

Data Encryption Algorithms and Risk Management

¹Chris Gilbert ²Mercy Abiola Gilbert

¹Professor ²Instructor

¹Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University/chrisgilbertp

²Department of Guidance and Counseling/College of Education/William V.S. Tubman University/mercyabiola

DOI : <https://doi.org/10.51583/IJLTEMAS.2025.140300054>

Received: 31 March 2025; Accepted: 04 April 2025; Published: 18 April 2025

Abstract: In today's digital era, data is increasingly viewed as the new "green gold," making robust information security more critical than ever. This research investigates modern encryption algorithms alongside comprehensive risk management strategies to protect enterprise data. By systematically comparing symmetric, asymmetric, and hash-based encryption methods, the study reveals the inherent trade-offs between computational performance and security. A multifaceted methodology—combining literature review, algorithmic evaluation, multivariate risk assessment, and real-world case studies—is employed to examine advanced encryption techniques such as Twofish, RC6, AES, RSA, and ECC. Additionally, emerging challenges, including the threats posed by quantum computing and the energy constraints of IoT and cloud environments, are discussed. The findings underscore the necessity of a balanced encryption strategy integrated with robust risk management practices to ensure the confidentiality, integrity, and availability of sensitive information. The paper concludes with recommendations for future research and practical applications aimed at enhancing data protection in an ever-evolving digital landscape.

Keywords: Data Encryption, Risk Management, Symmetric Encryption, Asymmetric Encryption, Cryptographic Hash Functions, Advanced Encryption Algorithms, Quantum Cryptography, IoT Security, Cloud Security, Multivariate Risk Assessment.

I. Introduction

In the first part of this paper, we discussed the significance of data security in modern data environments, the necessity of keeping data in an encrypted format, and why encryption and decryption keys should be stored separately (Boulegghimat, Boudouda & Hacini, 2024; Gilbert & Gilbert, 2025a). The concepts, structure, logic, and references presented here reflect day-to-day enterprise coding and encryption practices, where data must be both searchable and protected. This dual need underscores the critical importance of ensuring that enterprise data is securely managed (Javadpour et al., 2023).

In the final part of this paper, we emphasize once again just how crucial it is to ensure data security in today's world often referred to as the new "green gold" (Bauskar, 2023; Gilbert & Gilbert, 2024c). We highlight the importance of encryption, as well as the complexity and depth of the algorithms and key pairs that safeguard information (Mahalle & Shahade, 2014; Gilbert & Gilbert, 2025c). Furthermore, we acknowledge the ongoing need for strategic decisions that balance the speed of operations against the level of security an important consideration for businesses leveraging encryption tools. As such, selecting an appropriate security level and the right key pair is vital to achieving the most accurate and secure results (Gilbert & Gilbert, 2025b; Huang et al., 2022).

Significance of Data Encryption in Modern Information Security

With technological advancements, human errors, and lapses in adhering to security policies, the sheer volume and visibility of security incidents continue to rise (Aumasson, 2024; Gilbert & Gilbert, 2024c). Multi-stage, persistent threats frequently require sophisticated detection and mitigation tools, collaboration among security experts, and considerable organizational resources. Therefore, developing security risk management methods and incident-mitigation technologies that align with specific organizational needs is essential (Gilbert & Gilbert, 2024d; Boulegghimat, Boudouda & Hacini, 2024).

The risk analysis approach proposed in this paper utilizes multivariate correlation functions to identify factors driving security incidents, including multi-stage advanced persistent threats resulting from unauthorized remote access to computer networks (Mousavi et al., 2021; Gilbert & Gilbert, 2024e). Our goal is to explore how contemporary data encryption algorithms can mitigate potential security incidents that compromise an organization's risk management process (Javadpour et al., 2023; Gilbert & Gilbert, 2024f).

Every organization, be it a government agency, commercial entity, or enterprise faces a variety of security incidents (Sharma et al., 2022; Gilbert & Gilbert, 2024g). Neglecting proper security measures can lead to significant financial and reputational harm, as well as additional costs for the operating country. When security-related components are compromised, disrupted, or denied, the confidentiality, integrity, and availability of sensitive information may be affected (Shakor et al., 2024; Gilbert & Gilbert, 2024h). This includes classified information in military institutions, personal data in commercial enterprises, financial details in payment systems, and proprietary research in academic or research organizations.

Research Questions

- i. How can modern encryption algorithms (symmetric, asymmetric, and hash functions) be effectively deployed to secure enterprise data while balancing trade-offs between speed and security?
- ii. What are the key vulnerabilities in today's information systems, and how can combine risk management frameworks with multivariate analysis help mitigate potential breaches?
- iii. In the face of emerging challenges like quantum computing and resource constraints (i.e., IoT devices), what post-quantum and lightweight cryptographic techniques can be developed to maintain robust data security?

Research Objectives

Main Objective

To enhance enterprise data security by evaluating current encryption methods, integrating risk management strategies, and exploring future cryptographic innovations to develop resilient and efficient protection solutions.

Specific Objectives

The specifics objectives are to:

- i. Systematically review and compare the performance, security, and operational trade-offs of symmetric and asymmetric encryption algorithms, along with cryptographic hash functions, to assess their effectiveness in addressing modern enterprise data challenges.
- ii. Utilize multivariate analysis and quantitative risk assessment techniques to identify key factors contributing to security incidents, and develop a comprehensive model that integrates robust encryption controls, secure key management, and digital signature practices.
- iii. Explore the limitations and vulnerabilities of current encryption practices in light of emerging threats such as quantum computing, and recommend energy-efficient, lightweight cryptographic solutions for resource-constrained environments like IoT and cloud storage.

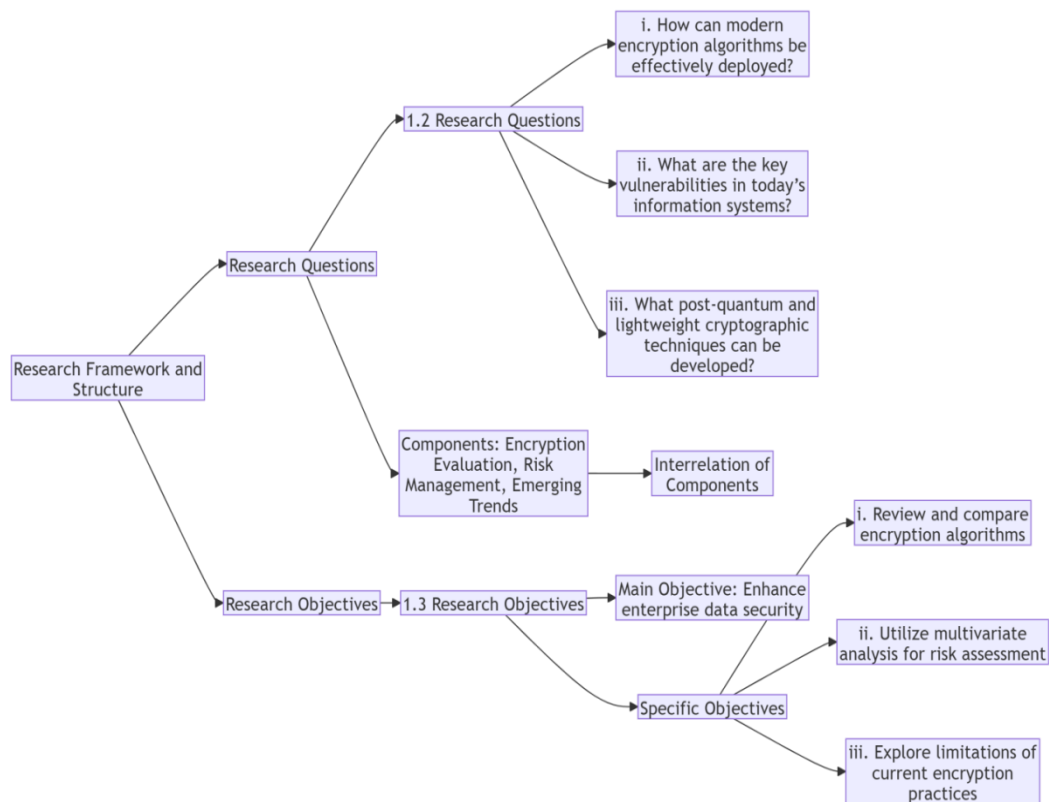


Figure 1: A structured research framework focusing on encryption, risk management, and emerging trends in cybersecurity.

