be decrypted back to plaintext (Yang et al., 2004). The choice of technique influenced the system's architecture and the type of key generation. The two main types of algorithms are symmetric and asymmetric key algorithms. Examples of symmetric key algorithms are AES (Advanced Encryption Standard) and DES (Data Encryption Standard). Symmetric systems are usually faster and work well when processing large volumes of data. The main issue that this type system presents is the safe transfer of keys (Elminaam et al., 2010; Panda, 2016). This type of system is therefore less secure

compared to its asymmetric counterpart, which utilizes a pair of keys: a public key that an encrypting community uses and a private key that the decrypting community uses. Although this method is less efficient, it is more secure and simplifies the key exchange problem. A common example of this method is the RSA (Rivest-Shamir-Adleman) algorithm (Panda, 2016; Sihotang et al., 2020). Homomorphic Encryption is an advanced cryptographic technique that allows one to perform operations on encoded information without the need to decrypt the data first. This is useful for privacy-preserving computations and secure cloud data handling, especially because it allows for meaningful manipulation without losing confidentiality (Hamza et al., 2022; S. J. Mohammed & Taha, 2022). Designing Encryption algorithms requires one to consider several competing factors; varying degrees of security, speed, computational burden, and overall resource requirements. In particular, security algorithms of high-grade demand onerous computational and temporal requirements, which is problematic for resource constrained environments (Panda, 2016; Yeow & Ng, 2023). Enhanced security without sacrificing efficiency is achievable through Hybrid Encryption methods which utilize both symmetric and asymmetric techniques. For example, a hybrid system may implement a symmetric key algorithm to encrypt the data and an asymmetric key algorithm to exchange the symmetric key (Akter et al., 2023; Chowdhary et al., 2020). Although symmetric and asymmetric algorithms are foundational to encryption, new techniques such as optical encryption and neural network-based encryption are being developed that are believed to provide improved security and efficiency (Yeow & Ng, 2023; F. Zhang et al., 2023).

Symmetric and asymmetric cryptography each has unique characteristics and benefits and drawbacks pertaining to secure communications in computer systems. With symmetric cryptography the same key is used to encrypt and decrypt information. This method is efficient and time sensitive since less computational power is used, thus making it useful in encrypting large amounts of data (Henriques & Vernekar, 2017; Q. Zhang, 2021). A major difficulty in symmetric encryption is the secure distribution of the authentication keys, since both parties in the communication require the same key, which may become exposed to eavesdroppers (Q. Zhang, 2021). Asymmetric cryptography, also known as public key encryption, utilizes key pairs consisting of a public key and a private key. The public key is open for anyone to use, but the private key is never shared. They work in pairs such that data encoded with one key can only be decoded with the other (Banerjee, 2024; Maqsood et al., 2017). It is good practice for the private key to never be sent to a receiver because it can be exposed to attacks. Nevertheless, asymmetric cryptography is more difficult to process and slower than symmetric cryptography, which makes it inefficient for large amounts of data (Hammad et al., 2020; Mcloone & Robshaw, 2006). Due to the limitations of each cryptography system, most applications use a hybrid of the two systems. In this methodology, asymmetric cryptography is used to safely share symmetric keys, while symmetric cryptography is used for the actual data transfer. This combination of methods improves security and performance since asymmetric cryptography is slower and more complex (Chowdhary et al., 2020; Q. Zhang, 2021).

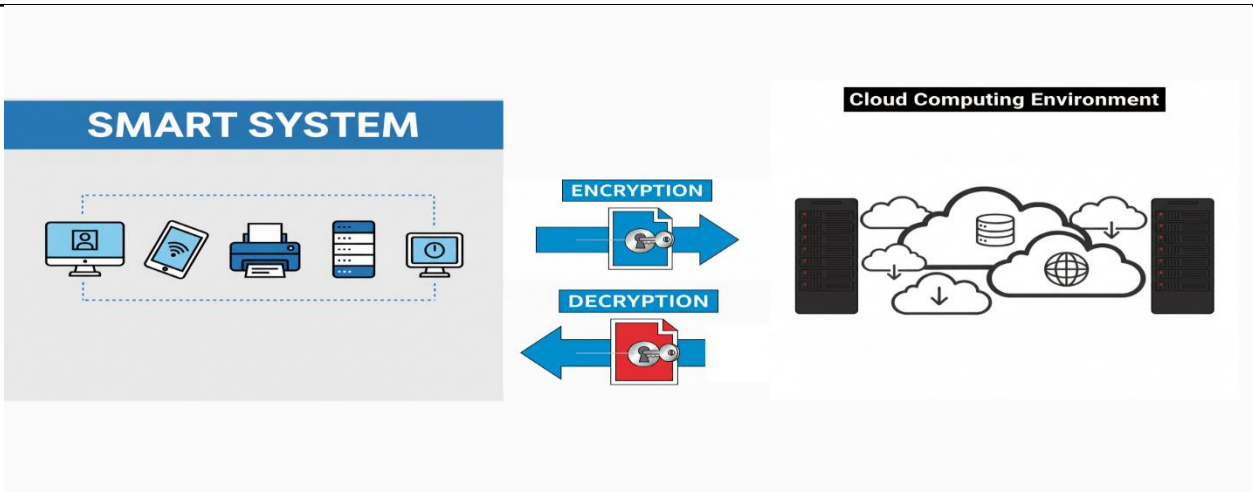

Fig. 2.1. Smart System: Encryption and Decryption

Encryption Algorithms

In the realm of computer science, encryption algorithms are imperative for the protection of data while preserving confidentiality during

transmission. Some of the most important symmetric encryption algorithms are DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Blowfish, which are primarily used for fast and efficient encryption of data.

DES (Data Encryption Standard):

Historically, DES was a symmetric-key algorithm frequently employed for encrypting and securing data. It utilizes a 56-bit key to encrypt data in 64-bit blocks. However, due to advancements in computing power, DES is considered insecure for various uses (Yassein et al., 2017).

AES (Advanced Encryption Standard):

AES is a more secure symmetric key algorithm and the new global standard for securing electronic data. AES guarantees optimum performance and strong security for three key lengths (128, 192, and 256 bits) (Mandal et al., 2012).