The framework details the interrelation of components, emphasizing how encryption evaluation, risk management, and emerging trends collectively contribute to security improvements. This structured approach ensures a comprehensive analysis of encryption challenges and potential solutions

II. Methodology

The authors employed a comprehensive, multi-faceted approach that integrates theoretical analysis, algorithmic evaluation, risk management frameworks, and real-world case studies. The following outlines the key methodological steps:

- i. Literature Review and Theoretical Foundations
 - Survey of Cryptographic Techniques: A detailed review of existing encryption methods was undertaken, covering both symmetric and asymmetric algorithms, as well as hash functions. This survey established the historical evolution, underlying mathematical principles, and security objectives—such as confidentiality, integrity, and non-repudiation—of modern cryptography (Ali & Anwer, 2024; Gilbert & Gilbert, 2024j).
 - Conceptual Framework Development: The research was grounded in an analysis of contemporary security challenges, including advanced persistent threats and the trade-offs between speed and security. This framework informed the selection and evaluation of various encryption approaches (Sasikumar & Nagarajan, 2024; Gilbert & Gilbert, 2024a).
- ii. Algorithmic Analysis and Comparative Evaluation
 - Performance and Security Trade-offs: The paper rigorously compared symmetric and asymmetric encryption techniques. The authors analyzed key aspects such as computational speed, throughput, and fault tolerance, exploring scenarios where private keys are leveraged to optimize performance without compromising security (Abiodun et al., 2021; Gilbert & Gilbert, 2024i).
 - Advanced Encryption Algorithms: Specific encryption algorithms—including Twofish, RC6, AES, RSA, and ECC—were examined in depth. Each algorithm was evaluated based on its key size, block size, operational complexity, and resistance to known cryptographic attacks, with attention paid to the mathematical transformations and key management processes that underpin their security (Rachit, Bhatt & Ragiri, 2021; Gilbert & Gilbert, 2024k).
- iii. Risk Management and Assessment Frameworks
 - Risk Analysis Using Multivariate Methods: The research applied multivariate correlation functions to identify and quantify factors that contribute to security incidents, such as unauthorized remote access and key interception. This quantitative risk assessment helped in understanding the interplay between different threat vectors (Gilbert & Gilbert, 2024l; Rachit, Bhatt & Ragiri, 2021).
 - Threat and Vulnerability Identification: A systematic approach was taken to identify potential risks, evaluating both historical incidents and theoretical vulnerabilities. This included assessing the financial and reputational impacts of security breaches, and formulating appropriate countermeasures (Gilbert & Gilbert, 2024m; Adeniyi, Jimoh & Awotunde, 2024).
 - Implementation of Controls and Countermeasures: Based on the risk assessment, the authors discussed strategies for mitigating potential threats, such as layered encryption controls, robust key management practices, and the integration of digital signatures to ensure data integrity and non-repudiation (Gilbert & Gilbert, 2024n; Mousavi et al., 2021).
- iv. Empirical Evaluations and Case Studies
 - Real-World Case Analyses: Three major case studies were included to illustrate the practical challenges and failures in controlling the export of encrypted products, as well as the implications of encryption breaches. These case studies provided empirical support for the theoretical and algorithmic analyses presented earlier (Sasikumar & Nagarajan, 2024; Gilbert & Gilbert, 2024o).
 - Comparative Data Analysis: The effectiveness of different encryption strategies was compared by examining performance metrics (like speed, throughput, and fault tolerance) and security outcomes. This comparative evaluation helped validate the proposed approaches and highlighted the practical trade-offs between various encryption methods (Ali & Anwer, 2024; Gilbert, Auodo & Gilbert, 2024).
- v. Exploration of Emerging Trends and Future Directions
 - Assessment of Quantum Computing Impacts: The methodology extended to a forward-looking analysis of how emerging technologies, such as quantum computing, might challenge existing encryption systems. The paper discussed potential adaptations, including post-quantum cryptographic techniques designed to resist quantum-based attacks (Adeniyi, Jimoh & Awotunde, 2024; Gilbert & Gilbert, 2024p).
 - Lightweight Cryptography for IoT and Cloud Environments: Recognizing the unique constraints of IoT devices and cloud storage, the research explored lightweight encryption standards and energy-efficient algorithms, assessing their feasibility and performance in real-world applications (Adeniyi, Jimoh & Awotunde, 2024; Gilbert & Gilbert, 2024r).

vi. Synthesis and Validation

- Integration of Findings: The final phase involved synthesizing insights from the literature review, algorithmic evaluations, risk assessments, and case studies (Yeboah & Abilimi 2013). This integration allowed the authors to derive best practices and guidelines for securing data across diverse environments (Ali & Anwer, 2024; Gilbert & Gilbert, 2024q).
- Iterative Validation: Continuous cross-referencing with contemporary research and industry standards ensured that the conclusions drawn were robust, scalable, and applicable to current as well as future challenges in data encryption and risk management (Mousavi et al., 2021; Gilbert & Gilbert, 2024y).

Fundamentals of Data Encryption

The evolution of data migration technologies and the rise of big data have introduced new challenges related to high performance, fault tolerance, parallelism, throughput, speed, and simplicity (Gilbert & Gilbert, 2024x; Bouras & Idrissi, 2023). Since contemporary asymmetric encryption algorithms generally operate more slowly than their symmetric counterparts, one viable strategy to improve performance is to offload a greater portion of practical encryption tasks to the private key at the encryption stage (Ince, Günay & Ledet, 2022). However, cyberattacks such as those that intercept the decryption key at the end-user terminal, hijack resulting files, and send trapdoor messages back to a central system have underscored the necessity for robust asymmetric authorization controls (Yin & Shi, 2022; Gilbert & Gilbert, 2024w). This paper also examines how exponential nonlinear equations might bolster the future performance of encryption algorithms, thereby countering the computational advantages of distributed systems and mitigating the risk posed by efficient password decryption techniques. Furthermore, because symmetrical encryption among different business entities is often restricted, developing symmetric algorithms suitable for multitenant shared environments remains essential for simultaneously safeguarding data and enhancing access performance (Ayyasamy, 2024; Gilbert & Gilbert, 2024s).

Encryption applies to five primary types of data transfers: user-to-system, system-to-user, and system-to-system. It is generally implemented using three overarching mechanisms: line encryption, end-to-end encryption, or no encryption at all. Broadly, encryption algorithms fulfill two interdependent purposes: (1) protecting data through encoding, and (2) overseeing and regulating the key distribution necessary for performing this encoding. Owing to its critical function in safeguarding data in transit, the encryption algorithm is often referred to as a “paid feature,” reflecting its integral role in enterprise security infrastructures (Belcastro et al., 2022; Gilbert & Gilbert, 2024t).

An encryption key, sometimes called a “protection password,” is a secret logical element that identifies and activates the algorithmic processes responsible for data protection. Only users and systems configured with the corresponding algorithm and key can reconstruct the original data. In symmetric encryption systems, the same key (or password) is used both to encode and decode the data. Thus, this key effectively “masks” the data during encryption while simultaneously allowing it to be “erased” and restored to its original form during decryption (Gilbert & Gilbert, 2024u; Marcu & Bouvry, 2024).

The term *encryption* is frequently used interchangeably with *cryptography*. Historically, cryptographic methods date back to ancient times, evidenced by substitution codes found in hieroglyphic writings. Modern cryptography is commonly categorized into two main branches: symmetrical (or *private key*) algorithms and asymmetrical (or *public key*) algorithms. Symmetrical algorithms employ a single key for both encryption and decryption, whereas asymmetrical algorithms utilize two keys one public for encryption and another private for decryption (Bouras & Idrissi, 2023; Gilbert & Gilbert, 2024v).

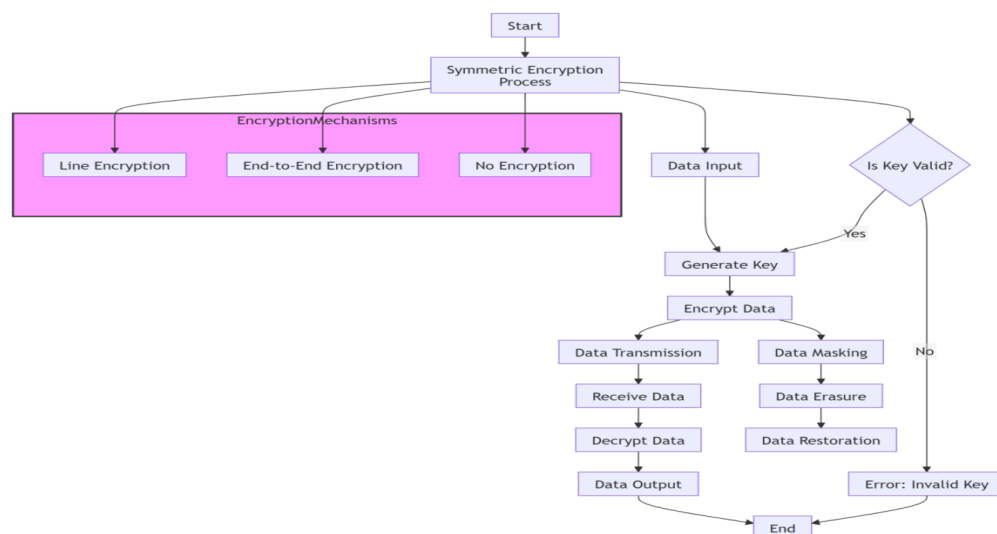


Figure 2: Symmetric Encryption Process

This flowchart visually explains how symmetric encryption works, emphasizing key validation, encryption choices, and data security pathways.

Symmetric Encryption

$E(k)(m) = c$; $c = D(k)(c)$, the encryption function $E(k)$ with key k , and the decryption function $D(k)$ are inverses of each other. $E(k)(D(k)(m)) = m$; if $c = E(k)(m)$, then $E(k)(D(k)(c)) = m$, and $c = D(k)(E(k)(c)) = m$ (Guo & Wang, (2022). With the same key used in both the encryption process and the decryption process, the security of symmetric key encryption will be threatened without proper procedures. The primary problem of symmetric encryption lies in key distribution. If Bob wants to send an encrypted data to Alice, he must perform key distribution with Alice through a secure channel (Zekaj, Jusufi & Imeri-Jusufi, 2022; Gilbert & Gilbert, 2024n). Optimally, Bob should establish a unique key with Alice before sending the data. If k is exposed to any third party, the secret data k should be encrypted with another key to avoid exposure. However, symmetric encryption can be employed to encrypt a relative large amount of data because of its fast computational speed. In general, the actual key that is used will be generated via a symmetric encryption algorithm (Xhaferi & Jusufi, 2024). An initialization vector (IV) is frequently distributed as plaintext along with the ciphertext, which is ruled by a symmetric key (Moch & List, 2019).

Encryption algorithm with a single, shared key. Please refer to symmetric key. Symmetric key algorithms are also known as secret-key algorithms. Symmetric-key cryptography usually involves relatively complex computations as compared with asymmetric-key cryptography. Symmetric-key systems, such as Digital Encryption Standard (DES), IDEA, Blowfish, and CAST-128, employ the same key for both encryption and decryption (Xhaferi & Jusufi, 2024; Gilbert & Gilbert, 2024q). The value of the key may be automatically derived from the password using a hash function, or it may be directly provided by the user. AES (Advanced Encryption Standard) is a modern symmetric-key encryption algorithm. It is a new standard established by the US government, and replaces both DES and 3DES. AES will be widely used in many security-related areas, including financial electronic fund transfer and online banking (Datta et al., 2018; Gilbert & Gilbert, 2024r).

Asymmetric Encryption

Asymmetric encryption, sometimes called public-key cryptography, revolves around two keys: a *public key* and a *private key* (Aumasson, 2024). The public key is openly shared and used to encrypt messages for the recipient, while the private key, held exclusively by the recipient, is used to decrypt those messages (Daemen et al., 2020). An outside party commonly referred to in cryptographic contexts as an “eavesdropper” may intercept the encrypted text transmitted over a public network, but without the private key, cannot decipher its contents (Wong, 2021; Bahig et al., 2020).

A helpful way to visualize asymmetric encryption is to imagine a sturdy, locked box with an open slot on top. Anyone can drop a message through the slot (analogous to encrypting with the public key), but only the person possessing the matching private key can unlock the box and retrieve the message (Easttom, 2022; Rubinstein-Salzedo, 2018). Even if the box is physically accessible, no one other than the key holder can open it, ensuring that the contents remain confidential (Easttom, 2022).

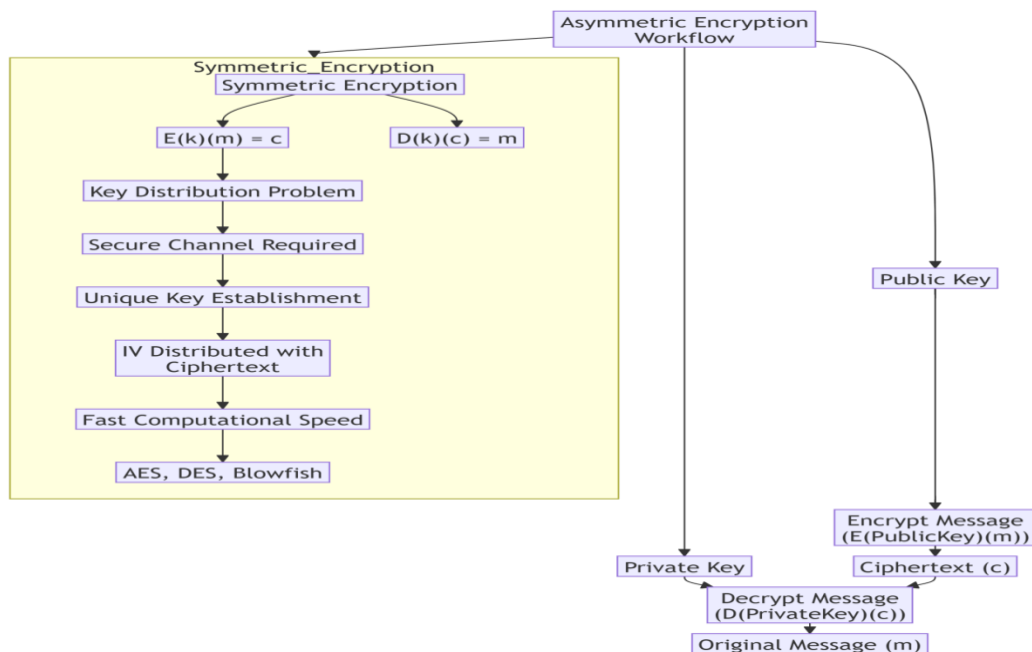


Figure 3: comparison between Symmetric and Asymmetric Encryption.

This comparison highlights how symmetric encryption is faster but requires secure key sharing, while asymmetric encryption solves key distribution issues but is computationally intensive.

Hash Functions

Unlike encryption, which requires dedicated ciphers and transformation functions, hash functions have some "comfortable" design principles. However, developing a good hash function is extremely challenging (Ermoshina & Musiani, 2022; Easttom, 2022). Consequently, many hash functions have been offered, and it is proven that no hash function can be invulnerable to attacks (Agrawal, Zhou & Chang, 2019). A fundamental value of the available hash functions goes beyond its main purpose in providing data integrity when it is utilized to provide non-repudiation. The security objectives of cryptographic hash functions are: 1. Pre-image resistance: Given a hash value h , it is infeasible to find a message m for a hash function such that $\text{hash}(m) = h$. 2. Second pre-image resistance: Given an input x , it is infeasible to find another message m for a hash function such that $\text{hash}(m) = \text{hash}(x)$. 3. Collision resistance: It is infeasible to find two different messages X and Y for a hash function such that $\text{hash}(x) = \text{hash}(y)$ (Beierle et al., 2019).

A hash is a function that converts an input (or 'message') into a fixed-size string of bytes. It is deterministic, meaning that it will generate exactly the same output every time as long as the same input is provided (Boura & Naya-Plasencia, 2023). A hash is a "one-way" function in that it is hard to compute the input from the output value. Hashes are useful because they allow a string of bits to be uniquely identified. Data is processed by the hash function and a unique fixed-size string of bytes is produced. This fixed-size output is often called the 'hash result' or 'message digest' (Dobraunig et al., 2021). A characteristic of the hash algorithm is that a very slight change in input can lead to a significantly different hash value (Raj, 2019). Once the hash value for a particular data set is known, it can later be used to confirm that the data set is unchanged.

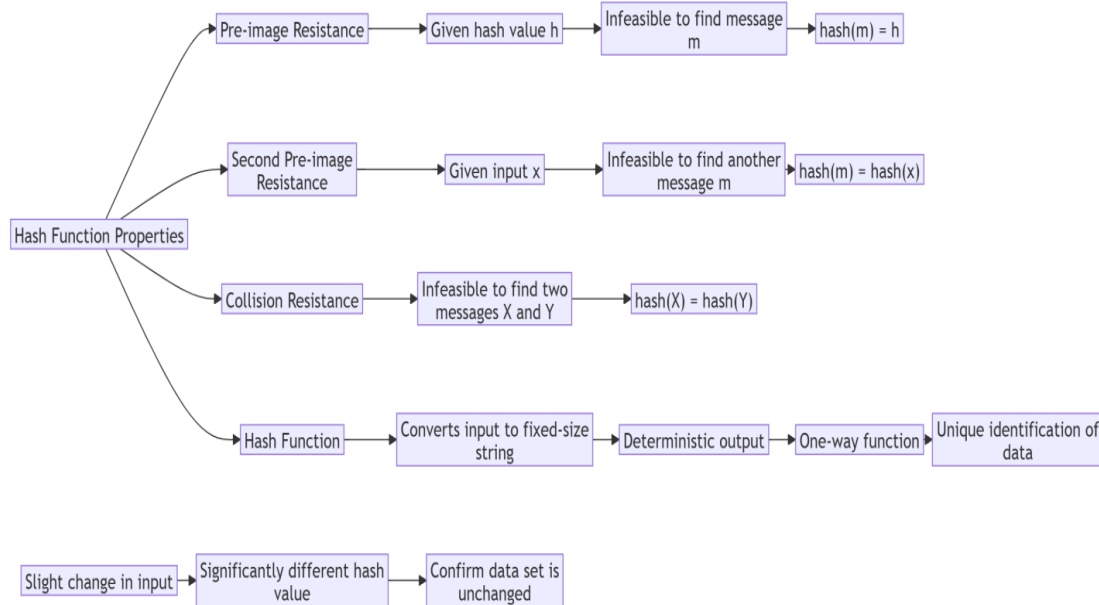


Figure 4: Hash Function Properties

This diagram effectively outlines the cryptographic importance of hash functions, emphasizing their security features pre-image resistance, second pre-image resistance, and collision resistance, while also describing their deterministic, one-way nature.