Blowfish:

Blowfish is a symmetric block cipher that is fast, effective, and economically secure. It works on 64-bit blocks and has key sizes between 32 and 448 bits, meaning it has a great deal of flexibility for varying security requirements (Alanzy et al., 2023).

Asymmetric algorithms,

like RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman, significantly secure data through the use of public and private key pairs which substantially improve data confidentiality in an encrypted format, secure key exchanges, and digital signatures.

Rivest–Shamir–Adleman (RSA):

The RSA algorithm is widely accepted in the provision of secure asymmetric encryption, as it employs the mathematical arms race and large integer factorization. RSA is able to secure sensitive information because of the encryption algorithm's use of large prime number manipulation (Q. Zhang, 2021).

Diffie–Hellman Key Exchange:

The algorithm is notable for the secure exchange of cryptographic keys in a public channel. It permits the transacting parties' to produce a shared secret cryptographic key intended for encryption under the symmetric algorithm (Yassein et al., 2017).

Elliptic Curve Cryptography (ECC):

The cryptography (ECC) is able to provide equivalent security to the RSA algorithm, while significantly reducing the key sizes, making it a great resource. The compact and rapid implementations are able to increase the security of data, and hence, ECC is

favoured in resource limited devices (Yassein et al., 2017).

Apart from the standards, SHA and MD5. are also used in the algorithm's construction for the security and integrity of data. A hash or message digest is a one-way irreversible construct of a data input, of a fixed and predetermined length. A hash cannot be reversed or decompiled to retrieve original data, therefore, it maintains security. The idiosyncratic attributes of the peculiar functions of cryptography make the functions of peculiar cryptography eternally remain as the only option to verify if a set of data is unchanged.

The functions of peculiar cryptography yield a one-of-a-kind code for every one-of-a-kind data set. On the case of the peculiar functions of cryptography to data sets for integrity purposes, the functions of cryptography verify if the data set is altered. The altered data set will generate a different value ascertaining a change has occurred (Windarta et al., 2022). The functions of peculiar cryptography are vital in the underlining of authentication of message and the digital signatures. The verification primitives' digital signatures offer are pivotal (Anwar et al., 2021; Sklavos & Koufopavlou, 2003). On cryptography, the functions of peculiar cryptography act as zero proofs of the content of a data set. Especially in keeping areas of preserved integrity without revealing the details of the data set (Achar et al., 2025). An efficient merchanism to verify and ascertain data integrity is provided by the functions of cryptography to large sets of data, digital certificates, and blockchain transactions (Anwar et al., 2021). The use of hash functions in blockchain technology further demonstrates how these functions maintain the integrity of data. Blockchain employs the use of cryptographic hash functions such as SHA-256 and SHA-3 as one of the primaries means of securing data and verifying transactions in the distributed ledger. This means that any and all changes to blockchain data will easily be recognized and tracked, maintaining the security and immutability of the blockchain (Kahri et al., 2016; Kuznetsov et al., 2024). Some hash algorithms provide more security than others. Older algorithms such as MD5 provide little to no security and are vulnerable to devastating collision attacks, where two different pieces of data produce the same hash. Consequently, newer algorithms such as SHA-2 and SHA-3 provide more secure enhancements and effective collision resistance (Alshuaibi et al., 2025; Kahri et al., 2016).

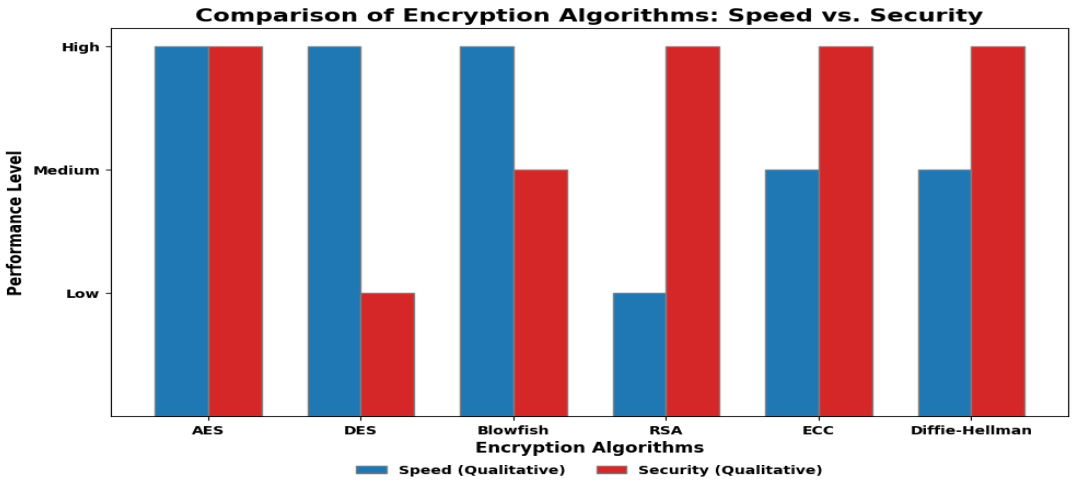

Fig. 3.1. The Comparison of Encryption Algrothms

Decryption is vital to ensure the completion of data recovery in an accurate and timely manner. This is done through the use of secure cryptographic algorithms and structures that provide protection to the integrity and privacy of data while facilitating effective key management and exchange. Several key factors surrounding the articulation of a given encryption and decryption will either aid or hinder the accurate recovery of data.

To begin with, effective key management encompasses secure key generation, exchange, and storage. For instance, Oblivious Key Management Systems (KMS) resorts to Oblivious Pseudorandom Functions (OPRF) to securely conceal keys and even offers unconditional safe transport of keys which are protected from breaches during transmission (Jarecki et al., 2019). In different environments, the dynamic management of keys incorporates card management strategies to regularly update keys and resources to avoid unauthorized access from any compromises, both past and future (Jarecki et al., 2019).

Collaborative key management protocols designed for Ciphertext Policy Attribute-Based Encryption (CP-ABE) facilitate the mitigation of key escrow and enhance the decryption amortization process through the decentralized generation and storage of keys and resources without the burden of new infrastructure (Lin et al., 2017). Therefore, authorized users are guaranteed the ability to decrypt and retrieve data, preserving its integrity throughout the process.