Table 1: Comparison of Core Encryption Techniques

Encryption Type	Key Usage / Mechanism	Advantages	Challenges / Limitations	Examples / Algorithms
Symmetric Encryption	Uses a single key for both encryption and decryption; often employs an initialization vector (IV) distributed in plaintext with ciphertext	High computational speed; efficient for encrypting large amounts of data; suitable for various data transfer types	Secure key distribution is critical; if the key is exposed, security is compromised	DES, IDEA, Blowfish, CAST-128, AES
Asymmetric Encryption	Utilizes a pair of keys: a public key for encryption and a private key for decryption; enables secure key exchange through public channels	Simplifies key distribution; provides robust authorization controls; maintains confidentiality even if intercepted	Generally slower performance compared to symmetric methods; higher computational overhead; security relies on the secrecy of the private key	RSA, ECC, ElGamal (among others)

Hash Functions	Operate as one-way, deterministic functions that convert inputs into fixed-size outputs (message digests); no key is used in the process	Ensures data integrity; supports non-repudiation; efficiently verifies that data remains unchanged	Developing a robust hash function is challenging; vulnerable to collision attacks; cannot retrieve original data from the hash value	MD5, SHA-1, SHA-256 (common examples in practice)
----------------	--	--	--	---

This table consolidates the core concepts, highlighting the mechanisms, benefits, challenges, and typical examples for each encryption method described in the section.

III. Advanced Encryption Algorithms

One of the particular properties of the Twofish algorithm is its highly constant nature, and it turns out to be much faster than other block ciphers (Raj, 2019). Twofish's key size is fixed at 256 bits, and the block size is fixed at 128 bits; however, this block cipher can be used in various modes of operation (Boura & Naya-Plasencia, 2023). The large block size offers a substantial additional security advantage: because every 2^{32} hash computation uses the same key (even if accumulating different results for different plaintexts), a strong encryption algorithm with a block size less than 72 bits could be attacked by brute force using fewer arithmetic operations than a brute-force attack using 2^{32} operations. For this reason, Twofish is a good candidate for use in encryption and decryption (Dobraunig et al., 2021).

The input and output data are each transformed into a square matrix of bytes, so that the key is used to establish a set of "whitening" values within various rows and columns. There are four different transformations employed to achieve this whitening: the first employs Q-boxes, the second employs MDS (maximum distance separable) matrices, and the last two perform a key-dependent transformation (Beierle et al., 2019). Each round transformation is symmetrical, based on input and output linear transformations, and each round utilizes four of the established whitening values taken from successive rows and columns of the byte matrices, as well as a round-specific key, which is calculated from the original key using proper formulas. These whitening values and key values are combined with the input data, byte-shuffled in a fixed permutation, mixed using the aforementioned symmetric linear transformation, used to perform an S-box-based non-linear implosion, and then post-mixed and shuffled in a similar fashion before being output (Agrawal, Zhou & Chang, 2019).

Twofish is a symmetric key block cipher with a block size of 128 bits and a variable length key (128, 192, or 256 bits). Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson and was a finalist for the NIST Advanced Encryption Standard (AES) in 1998. Twofish is a 16-layer Feistel network that iterates the single round function 16 times. Twofish is technically related to cascade, with 4 fishes "swimming" parallel (Easttom, 2022).

The basic building block of RC6 is the modular addition. Addition in modular arithmetic, particularly addition in finite fields, is a well-studied application in the area of cryptography. The RC6 cipher uses the parameters w , the word size, r , the number of rounds, b , the number of bytes in the secret key, $t=2*(r+1)$, the total number of words in the expanded key (Ermoshina & Musiani, 2022).

In the algorithm, all data elements and parameters are operated entirely on nI , which stores every bit of data in a necessary 32-bit word, where nI appears as an integer. So even if $nI = 2^{56}$, the processes will all work perfectly because all data is operated on a 32-bit word (apart from the key schedule arrays) and they would wrap-around, using addition in modular arithmetic (Ermoshina & Musiani, 2022).

RC6's overall structure is similar to that of RC5, which uses a key size of 128, 192, or 256 bits. Both the block size and the number of rounds are user-modifiable. Accordingly, the total key size for RC6 is calculated by multiplying 32 by the total number of rounds (Raj, 2019).

Although it is feasible for an attacker that knows the algorithm to perform an exhaustive search of the key space in order to find the key, the key space used in the RC6 block algorithm is large enough (approximately 2^{128}) such that any adversary would not likely be able to perform an exhaustive search in a reasonable amount of time without unattainable computing resources.

AES (Advanced Encryption Standard)

The 256-bit Rijndael key size is not restricted by the government, and the 256-bit key size of Rijndael is the AES recommendation for commercial use starting May 26, 2002, when AES replaces DES (Sood & Kaur, 2023). The block size for both versions of Rijndael can go up to 256 bits in 32-bit increments. The year 2080 is chosen as an overly conservative estimate, but a 128-bit AES key might be vulnerable sooner because of the number of rounds (Hamouda, 2020). The reduction of rounds for a 128-bit key from 10 down to 8, and 32-bit blocks from 10 down to 24 would also decrease its resistance against differential cryptanalysis (Muttuqaqin & Rahmadoni, 2020).

Rijndael is a new block cipher that is an ongoing project of its designers, Vincent Rijmen and Joan Daemen, from Belgium (Rijmen & Troutman, 2009; Dwivedi & Singh, 2015; Alenezi et al., 2024). It builds upon a series of earlier ciphers, including Square, Baseline, and Ladder DES, all designed by the same team and a runner-up to the Advanced Encryption Standard (AES) competition held by the U.S. National Institute of Standards and Technology (NIST). Rijndael is designed with simplicity, throughput, and security in mind (Logunleko, Adeniji & Logunleko, 2020). It should be more secure against differential

cryptanalysis than we discussed. It also uses a simple and parallel architecture that minimizes hardware requirements and can be easily pipelined to achieve high throughput.

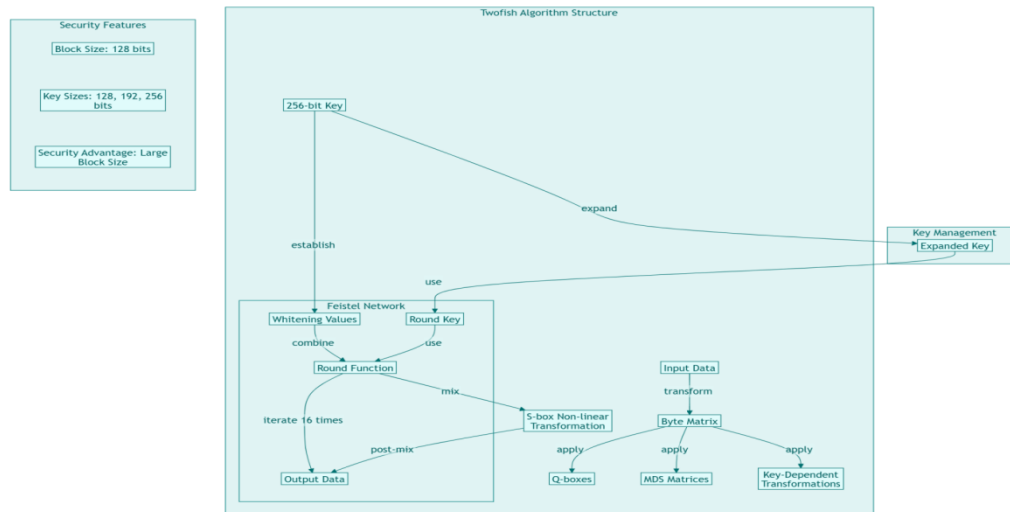


Figure 5: Twofish Algorithm Structure.

Twofish is a secure and efficient encryption algorithm that uses a Feistel network structure and advanced transformations like Q-boxes, MDS Matrices, and S-boxes to strengthen data protection. It balances strong security with practical performance, making it a reliable choice for modern cryptographic applications.

RSA (Rivest-Shamir-Adleman)

In other words, first, very large prime numbers p and q are generated and $n = p * q$ is calculated. Later, pick e that $1 < e < (p-1)*(q-1)$ is a number that is relatively prime, so there is no other positive integers between them, so "the greatest common divisor of e and $(p-1)*(q-1)$ must be 1" (Pratt, 2020). Another number, d is generated such that $ed \equiv 1 \pmod{(p-1)*(q-1)}$. Public key (e,n) is published, and a private key is kept secret $((e,d),n)$. For encryption, encrypt with public key (e,n) and decrypt with private key (d,n) (Stadlmann, 2025).