Hybrid (RSA & AES) encryption and other contemporary encryption techniques utilize several different keys (public, private, and secret keys) for encryption and decryption, which helps keep data secure and enhances security through redundancy (Mahalle & Shahade, 2014). Asymmetric cryptography helps in safe and secure key exchanges, which help in accurate decryption, while minimizing the chances of an adversary intercepting and abusing the keys.

Incorporating new techniques, such as the use of blockchain in key management systems, improves security through the decentralization of key storage and enhances the integrity and auditability of the stored and transferred data (Shakor et al., 2024). Such approaches minimize reliance on centralized systems which are the primary targets of security attacks while providing robust systems for key exchange and authentication.

Table 3.1. Comparative Analysis of Core Cryptographic Algorithms and Hash Functions

Algorithm	Type	Key Features	Strengths	Weaknesses	Applications	Reference
AES	Symmetric	128, 192, 256-bit keys; fast and secure	High efficiency; strong security; global standard	Key distribution challenges	Cloud storage, IoT, machine learning data security	[Mandal et al., 2012; Yeow & Ng, 2023; Ibrahim et al., 2024]
DES	Symmetric	56-bit key; 64-bit block size	Historically widely used; fast for its time	Insecure due to short key length; vulnerable to brute-force attacks	Legacy systems (largely replaced by AES)	[Yassein et al., 2017; Panda, 2016]
Blowfish	Symmetric	32–448-bit keys; 64-bit blocks	Flexible key sizes; fast and secure	Less common than AES; block size limitations	Data encryption in resource-constrained environments	[Alanzy et al., 2023]

RSA	Asymmetric	Public/private key pair; based on prime factorization	Secure key exchange; widely used for digital signatures	Slower than symmetric; vulnerable to quantum attacks	Online voting, secure key exchange, digital signatures	[Q. Zhang, 2021; Sihotang et al., 2020; Rahman et al., 2024]
ECC	Asymmetric	Smaller key sizes; based on elliptic curves	High security with smaller keys; efficient for resource-constrained devices	Complex implementation; vulnerable to quantum attacks	IoT, mobile devices, secure communications	[Yassein et al., 2017; Alluhaidan & Prabu, 2023]
Diffie-Hellman	Asymmetric	Secure key exchange over public channels	Enables secure symmetric key sharing	Not used for data encryption directly	Key exchange for symmetric encryption	[Yassein et al., 2017]
SHA-2/SHA-3	Hash Function	One-way, collision-resistant	Ensures data integrity; used in blockchain	Not for encryption; older versions vulnerable to collisions	Blockchain, digital signatures, data integrity verification	[Kahri et al., 2016; Kuznetsov et al., 2024; Alshuaibi et al., 2025]
MD5	Hash Function	Fast, fixed-length output	Simple and fast	Vulnerable to collision attacks; considered insecure	Legacy systems (not recommended for security)	[Kahri et al., 2016; Alshuaibi et al., 2025]

With regard to the application of cryptography, system architecture, specific application needs, and the deployed techniques, there are multiple influences on the secure system's decryption efficiency and reliability.

Algorithm Type and Complexity: The type of cryptographic algorithm chosen affects the decryption effort and its reliability. Each algorithm, such as RSA and AES, hybridizes, and as a result,

affects its decryption quickly and securely. For example, a hybrid encryption technique combines RSA with AES-128 and exhibits a notable improvement in security and efficiency in cloud computing (Akter et al., 2023). Also, dynamic-key neural network-based algorithms can improve speed and anti-deskilling performance (Liang et al., 2019; Yeow & Ng, 2023).

Available Computational Resources:
The available computational resources, particularly for weaker IoT devices, are limited. For decryption throughput to improve without overburdening the device resources, lightweight cryptography, such as uBlock, is utilized. Liu et al. (2022) reports that this approach achieves performance levels needed for high-bandwidth communications, for instance, 5G.

Support for Parallel Processing:
The ability to perform parallel processing on cryptographic algorithms can enhance decryption speed and, most importantly, reliability. The use of spatiotemporally chaotic cryptosystems is one technique that allows parallel decryption flows, thus, increasing performance with high-security levels maintained against interference (Lü et al., 2004).

Integration with Other Security Protocols:
The encryption's addition of other protocols, particularly HMAC for data integrity, improves the security framework. This hybrid model can reduce risks and improve reliability during data transmission (Akter et al., 2023).

Application-Specific Requirements: Trade-offs between decryption speed, security, and resources can be predetermined by a given use case. For example, healthcare data encryption which requires strong security, can use quantum cryptography, which is also efficient and precise (Basha, 2024).

Advancements in Technology:
In nanotechnology and computation, continuous improvements will lead to better algorithm performance. Increases in throughput by a factor of two, as driven by advances in computation, is a reasonable expectation (Liu et al., 2022).

Applications
Data confidentially and unauthorized access protection relies on effective encryption and decryption techniques. AES, DES, and RSA are examples of encryption standards. In terms of performance, AES, a symmetric encryption algorithm, is suitable for securing cloud-stored electronic documents and data protected in machine learning applications (Ibrahim et al., 2024; Mota et al., 2017; Yeow & Ng, 2023). Processing data in cloud environments using homomorphic encryption permits users to execute encrypted documents while safeguarding confidentiality (Chauhan et al., 2015). Furthermore, dynamic key generation and decentralized key storage using blockchain technology provide enhanced security and protection against key compromise (Shakor et al., 2024).
Encryption and cryptography techniques like digital signatures and hashing serve to ensure transaction data within a blockchain remains private and unaltered. In a blockchain network, homomorphic and cryptographic attribute encryption techniques allow access to secured data while maintaining privacy (Wang et al., 2024; Xu et al., 2022). Other than described above, blockchain technology employs digital signatures for transaction verification and immutability of data via cryptographic principles (Zhai et al., 2019). Digital signatures are essential in certifying the validity and integrity of messages and documents. These techniques are prevalent in digital communication, utilizing RSA and the Digital Signature Algorithm to integrate signature generation and verification, and public key cryptosystems for enhanced security (Aufa et al., 2018). In IoT communication systems, the integration of interconnected devices and the need for robust security pose challenges in the use of limited resources, thereby necessitating encryption. Efforts have been made to optimize the use of resources while securing devices interconnected in wireless networks, including the use symmetric and asymmetric techniques as well as Elliptic Curve Cryptography (ECC) (Alluhaidan & Prabu, 2023; Mousavi et al., 2021). Mixed or hybrid encryption techniques enact the use multiple encryption methods while providing confidentiality and

integrity of the resources or data (Kumar & Kumar, 2024; Yousefi & Jameii, 2017).

Security Challenges

All encryption and decryption algorithms have specific weaknesses in security. One such weakness is brute-force attacks where all potential keys are tried until the right one is found. This is a major concern for all underprotected algorithms with shorter keys. Shorter keys can be guessed and cracked in a much shorter period of time (Panda, 2016; Ramesh & Suruliandi, 2013). Key leakage is also a major weakness, in addition to key management problems in which encryption keys are stored or sent in an unreliably weak way, and unauthorized users gain access (Gour et al., 2024). The aforementioned weaknesses demonstrate the need for robust encryption algorithms, in conjunction with poorly managed weak keys to improve data security.

The surge in quantum computing capabilities creates new threats to traditional cryptography. Quantum computers can conduct integer factorization and compute discrete logarithms at unprecedented speeds, making the cornerstone computations of encryption ineffective. RSA and elliptic curve cryptography (ECC) as well as even symmetric-key algorithms like AES are particularly at risk, as the threats to these algorithms are predicated on the feasibility of the computations that protect the algorithms (Sodiya et al., 2024). Ajala et al. (2024) and Rawal & Curry (2024) note that Shor's algorithm enables quantum computers to break RSA and ECC, factoring large numbers in a way exponentially faster than what classical computers can accomplish.

In response, cryptographers are working on post-quantum cryptography (PQC), focusing on quantum-attack resilient algorithms. Techniques based on lattice, hash, and codes are seen as the most resilient forms of cryptography, as PQC will utilize these methods (Cherkaoui Dekkaki et al., 2024). Gitonga (2025) discusses hybrid cryptographic systems to PQC, which creates a bridge to PQC, while still cryptographically supporting legacy systems. Brute-force attacks pose a fundamental risk to the security of encryption and decryption algorithms in which attackers gain access to the encryption key by unscrupulously trying all the possible combinations in a systematic fashion. This method is particularly dangerous for encryption standards which use short keys, as short keys are guessed and cracked in a matter of seconds (Panda, 2016; Ramesh & Suruliandi, 2013). A third and most important security challenge arises from key leakages and key management when keys are poorly stored and poorly secured, which allow unauthorized individuals to gain access and utilize the keys (Gour et al., 2024). This and other security vulnerabilities stress the use of strong encryption standards, as well as key management systems, for the improvement of data security.

Quantum computing has begun to breach the gaps of current systems of cyber security. This breach is the result of breaking the mathematics that form the basis of modern systems of cyber security. Quantum computers can process immense amounts of data which can lead to the rapid computation of fundamental mathematical problems. Quantum computers can lead to the rapid computation of fundamental mathematical problems that imply the breaking of the RSA, discrete, and symmetric key algorithm and systems of cyber security like AES (Sodiya et al., 2024). Cryptanalysts can use Shor's algorithm to break RSA and ECC systems of cyber security which constitute some of the weakest systems that can be attacked using quantum computers (Ajala et al., 2024; Rawal & Curry, 2024). In a bid to solve the problems of cyber security that quantum computing breaches, the current focus has switched to post quantum cryptography (PQC) which aims to solve the problem of cyber security in a quantum environment. Cryptography in the form of lattices, hash, and code is one of the areas of post quantum cryptography being explored which proves to be resilient to quantum cryptography (Cherkaoui Dekkaki et al., 2024). The transition to PQC can be in the form of hybrid cryptography systems which can be cryptography systems that offer backward compatibility that can transition and form quantum cryptography systems (Gitonga, 2025).

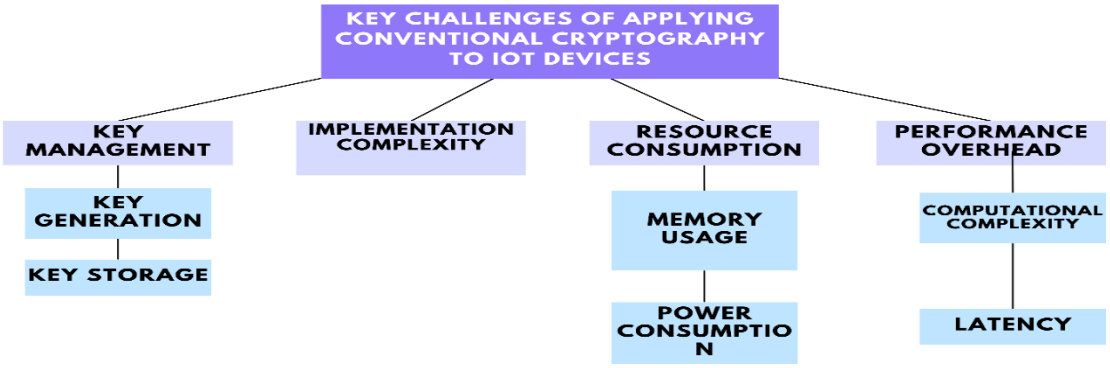

Fig.5.1 Key Challenges of applying Conventional cryptography to IOT Devices

Future Trends

The emergence of quantum computing technologies brings with it the potential to dramatically change the methods used for the encryption and decryption of data. Current methods of encryption, such as RSA and ECC, will become obsolete, as quantum algorithms will be able to perform integer factorization and solve discrete logarithm problems in a fraction of the time it takes classical algorithms to do so. This leaves encryption methods highly vulnerable to Shor's algorithm (Sharma et al., 2023). The newer algorithms developed in post-quantum cryptography (PQC) will provide additional layers of protection, with the intention of remaining effective against quantum computing attacks. Such techniques incorporate lattice and multivariate cryptography, hash-based signatures, and code-based cryptography. Each of the outlined methods attempts to protect data from the significant and aggressive computational resources that quantum computing will have relative to classical computing (Mavroeidis et al., 2018). In particular, lattice-based cryptography is a strong candidate for a range of applications such as encryption, digital signatures, and key exchange, because it combines strong security and computational efficiency (Nejatollahi et al., 2019). Integrating PQC entails performance trade-offs along with current systems and the existing infrastructure's compatibility. Global efforts to plan and ensure the new cryptographic methods can be combined and integrated will be crucial to achieving widespread adoption (Singh et al., 2024). Besides the above, stakeholders in the cybersecurity community will also need to ensure systems surviving future quantum threats (Sodiya et al., 2024).