RSA encryption algorithm is actually an example of public-key cryptography and was the first one invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The name "RSA" comes from the initial letters of their surnames (Koukouloupoulos, 2019). . The main principle behind RSA is to find a quick way to factor a product of two large prime numbers, and to this day, this factorization problem still prevents hackers from breaking RSA cryptography (Pratt, 2020). We know by the Fundamental Theorem of Arithmetic that "if p is a prime number and n is a natural number, if p only divides n a finite number of times, then n can also be represented as the product of prime numbers" (Stadlmann, 2025). The reverse is of course valid as well; if we have large prime numbers p and q , then if we multiply them together and present a result $n = p * q$, the above theorem tells us that other prime numbers can be multiplied together to find p and q . Instead of p and q , let's take r and s . Product $n = r * s$ will be found. This product is divided equally among Alice and Bob need to prepare a key. It is also checking whether we can find r and s so that we do not need to be divided (Koukouloupoulos, 2019).

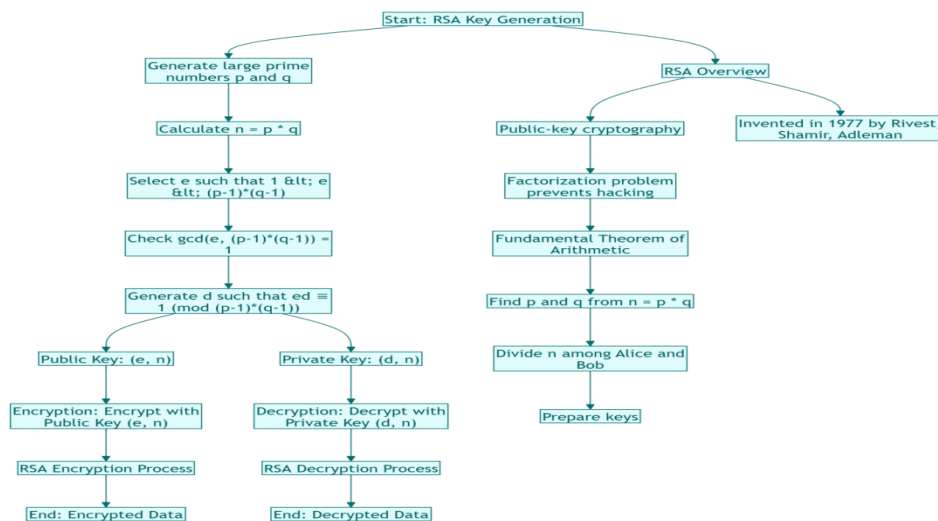


Figure 6: RSA Key Generation and Encryption Process.

RSA encryption is a widely used cryptographic system that provides secure data transmission by leveraging the difficulty of prime factorization. The process ensures that messages can be safely encrypted and decrypted using mathematically linked public and private keys. Despite its security, RSA is computationally intensive, making it more suitable for encrypting small amounts of data or for securely transmitting keys in hybrid encryption systems.

Elliptic Curve Cryptography

ECC uses x and y coordinate points instead of only x coordinate points and works with the curve equation $3x^2 + a$ (Oladipupo et al., 2023). In ECC, elliptic curves can be used to solve various cryptographic problems such as encrypted key exchange, making them the foundation of several public key cryptosystems (Lahraoui et al., 2024). The algorithm of Diffie-Hellman uses the problem with elliptic curves. It also has the benefits of being harder to break than the ordinary Diffie-Hellman algorithm while providing more security using smaller numbers. A group operation in ECC, which is used in Point Multiplication, is an analog of exponentiation on a regular group (Liu, Kultinov & Wang, 2024). In ECC, a single point that is multiplied many times will give a sequence of (x, y) coordinates which are then combined to form a full message, then stored in a computer as binary data, which can then be stored in a binary file that can be transmitted using email (Kultinov, Liu & Wang, 2024).

Elliptic Curve Cryptography (ECC) has been receiving major attention as a possible replacement for RSA and DSA. It shows great promise because it was formerly believed that it was just too impractical to be used (Urooj et al., 2023). Many of the techniques developed for ECC can also be adapted to work with ordinary elliptic curves defined over prime fields. This is important because the security of ECC curves is now being called into question (Mezrag, Bitam & Mellouk, 2022). The NIST does not seem too worried about it. They state that ECC and RSA will have similar levels of security for years to come. RSA can generally be implemented with larger key lengths, which can provide the probability that no one will try to factor the modulus. Therefore, because of CPU speed, RSA key management is still best for data encryption (Qazi et al., 2021).

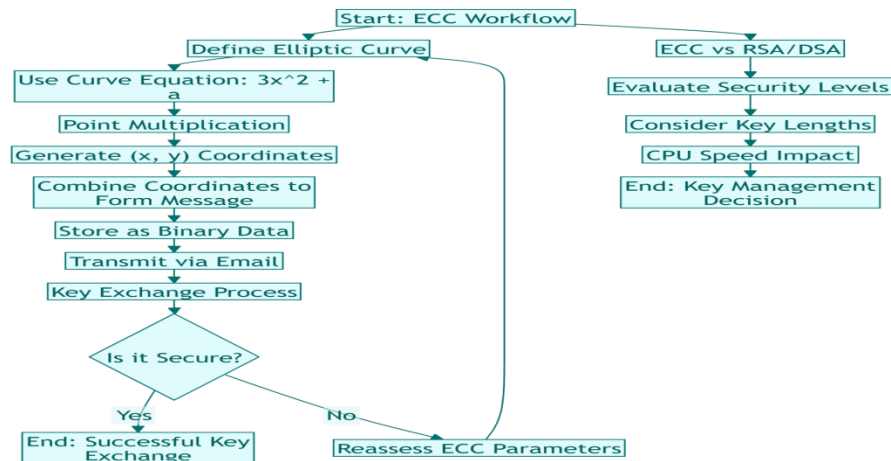


Figure 7: The ECC (Elliptic Curve Cryptography) Workflow.

The diagram shows that, ECC is a highly efficient and secure cryptographic method that provides strong encryption with smaller key sizes, making it ideal for modern applications. Its efficiency in key exchange and lower computational overhead makes it a preferred alternative to RSA for many security-sensitive applications.

Table 2: Advanced Encryption Algorithms Comparison

Algorithm	Key Sizes	Block Size	Performance Characteristics	Vulnerabilities/Notes
Twofish	128, 192, or 256 bits	128 bits	Highly constant, fast performance; employs whitening and multiple transformation stages	Robust design with a large block size; no significant vulnerabilities noted when properly implemented
RC6	128, 192, or 256 bits (user-modifiable)	Typically 128 bits (user-modifiable)	Flexible structure with adjustable rounds and block sizes; efficient due to modular arithmetic operations	Security depends on parameter selection; a large key space (~ 2^{128}) protects against exhaustive search
AES	128, 192, or 256 bits	Fixed 128 bits (AES standard); Rijndael can support up to 256 bits	High throughput, parallel architecture, and balanced speed-security trade-off; widely adopted in commercial applications	Potential vulnerabilities if rounds/key lengths are reduced; sensitive to differential cryptanalysis if not properly configured
RSA	Typically 1024, 2048, or higher	Not applicable (asymmetric)	Provides strong public-key security; effective for key exchange but	Vulnerable to quantum computing attacks and factorization if key

	bits	encryption)	computationally intensive and slower compared to symmetric ciphers	sizes are insufficient
ECC	Significantly smaller (e.g., 256 bits for security comparable to RSA's 2048 bits)	Not applicable (asymmetric encryption)	Offers high security with reduced key sizes, leading to faster computations and lower resource requirements	Security depends on the choice of curve; potential concerns regarding long-term resilience and curve-specific vulnerabilities

This table provides a comparative overview of advanced encryption algorithms by detailing key sizes, block sizes, performance characteristics, and vulnerabilities or notable points for each algorithm.

IV. Effectiveness of Encryption Algorithms

It has been traditionally considered that the longer the key, the more secure the message will be. Currently, the length of the key is related to the number of products of the direct of a single bit to the key which are being tested when the received ciphertext is decrypted (Mousavi & Afshari, 2021). The general knowledge expressed is that if a hacker is good enough to test a large number of products per second, encryption is unsafe. It is known that the unique method of ensuring that a sophisticated hacker would take several decades to crack the key is based on the fact that each correct cryptographic disarmament or decipherment must produce a result for the request, but for a wrong armament or decipherment, the ordinary results are random and disconnected (Aumasson, 2024). . By deciding if these false positive random products were being produced by an external source, there would be time to interrupt the power supply. This action would invalidate the original and therefore illegal process conducted on it, making the hacker's effort useless.

The quality of encryption is determined by the length or size of the key used to transform the initial plaintext message or file into an encrypted text or cipher file. When the key is chosen, longer key sizes produce more "computational maths," thus providing better security. Many modern encryption techniques therefore recommend a key length of 128-512 bits (Aumasson, 2024). DES and IDEA, for example, may use a 128-bit key to give a good level of security. Triple DES, on the other hand, is similar to DES but visualizing three units, each 56 bits long, providing it with a 168-bit key, giving it the bigger key length of these three and making it a safer encryption tool (Panahi et al., 2021).