PQC systems will require more than the quantum attack focus. Characteristic challenges like increased key sizes and the computational cost of some new cryptographic methods will need to be solved. Promising solutions, like the application of genetic algorithms to optimize key generation in lattice-based cryptography to eliminate the need of certain memory and computation resources, may be the answer to deploying PQC in resource-constrained settings (Al Attar & Mohammed, 2025). All in all, the cryptographic community is looking to PQC to be the first of many future efforts to ensure disruptive quantum computing technologies will not severely alter the digital infrastructure and communication for it. To achieve this will require more than just PQC, and effort will be needed in the areas of research, development, and collaboration throughout the cybersecurity ecosystem to secure the data for the new quantum age (Ajala et al., 2024).

In modern security landscapes, the synergies of Artificial Intelligence (AI) and light-weight cryptography provide solutions for complex and evolving security challenges. AI-Driven Cybersecurity has the ability to enhance digital security systems by facilitating the sophisticated instruments needed for intrusion detection, anomaly detection, and incident response systems (Folorunso et al., 2024; Thapaliya

& Bokani, 2024). Advanced forms of AI, like machine learning and deep learning, can rapidly analyze and interpret large volumes of data to detect patterns similar to cyber-threats, which include zero-day vulnerabilities, advanced persistent threats (APTs) and ransomware (Folorunso et al., 2024; Thapaliya & Bokani, 2024). AI systems increase the precision and speed of real-time threat detection in a system, making them invaluable in the evolving world of cyber security (Hu et al., 2021; Sarker et al., 2021). Moreover, AI technologies-implemented Automated Security Compliance Monitoring Systems assist in the routine, compliance-focused security task of auditing which parallels the organization-focused compliance requirements of the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) (Folorunso et al., 2024). Lastly, deploying AI systems in cyber security also invokes the underlying risks of adversarial attacks, bad data, and black-box AI systems (Jeong, 2020). These risks demand further research to ensure that the cyber security shields offered by AI systems are integrated with sufficient cyber security and protective measures (Weng & Wu, 2024).

Unlike other types of cryptography, lightweight cryptography manages the trustworthiness of data in IoT systems. Cryptography takes up too many resources for IoT devices and systems, which have limited computation, memory, and power as IoT devices are battery powered (Dewamuni et al., 2023; Dhanda et al., 2020). Algorithms in lightweight cryptography generally try to optimize the resource footprint needed to perform basic security tasks such as data encryption, integrity checks, and active key exchange. With such resource optimized cryptography, sensitive data can be exchanged even in systems where traditional cryptography is infeasible (F. Li, 2024; Schinianakis, 2017). In the secured IoT environment, lightweight cryptography mitigates the impact of eavesdropping, denial of service, and data fabrication attacks. It's lightweight cryptography that finally enforces the confidentiality and integrity of data streams in and out of IoT devices (Bhardwaj et al., 2017; Sable et al., 2024). Constructing appropriate security primitives such as block ciphers and hash functions encourage the realization of secured and dependably functioning IoT systems (Amrita et al., 2024; Buchanan et al., 2017).

Conclusion

There are plenty of reasons for the constant development of new methods in encryption and decryption. As time goes on, the methods we use to encrypt and protect our data might become weak against attacks. This is why it is important to work on encryption technology. This will ensure that sensitive information is constant and will remain intact (Abudalou, 2024; Nwobodo et al., 2024). The innovations within the field are important to keep pace with the rise of new technologies, such as quantum computing. Quantum computing creates the opportunity to shatter the methods we use to encrypt our data. New methods that incorporate quantum-resistant algorithms are innovations that work to mitigate the risks of quantum computing (Nguyen et al., 2024). The use of artificial intelligence (AI) in encryption can expand the enhancements of digital data secrecy and protection. This is due to the new ability to find patterns and outliers in large information and the predicted behavior that developed systems lack. These advancements will improve our ability to identify and resolve forming issues due to the lack of time, and therefore, the strength of the proposed systems will increase drastically (Folorunso et al., 2024; Nitaj & Rachidi, 2023).

New approaches and frameworks for protecting data are developed and implemented by advanced algorithms and technologies for long-term data security. Take blockchain technology, for example. It implements decentralized and more secure key management for data integrity. Risks involved with centralized key storage are mitigated by blockchain technology. “Encryption keys and related metadata are stored … distributed ledgers” (Shakor et al., 2024). Modern cryptography through homomorphic encryption technologies also works to data security. “It allows computations … to be performed … encrypted data and … decryption” (Chauhan et al., 2015). Data threat automation by machine learning and advanced neural networks works through lots of data rapidly, making them essential for long-term data safety. “They analyze large volumes and breaches” (M. S. Mohammed & Talib, 2024; Okoli

et al., 2024). The automation of threat detection and data breach identification works in real-time to defend data. "It improves response and accuracy" (M. S. Mohammed & Talib, 2024; Okoli et al., 2024). Automating these processes for rapid adaptation of security frameworks for fast-evolving threats is essential and advanced algorithms are key to making that happen.