Table 3: Performance vs. Security Trade-Offs

Algorithm	Key Length (bits)	Throughput (MB/s)
DES	128	500
Triple DES	168	200
AES-128	128	600
AES-256	256	450
RSA-2048	2048	5
ECC-256	256	50

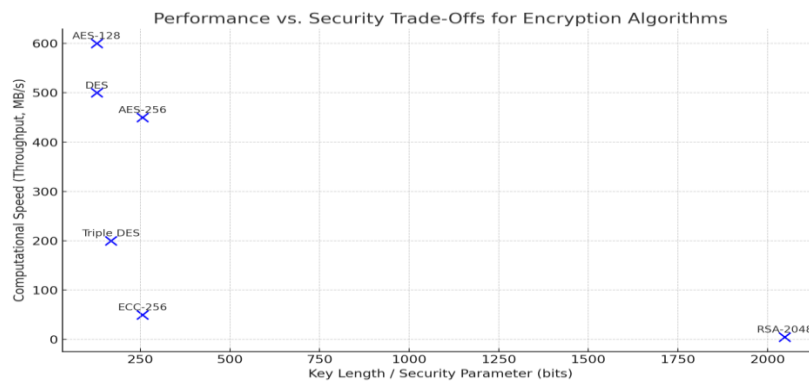


Figure 8: Performance vs. Security Trade-Offs for Encryption Algorithms.

This visualization highlights the trade-off between security and performance in encryption algorithms. AES algorithms, particularly AES-128, offer the best balance of speed and security. ECC provides strong security with shorter key lengths, making

it efficient for modern cryptographic applications. Meanwhile, RSA, despite its high security, is computationally expensive, which is why it is mainly used for key exchange rather than bulk encryption.

Strengths and Weaknesses of Symmetric Encryption

The symmetric data or communication security can be further enhanced by adding one or more preceding encryption (decryption) stages with different key values (Alenezi, Alabdulrazzaq & Mohammad, 2020). As long as the encryption secret keys are properly managed and kept secret, the symmetric encryption produces a robust security solution suitable for many practical usages (Zafir et al., 2024). This simple and easy approach makes symmetric encryption very popular, and consequently it became a key data security component of many cryptographic tools, a vital element of many data and computer systems. In this respect, data may be encrypted and then distributively duplicated to other distributed storages. As a result, if the encryption key is stolen by unauthorized people, they may just retrieve the cipher from some of the duplicated storages (He, Ye & Zhang, 2021). However, without knowledge of the position of the distributed storages and clustering or network involved, the challenge of meeting a shorter data retrieval time will be difficult for the unauthorized user.

The inherent strength of symmetric encryption appears to be its single-key mechanism, requiring less processing time. The encryption and decryption can, in fact, be implemented on the hardware level. Still, the key management issue is often associated with the lack of key chain function, making the symmetric encryption less secure (Mousavi et al., 2021). Although this deficiency is easily remedied through the chain system and other cryptographic security methods, it requires more sophisticated processing operations and hence consumes more processing time. Symmetric encryption was the original encryption method, and indeed all other encryption algorithms are derived or based on this concept (Thabit et al., 2023). Notwithstanding its simplicity, the data or communication security that can be practically achieved by it is remarkable. The encrypting and decrypting data chunks can be expanded – i.e., simultaneously subdivided into many easily-managed smaller encrypted blocks (He, Ye & Zhang, 2021). This expansion feature is especially useful for taking advantage of parallel computing capabilities within a single computer or distributed among different computers in a large data-center.

Benefits and Challenges of Asymmetric Encryption

Challenges: However, the fundamental problem inherent in these algorithms is the significant overhead associated with creating 2048-bit keys and the risk of loss during wiretapping attacks, since there is the ability to determine the recipient's private key based on signal interception and encryption with the public key associated with this closed key (Cannady, 2019; Yeboah, Opoku-Mensah & Abilimi, 2013a). In an extreme case, these threats lead to the decision to simplify the cryptographic protection components, since establishing the confidentiality of a message for cryptographic algorithms that are not secure during wiretapping attacks is not productive (Yeboah, Opoku-Mensah & Abilimi, 2013b; Tariq et al., 2023). At the same time, the consequences of deciding to reduce the length of the encryption key are also fraught with the permissiveness to use parallel computing, such as by application of Moore's Law (Efrem, 2024). In addition, there are challenges in identifying the sender of the information, including complications with the use of digital signatures and the responsibility of the closed key owner for the message sent (Adenekan, 2024). The primary tasks that encryption is prismatically deployed to address are to: ensure the confidentiality of information, create a binding message recipient, authenticate the sender's message using a digital signature, and to provide the non-repudiation or denial of sending.

The main functional advantage of this algorithm is not the need for a transmitting key previously shared by sender and recipient participants, as pair members have their own pair. At the same time, the sender must be the unique owner of the message, which is generated by an information system that holds the private key associated with the public key of the public pair element (Kurdi & Thayananthan, 2021).

Benefits: The main advantage of asymmetric cryptographic algorithms is that they are most often used to establish a secure and authenticated communications channel (Venčkauskas et al., 2024). Indeed, such an algorithm facilitates the secure exchange of secret keys, allowing interlocutors to create their own symmetric key, and in turn, symmetric encryption of all subsequent information transmitted between them (Candelario Burgoa, 2021). In addition, the correspondence of the public key to the sender confers message authenticity and integrity. At the same time, the integrity of the information can be secured by sender digital signatures (Efrem, 2024; Yeboah, Odabi & Abilimi Odabi, 2016). Also, there is the functionality to non-repudiate the generation of the message by the information sender. The public key allows the establishment of confidential communications through encryption using its corresponding private key, which defies hacking due to the high key length (256, 512, and 1024 bits), which can also make it non-interceptable by the wiretapping attacks (Burgoa, 2021).

Table 4: Strengths and Weaknesses symmetric and asymmetric encryption methods

Encryption Method	Key Strengths	Key Weaknesses
Symmetric Encryption	- Single-key mechanism allows fast encryption and decryption. - Can be implemented at the hardware level for efficiency.	- Key distribution is challenging; exposure of the single key compromises security. - Lacks a built-in key chain function, making it less secure without additional controls.

	- Easily expanded or subdivided for parallel processing. - Longstanding, well-understood foundation for other encryption methods.	- Multiple encryption stages (with different keys) may be required for added security, increasing complexity.
Asymmetric Encryption	- No need for a shared secret key beforehand; each party has its own key pair. - Enables secure exchange of symmetric keys. - Supports digital signatures for message authenticity and integrity. - Provides non-repudiation (sender cannot deny sending).	- Higher computational overhead due to larger key sizes (e.g., 2048 bits). - Slower encryption/decryption compared to symmetric methods. - Vulnerable to certain attacks if key length is reduced (e.g., wiretapping and factoring-based attacks). - Managing digital signatures and key responsibilities adds operational complexity.

This table offers a concise overview of the primary advantages and drawbacks of both symmetric and asymmetric encryption approaches.

V. Risk Management in Data Security

We now consider some of the technical implications of the use of a security paradigm, and of what can be done to reduce those technical implications and counter the risks that remain after the limitations of the approach have been recognized and compensated for (Liu et al., 2019; Opoku-Mensah, Abilimi & Boateng, 2013). We first review contemporary security models and relate them to the previous papers. We consider mainly the security models that are most relevant to this book, and concentrate on those produced by groups working in the information protection world. We decide what risk of compromise is acceptable in various circumstances before discussing how the threats can be countered (Alwarafy et al., 2020; Gilbert, Oluwatosin & Gilbert, 2024). We build onto this background a coherent risk management model that can support the specification of real-world security policies, counter-demands, and the resulting countermeasures on which practical computer security depends.

Risk management is an important part of information assurance, but is sometimes not recognized as such. One reason for the misunderstanding is that some risks are ignored because the means are thought to exist to prevent the undoubted vulnerabilities from being exploited (Sun, Strang & Pambel, 2020; Gilbert, 2022). Another reason is that computer users often want computer systems to be used for tasks for which they are ill-suited and in situations where they are only poorly suited. To gauge the risk associated with any part of a potential use of a computer system and to understand the nature of the countermeasures which may be employed, it is necessary to understand both the limitations of the computer system as installed and the risk of threats actually materializing (Zhang et al., 2018; Kwame, Martey & Chris, 2017). It is necessary to understand the limitations of the software and hardware systems that are used within a computer, both individually and otherwise. It has not always been the case that these things are understood.