References

Abudalou, M. (2024). Enhancing Data Security through Advanced Cryptographic Techniques. *International Journal of Computer Science and Mobile Computing*, *13*(1), 88–92. https://doi.org/10.47760/ijcsmc.2024.v13i01.007

Achar, S. D., Nandi, S., P, T., & Nandi, S. (2025). LiteHash: Hash Functions for Resource-Constrained Hardware. *ACM Transactions on Embedded Computing Systems*, *24*(2), 1–17. https://doi.org/10.1145/3677181

Ajala, O., Ofodile, O., Daraojimba, A., Arinze, C., & Okoye, C. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, *10*(1), 321–329. https://doi.org/10.30574/msarr.2024.10.1.0038

Akter, R., Soheli, S. J., Suha, N. J., Rahman, F., & Khan, M. A. R. (2023). RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing. *International Journal of Computational and Applied Mathematics & Computer Science*, *3*, 60–71. https://doi.org/10.37394/232028.2023.3.8

Al Attar, T. N. A., & Mohammed, R. N. (2025). Optimization of Lattice-Based Cryptographic Key Generation using Genetic Algorithms for Post-Quantum Security. *UHD Journal of Science and Technology*, *9*(1), 93–105. https://doi.org/10.21928/uhdjst.v9n1y2025.pp93-105

Alanzy, M., Alomrani, R., Almutairi, S., & Alqarni, B. (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. *Applied Sciences*, *13*(21), 11771. https://doi.org/10.3390/app132111771

Alluhaidan, A. S. D., & Prabu, P. (2023). End-to-End Encryption in Resource-Constrained IoT Device. *IEEE Access*, *11*, 70040–70051. https://doi.org/10.1109/access.2023.3292829

Alshuaibi, A., Maayah, M., & Arshad, M. W. (2025). A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security. *Journal of Cyber Security and Risk Auditing*, *2025*(3), 42–56. https://doi.org/10.63180/jcsra.thestap.2025.3.6

Amrita, A., Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight Cryptography for Internet of Things: A Review. *EAI Endorsed Transactions on Internet of Things*, *10*. https://doi.org/10.4108/eetiot.5565

Anwar, M. R., Apriani, D., & Adianita, I. R. (2021). Hash Algorithm In Verification Of Certificate Data Integrity And Security. *Aptisi Transactions on Technopreneurship (ATT)*, *3*(2), 65–72. https://doi.org/10.34306/att.v3i2.212

Aufa, F. J., Endroyono, E., & Affandi, A. (2018, August 1). *Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm*. https://doi.org/10.1109/icstc.2018.8528584

Banerjee, S. (2024). Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations. *International Journal of Advanced Research in Science, Communication and Technology*, 607–620. https://doi.org/10.48175/ijarsct-18097

Basha, C. (2024). Enhancing Healthcare Data Security Using Quantum Cryptography for Efficient and Robust Encryption. *Journal of Electrical Systems*, *20*(5s), 1993–2000. https://doi.org/10.52783/jes.2535

Bhardwaj, I., Bansal, M., & Kumar, A. (2017). *A review on lightweight cryptography algorithms for data security and authentication in IoTs*. *4*, 504–509.

https://doi.org/10.1109/ispcc.2017.8269731

Buchanan, W. J., Li, S., & Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology*, *1*(3–4), 187–201. https://doi.org/10.1080/23742917.2017.1384917

Chauhan, K. K., Sanger, A. K. S., & Verma, A. (2015). *Homomorphic Encryption for Data Security in Cloud Computing*. 206–209. https://doi.org/10.1109/icit.2015.39

Cherkaoui Dekkaki, K., Cano, M.-D., & Tasic, I. (2024). Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies*, *12*(12), 241. https://doi.org/10.3390/technologies12120241

Chowdhary, C. L., Patel, P. V., Ijaz, M. F., Attique, M., Perumal, K., & Kathrotia, K. J. (2020). Analytical Study of Hybrid Techniques for Image Encryption and Decryption. *Sensors*, *20*(18), 5162. https://doi.org/10.3390/s20185162

Dewamuni, Z., Azam, S., Thennadil, S., & Shanmugam, B. (2023). Bibliometric Analysis of IoT Lightweight Cryptography. *Information*, *14*(12), 635. https://doi.org/10.3390/info14120635

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. *Wireless Personal Communications*, *112*(3), 1947–1980. https://doi.org/10.1007/s11277-020-07134-3

Elminaam, D., Kader, H., & Hadhoud, M. (2010). Evaluating the Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*, *10*(3), 213–219. https://doi.org/10.6633/ijns.201005.10(3).06

Folorunso, A., Okonkwo, R., Olawumi, T., Adewa, A., & Adewumi, T. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, *21*(1), 167–184. https://doi.org/10.30574/gjeta.2024.21.1.0193

Gitonga, C. K. (2025). The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography. *European Journal of Information Technologies and Computer Science*, *5*(1), 1–10. https://doi.org/10.24018/compute.2025.5.1.146

Gour, A., Singh, G., Kaur, G., & Singh Malhi, S. (2024). Hybrid Cryptographic Approach: For Secure Data Communication using Block Cipher Techniques. *E3S Web of Conferences*, *556*, 01048. https://doi.org/10.1051/e3sconf/202455601048

Hammad, B. T., Jamil, N., Ahmed, I. T., & Sagheer, A. M. (2020). A comparative review on symmetric and asymmetric DNA-based cryptography. *Bulletin of Electrical Engineering and Informatics*, *9*(6), 2484–2491. https://doi.org/10.11591/eei.v9i6.2470

Hamza, R., Hassan, A., Ali, A., Yousif, A., Bashir, M. B., Tawfeeg, T. M., & Alqhtani, S. M. (2022). Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms. *Entropy*, *24*(4), 519. https://doi.org/10.3390/e24040519

Henriques, M. S., & Vernekar, N. K. (2017, May 1). *Using symmetric and asymmetric cryptography to secure communication between devices in IoT*. https://doi.org/10.1109/iciota.2017.8073643

Hu, Y., Li, W., Li, K., Zhang, J., Kuang, W., Qin, Z., Li, K., & Gao, Y. (2021). Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys*, *55*(1), 1–36. https://doi.org/10.1145/3487890

Ibrahim, A., Sekhar, R., Tawfeq, J. F., Radhi, A. D., & Salih, S. Q. (2024). Security and Privacy Protection for Online Electronic Documents Based on Novel Encryption Techniques. *Journal of Intelligent Systems and Internet of Things*, *11*(1), 21–28. https://doi.org/10.54216/jisiot.110103

Jarecki, S., Krawczyk, H., & Resch, J. (2019). *Updatable Oblivious Key Management for Storage Systems*. 379–393. https://doi.org/10.1145/3319535.3363196

Jeong, D. (2020). Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, *8*, 184560–184574. https://doi.org/10.1109/access.2020.3029280

Kahri, F., Mestiri, H., Bouallegue, B., & Machhout, M. (2016). High Speed FPGA Implementation of Cryptographic KECCAK Hash Function Crypto-Processor. *Journal of Circuits, Systems and Computers*, *25*(04), 1650026. https://doi.org/10.1142/s0218126616500262

Kumar, D., & Kumar, M. (2024). Hybrid Cryptographic Approach for Data Security Using Elliptic Curve Cryptography for IoT. *International Journal of Computer Network and Information Security*, *16*(2), 42–54. https://doi.org/10.5815/ijcnis.2024.02.04

Kuznetsov, O., Kanonik, D., Karashchuk, S., Rusnak, A., Yezhov, A., & Kuznetsova, K. (2024). Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access*, *12*, 1. https://doi.org/10.1109/access.2024.3384705

Li, D., Wu, J.-M., Liang, Z.-H., Li, L.-Y., Dong, X., Chen, S.-K., Fu, T., Wang, X.-L., Wang, Y.-Z., & Song, F. (2022). Sophisticated yet Convenient Information Encryption/Decryption Based on Synergistically Time-/Temperature-Resolved Photonic Inks. *Advanced Science (Weinheim, Baden-Wurttemberg, Germany)*, *10*(5), 2206290. https://doi.org/10.1002/advs.202206290

Li, F. (2024). Application and challenges of artificial intelligence in cybersecurity. *Applied and Computational Engineering*, *47*(1), 262–268. https://doi.org/10.54254/2755-2721/47/20241480

Liang, C., Ma, J., Zhang, Q., & Li, K. (2019). Research on neural network chaotic encryption algorithm in wireless network security communication. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1476-3

Lin, G., Hong, H., & Sun, Z. (2017). A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. *IEEE Access*, *5*, 9464–9475. https://doi.org/10.1109/access.2017.2707126

Liu, C., Xu, J., Zhang, Y., Xiang, S., & Zhao, J. (2022). Ensuring the Security and Performance of IoT Communication by Improving Encryption and Decryption With the Lightweight Cipher uBlock. *IEEE Systems Journal*, *16*(4), 5489–5500. https://doi.org/10.1109/jsyst.2022.3140850

Lü, H., Hu, G., Li, X., Kuang, J., Wang, S., Tang, G., & Ye, W. (2004). A new spatiotemporally chaotic cryptosystem and its security and performance analyses. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *14*(3), 617–629. https://doi.org/10.1063/1.1772731

Mahalle, V. S., & Shahade, A. K. (2014). *Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm*. 146–149. https://doi.org/10.1109/inpac.2014.6981152

Mandal, A. K., Tiwari, A., & Parakash, C. (2012). *Performance evaluation of cryptographic algorithms: DES and AES*. 1–5. https://doi.org/10.1109/sceecs.2012.6184991

Maqsood, F., Mumtaz, M., Ahmed, M., & Ali, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6). https://doi.org/10.14569/ijacsa.2017.080659

Mavroeidis, V., Vishi, K., D, M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*,

9(3). https://doi.org/10.14569/ijacsa.2018.090354

Mcloone, M., & Robshaw, M. J. B. (2006). *Public Key Cryptography and RFID Tags* (pp. 372–384). Springer Berlin Heidelberg. https://doi.org/10.1007/11967668_24

Mohammed, M. S., & Talib, H. A. (2024). Using Machine Learning Algorithms in Intrusion Detection Systems: A Review. *Tikrit Journal of Pure Science*, *29*(3), 63–74. https://doi.org/10.25130/tjps.v29i3.1553

Mohammed, S. J., & Taha, D. B. (2022). *Performance Evaluation of RSA, ElGamal, and Paillier Partial Homomorphic Encryption Algorithms*. 89–94. https://doi.org/10.1109/csase51777.2022.9759825

Mota, A. V., Azam, S., Yeo, K. C., Shanmugam, B., & Kannoorpatti, K. (2017). *Comparative analysis of different techniques of encryption for secured data transmission*. *5*, 231–237. https://doi.org/10.1109/icpcsi.2017.8392158

Mousavi, S. K., Ghaffari, A., Afshari, H., & Besharat, S. (2021). Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), 1515–1555. https://doi.org/10.1007/s11276-020-02535-5

Muhammad, A. S., & Özkaynak, F. (2021). SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs. *Symmetry*, *13*(5), 824. https://doi.org/10.3390/sym13050824

Nejatollahi, H., Dutt, N., Cammarota, R., Regazzoni, F., Banerjee, I., & Ray, S. (2019). Post-Quantum Lattice-Based Cryptography Implementations. *ACM Computing Surveys*, *51*(6), 1–41. https://doi.org/10.1145/3292548

Nguyen, T., Hautamäki, J., & Sipola, T. (2024). Machine Learning Applications of Quantum Computing: A Review. *European Conference on Cyber Warfare and Security*, *23*(1), 322–330. https://doi.org/10.34190/eccws.23.1.2258

Nitaj, A., & Rachidi, T. (2023). Applications of Neural Network-Based AI in Cryptography. *Cryptography*, *7*(3), 39. https://doi.org/10.3390/cryptography7030039

Noor, N. S., Chahl, J., Hammood, D. A., & Al-Naji, A. (2022). A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication. *Computers*, *11*(3), 39. https://doi.org/10.3390/computers11030039

Nwobodo, L., Nwaimo, C., & Adegbola, A. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. GSC *Advanced Research and Reviews*, *19*(3), 203–214. https://doi.org/10.30574/gscarr.2024.19.3.0211

Okoli, U., Adewusi, A., Abrahams, T., & Obi, O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286–2295. https://doi.org/10.30574/wjarr.2024.21.1.0315

Othman, S. B., Youssef, H., Trad, A., & Bahattab, A. A. (2014). Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption. *Wireless Personal Communications*, *80*(2), 867–889. https://doi.org/10.1007/s11277-014-2061-z

Panda, M. (2016). *Performance analysis of encryption algorithms for security*. 278–284. https://doi.org/10.1109/scopes.2016.7955835

Rahman, K. N., Hridoy, M. W., Mizanur Rahman, M., Islam, M. R., & Banik, S. (2024). Highly secured and effective management of app-based online voting system using RSA encryption and decryption. *Heliyon*, *10*(3), e25373. https://doi.org/10.1016/j.heliyon.2024.e25373

Ramesh, A., & Suruliandi, A. (2013). *Performance analysis of encryption algorithms for Information Security*. *42*, 840–844. https://doi.org/10.1109/iccpct.2013.6528957

Rawal, B. S., & Curry, P. J. (2024). Challenges and opportunities on the horizon of post-quantum cryptography. *APL Quantum*, *1*(2). https://doi.org/10.1063/5.0198344

Sable, N. P., Rathod, S. B., Parlewar, P., Rathod, R. R., Rathod, V. U., & Waghmode, S. T. (2024). Efficient lightweight cryptography for resource-constrained WSN nodes. *Journal of Discrete Mathematical Sciences and Cryptography*, *27*(2-A), 349–359. https://doi.org/10.47974/jdmsc-1888

Sarker, I. H., Nowrozy, R., & Furhad, M. H. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3). https://doi.org/10.1007/s42979-021-00557-0

Schinianakis, D. (2017). Alternative Security Options in the 5G and IoT Era. *IEEE Circuits and Systems Magazine*, *17*(4), 6–28. https://doi.org/10.1109/mcas.2017.2757080

Shakor, M. Y., Alfarhood, S., Zhu, M., Safran, M., & Khaleel, M. I. (2024). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. *IEEE Access*, *12*, 26334–26343. https://doi.org/10.1109/access.2024.3351119

Sharma, S., Ramkumar, K. R., Mittal, S., Kaur, A., Singh, B., & Hasija, T. (2023). *Post-quantum Cryptography: A Solution to the Challenges of Classical Encryption Algorithms* (pp. 23–38). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-6383-4_3

Sihotang, H. T., Efendi, S., Mawengkang, H., & Zamzami, E. M. (2020). Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security. *Journal of Physics: Conference Series*, *1641*(1), 012042. https://doi.org/10.1088/1742-6596/1641/1/012042

Singh, N., Arya, V., Chui, K. T., Singh, S. K., Kumar, S., Bansal, R., & Rawat, Y. (2024). *Next Gen Security With Quantum-Safe Cryptography* (pp. 133–166). Igi Global Scientific. https://doi.org/10.4018/979-8-3693-5330-1.ch006

Sklavos, N., & Koufopavlou, O. (2003). *On the hardware implementations of the SHA-2 (256, 384, 512) hash functions*. *5*, V–156. https://doi.org/10.1109/iscas.2003.1206214

Sodiya, E., Atadoga, A., Amoo, O., & Umoga, U. (2024). Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets. *Global Journal of Engineering and Technology Advances*, *18*(2), 049–064. https://doi.org/10.30574/gjeta.2024.18.2.0026

Thapaliya, S., & Bokani, A. (2024). Leveraging artificial intelligence for enhanced cybersecurity: insights and innovations. *SADGAMAYA*, *1*(1), 46–52. https://doi.org/10.3126/sadgamaya.v1i1.66888

Wang, G., Li, C., Dai, B., & Zhang, S. (2024). Privacy-Protection Method for Blockchain Transactions Based on Lightweight Homomorphic Encryption. *Information*, *15*(8), 438. https://doi.org/10.3390/info15080438

Weng, Y., & Wu, J. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *5*(1), 392–399. https://doi.org/10.60087/jaigs.v5i1.211

Windarta, S., Pranggono, B., Suryadi, S., Gunawan, T. S., & Ramli, K. (2022). Lightweight Cryptographic Hash Functions: Design Trends, Comparative Study, and Future Directions. *IEEE Access*, *10*, 82272–82294. https://doi.org/10.1109/access.2022.3195572

Xu, G., Ma, C., Zhang, J., & Cliff, U. G. O. (2022). An efficient blockchain-based privacy-preserving scheme with attribute and homomorphic encryption. *International*

Journal of Intelligent Systems, *37*(12), 10715–10750. https://doi.org/10.1002/int.22946

Yang, M., Bourbakis, N., & Li, S. (2004). Data-image-video encryption. *IEEE Potentials*, *23*(3), 28–34. https://doi.org/10.1109/mp.2004.1341784

Yassein, M. B., Qawasmeh, E., Aljawarneh, S., Khamayseh, Y., & Mardini, W. (2017). *Comprehensive study of symmetric key and asymmetric key encryption algorithms*. 1–7. https://doi.org/10.1109/icengtechnol.2017.8308215

Yeow, S.-Q., & Ng, K.-W. (2023). Neural Network Based Data Encryption: A Comparison Study among DES, AES, and HE Techniques. *JOIV : International Journal on Informatics Visualization*, *7*(3–2), 2086. https://doi.org/10.30630/joiv.7.3-2.2336

Yousefi, A., & Jameii, S. M. (2017). *Improving the security of internet of things using encryption algorithms*. 1–5. https://doi.org/10.1109/iciota.2017.8073627

Zhai, S., Yang, Y., Zhao, J., Qiu, C., & Li, J. (2019). Research on the Application of Cryptography on the Blockchain. *Journal of Physics: Conference Series*, *1168*(3), 032077. https://doi.org/10.1088/1742-6596/1168/3/032077

Zhang, F., Guo, Y., Pu, M., Chen, L., Xu, M., Liao, M., Li, L., Li, X., Ma, X., & Luo, X. (2023). Meta-optics empowered vector visual cryptography for high security and rapid decryption. *Nature Communications*, *14*(1). https://doi.org/10.1038/s41467-023-37510-z

Zhang, Q. (2021). *An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption*. *7*, 616–622. https://doi.org/10.1109/cds52072.2021.00111