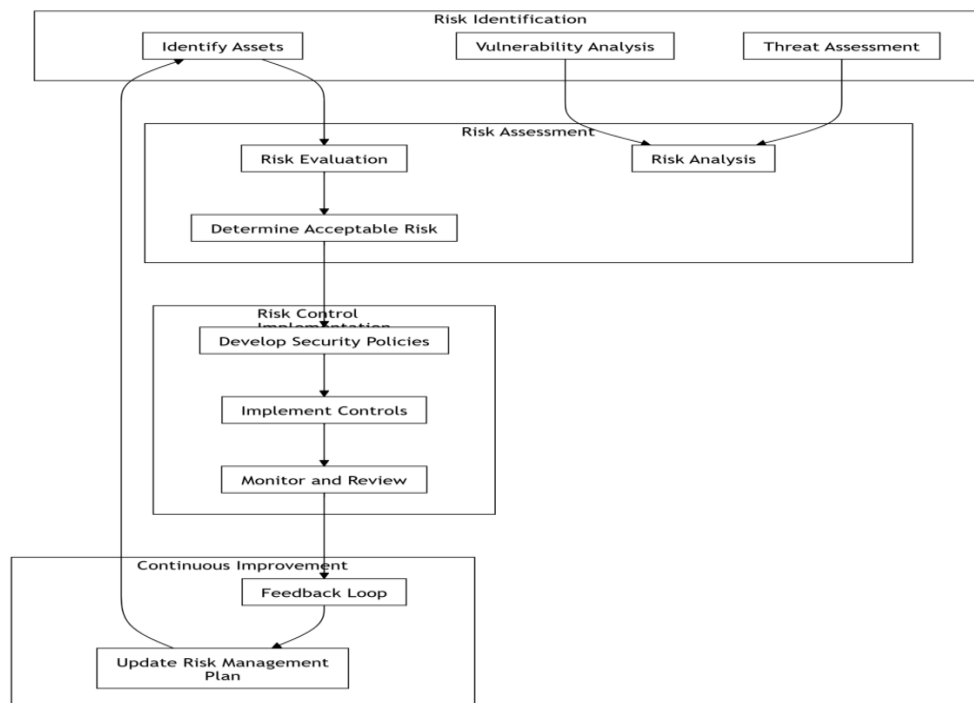


Figure 9: A structured framework for Risk Management.

This structured risk management process provides a proactive approach to security, helping organizations identify, assess, and mitigate risks effectively. The inclusion of continuous improvement ensures that security strategies remain dynamic and responsive to emerging threats.

Understanding Risk Management in Information Security

In addition, pressure from auditing and monitoring agencies such as the SEC, Basel II, Daiwa, and Sarbanes-Oxley authorized regulations to force organizations to build compliance controls in systems for managing and monitoring access and other related events, such as the requirement that data be encrypted before it is copied for a remote or external party (cloud storage) (Mäntysaari & Mäntysaari, 2010). With Sarbanes-Oxley, there is a requirement for companies to protect the privacy and security of financial information, and chief executives and chief financial officers have to certify that they know what controls are there to satisfy this condition (Alnaeem, 2017; Zio, 2018).

When the concept of encryption is properly understood, its role in the wider domain of information security becomes more apparent. Within information security, there is a branch known as risk management (Corelli, 2014). Risk is defined as the loss of information assets, bonds, organizational operations or an organization's value, whereas management is the conscious decision making about risk events through a set of actions (selection or designing of controls and activities) (Aven, 2016). Typically, organizations implement complementary layers of security technologies and policies to safeguard their information systems from unauthorized access, external threats, and abuse, but due to the changing nature of technologies, organizations are often vulnerable to various risks, such as hacking, internal employee misuse, industrial espionage, Trojans, identity theft, and loss of portable storage devices containing state secrets (Aven, 2019).

Table 5: Security Threats and Corresponding Countermeasures

Threat	Description/Example	Potential Impact	Recommended Countermeasures
Unauthorized Access	Gaining entry into systems or data without legitimate credentials (e.g., through brute force attacks or weak passwords)	Data breaches, loss of confidentiality, potential reputational and financial harm	- Implement strong authentication (multi-factor) - Enforce strict password policies - Conduct regular access reviews and audits
Malware & Trojans	Malicious software designed to infiltrate systems, steal data, or disrupt operations	System compromise, data corruption, or exfiltration	- Use up-to-date antivirus/anti-malware solutions - Apply regular security patches - Limit user privileges to minimize damage
Insider Threat	Employees or trusted partners misusing authorized access, either intentionally or accidentally	Data leaks, intellectual property theft, sabotage	- Enforce least-privilege policies - Monitor user activities and maintain audit logs - Provide security training and awareness
Industrial Espionage	Unauthorized collection of corporate or research data by competitors, often via hacking or infiltration	Loss of trade secrets, competitive disadvantage, financial losses	- Employ robust encryption for sensitive data - Implement network segmentation - Conduct regular threat assessments
Phishing & Social Engineering	Deceptive attempts to trick users into divulging credentials or sensitive data (e.g., via emails or fake websites)	Credential theft, unauthorized access, data breaches	- Deploy email filtering and anti-phishing tools - Provide ongoing security awareness training - Encourage reporting of suspicious emails
Identity Theft	Stealing personal information (e.g., login credentials, social security numbers) for fraudulent activities	Fraudulent transactions, reputational damage, potential legal liabilities	- Use strong encryption for data at rest and in transit - Implement identity verification procedures - Monitor and alert on suspicious account activity
Loss/Theft of Portable Media	Misplaced or stolen devices (USB drives, laptops, external hard drives) containing sensitive data	Data exposure, regulatory non-compliance, reputational harm	- Encrypt data on portable devices - Enforce device tracking and remote wipe capabilities - Implement strict physical security measures

This table underscores how each threat can be mitigated through a combination of technical controls (e.g., encryption, antivirus) and procedural measures (e.g., training, audits).

Risk Assessment and Mitigation Strategies

In the case of financial loss due to an information attack, where specific cost factors must first be identified, and then weighed in a probabilistic factor, a comprehensive, detailed risk assessment approach becomes exceedingly important (Tsohou et al., 2023). Without a comprehensive risk assessment scheme, a security attack would show up as a mere statistical fluctuation or an anomalous feature rather than an expected occurrence (Granato & Polacek, 2019). Similarly, an excessive number of false positives within a large, complex organization would paralyze the security system and lower public confidence, enhancing uncertainties in security protection and deterring critical information from being placed in the system (Palsson, Gudmundsson & Shetty, 2020). Often, attacks are stealthy - blending in with non-target threats, dramatically increasing security risks and seriously challenging the effectiveness of traditional threat models. Attacks that do not follow a defined pattern are not as well understood by risk assessment models and complicate the decision-making process (Franco et al., 2024; Gilbert, 2021).

Three approaches to identifying risk factors determine potential loss scenarios: (1) examine the probability factor, (2) assess harm or financial loss incurred by the loss, or (3) conduct an overall risk assessment scheme (Mukhopadhyay et al., 2019). The most complete risk assessment model generally includes both a physical and economic analytic application. A multi-level-based risk assessment approach based on diverse opinions in the field will result in a more equitable risk assessment model for public consumption (Lee, 2021).

1. Establishing and defining the context in which an organization is operating. 2. Identifying relevant threats, loss factors, and their sources (Yarovenko et al., 2021). 3. Analyzing the risk associated with the threats, loss factors, vulnerabilities, probability, and propensity for occurrence. 4. Identifying and evaluating suitable methods for mitigating probable loss factors. Threats are usually governed by proprietary rules, state, and federal laws (Dambra, Bilge & Balzarotti, 2020). As part of a well-prepared formal risk management plan, this process would require the security specialist to address: - Areas of potential vulnerability within an infrastructure that have been attacked before. - Areas of potential vulnerability that have never been attacked before. - Areas that are attacked less frequently than other, seemingly comparably inviting, areas (Ganin et al., 2020). 5. Making ultimately optimized risk management decisions based on risk assessment. Rates of acceptable risk, generally drawn from state and federal laws, using state and federal funding resources (Shetty et al., 2018; Gilbert, 2018).

Risk assessment forms the basis for the entire risk management process. As part of the planning and decision-making process, a risk assessment is generally shaped around the following key tasks:

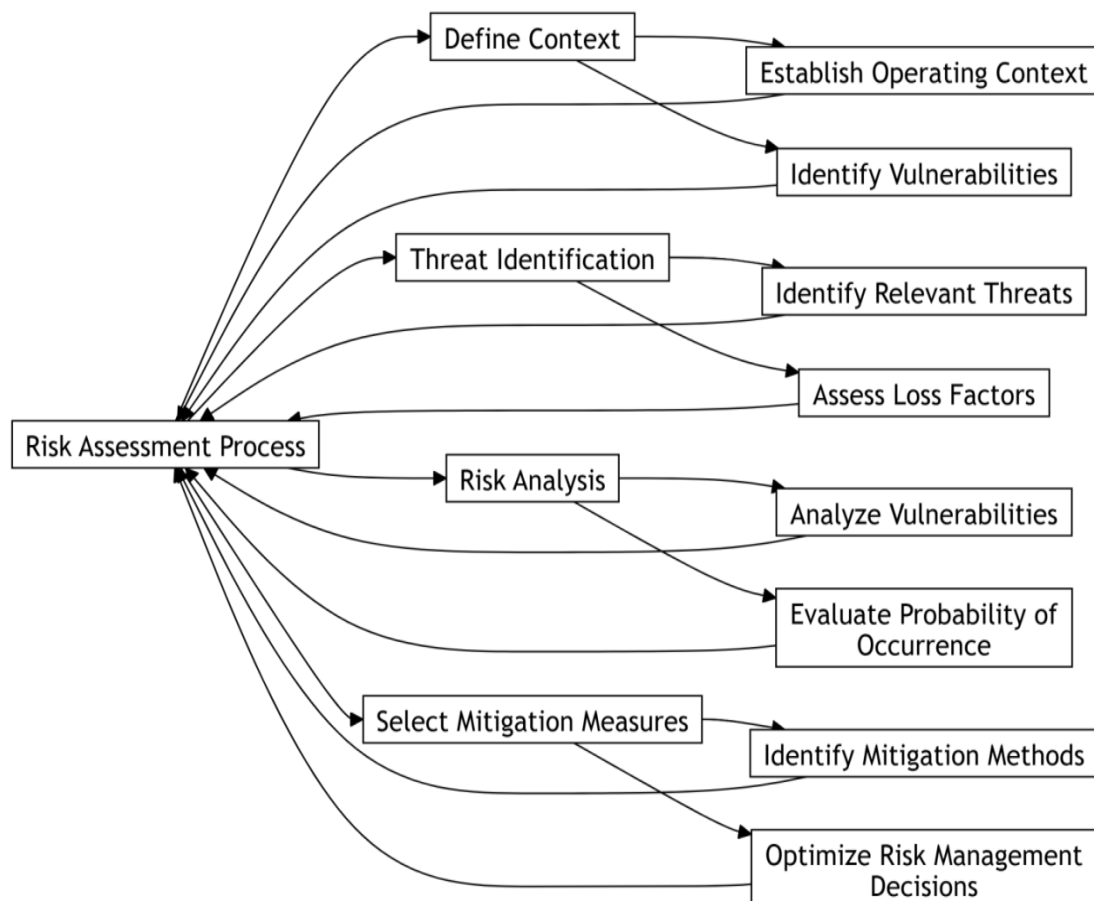


Figure 10: A Risk Assessment Process.

This risk assessment framework provides a systematic approach to managing risks, from identifying vulnerabilities to selecting and optimizing mitigation strategies. By following this process, organizations can proactively address threats, minimize potential damage, and improve overall security posture.

Identifying Data Security Risks

In identifying risks, there are "threat agents" who have "interplay" in all potential risk models due to their diverse ranges, different backgrounds, approaches, incentives, and terrorist groups (Fagade, 2018). It is the policy of the information security officer or the CISO to assist the business in managing and minimizing the complete threat profile of all users at all times. If the organization has sensitive data that could potentially be targeted, it might require a high level of security (Serfontein, 2020; Opoku-Mensah, Abilimi & Amoako, 2013). Fortunately, companies recognize their duty to safeguard personal financial information, and they work with their clients to mitigate and manage any risk of information. However, companies should not stop there (Rane, 2020).

Risk identification in the context of data security risks is to identify what compromises can take place. Risks can be identified because of previous experience or the industry's best practices (Jaiswal, Dwivedi & Dewang, 2024). If there is any doubt in identifying the risk of a particular compromise, then there are considerable sources of information available, including industry journals, journal articles, internet resources, or security consultants (Padur, Borrior & Hailes, 2025; Gilbert, 2012). The value of understanding the risks facing an organization is worldwide, as it is too easy to have a lackadaisical attitude toward securing data for a company, government, or organization by making investments in proprietary hardware and software (Rane, 2020). Without an effective data encryption and integrity solution, the investment ends up protecting nothing or no one.

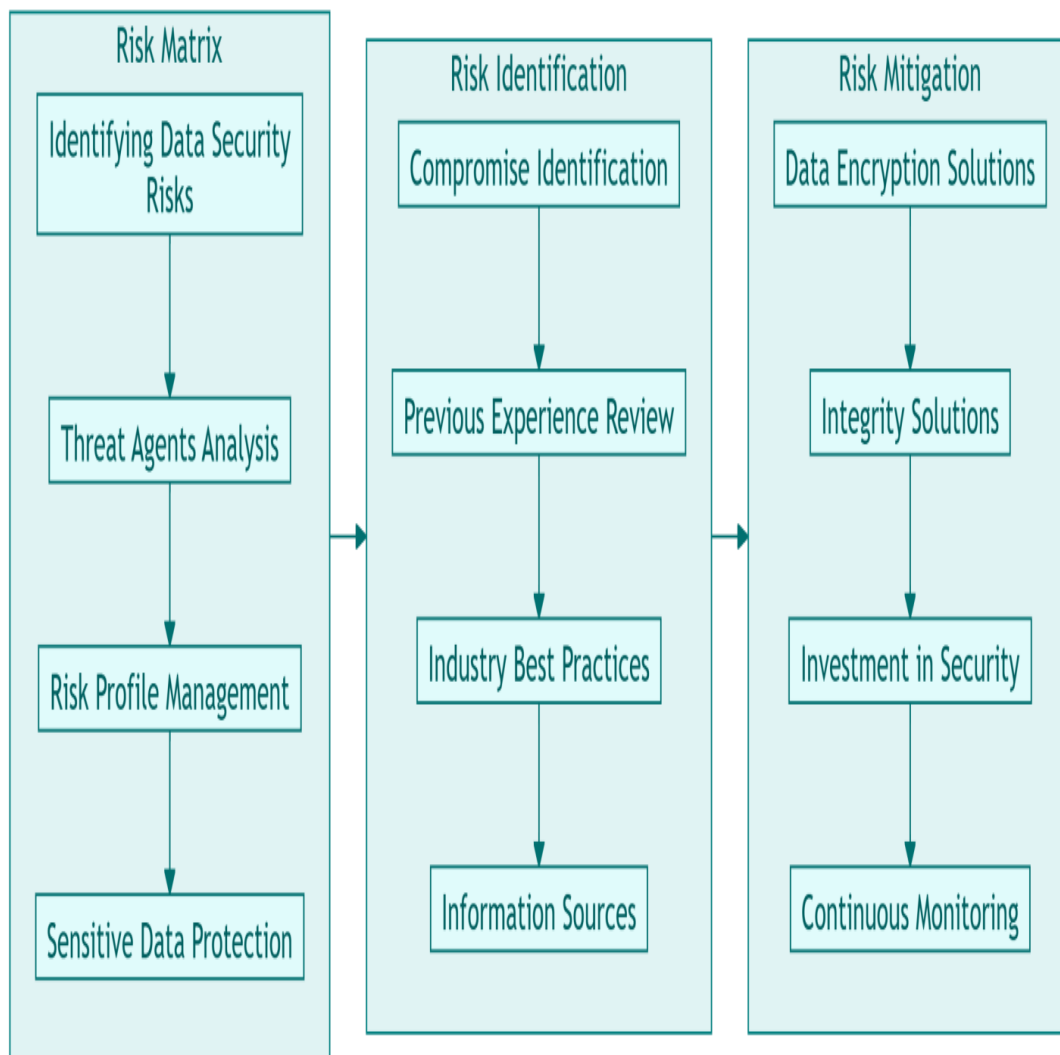


Figure 11: Data Security Risk Management.

This risk management framework provides a systematic approach to safeguarding sensitive data by identifying threats, assessing risks, and implementing mitigation strategies. By following these steps, organizations can proactively enhance their security posture, reduce vulnerabilities, and protect critical information assets.

Implementing Controls and Countermeasures

The protective treatment of information to protect it, including general information and digital information assets from unauthorized usage, unauthorized manipulation, and preservation, is called data security (Mitsarakis, 2023). As businesses undertake these valuable digital assets, the development of this sensitive information leads to cost-effective efforts to gain third-party regulatory guidelines and become a vital issue. This information has to be secured in an area that provides several uninterrupted requests for peace of mind to execute agreements and practice. The more sensitive the information, the higher is the applicable organizational requirement (Tovkun, 2023). The confidential stuff requires a load that is attached to the encryption of these data. Since security does not already generate a bonus, count uses data encryption opposed to perhaps cheaper key usage, for instance, you have to appoint the costs you need to bear to match your protection demands. Controls assure that implementation features for delivery of the security capabilities are all continuously active. They also ensure that limits and regulation specifications are still in compliance with the organization. Data encryption countermeasures require massive policies and processes implementation (Chairopoulou, 2024).

Implementing controls and countermeasures is necessary to strengthen security measures throughout the use of data encryption. The risk that can arise is a failure to implement adequately such controls and, therefore, the organization exposes to a security risk since encryption software is as flexible as dangerous as misused during the incorrect operation (AKINTOYE, 2023). An automated function that is useful for implementation and managing encryption routines in business is available. The data security is prepared with encryptions utilizing software codes technology. For the operating system, the latest encryption routines are initiated, which then provide additional protection from the driver, recording system and data storage layer throughout the operation. There is another problem that even when this mainframe integrated encryption solution is used (Obaidat et al., 2020). This process must still align with proper administrative reactive and proactive roles for protection functions. It must determine what function is to be accomplished and how function can be carried out without interfering with the data processing. The proper security countermeasure may put away the function.

Table 6: Risk Factors Analysis which details individual risk factors, their estimated likelihood, and potential impact

Risk Factor	Estimated Likelihood (Scale 1-5)	Potential Impact (Scale 1-5)	Notes
Unauthorized Access	4.5	5	High risk if access controls fail; may result in major data breaches and financial losses.
Malware Attack	3.5	4	Common threat; effective antivirus and timely patching are crucial to minimize disruption.
Insider Threat	3.0	3.5	Requires strict monitoring and access control; risk from both malicious and inadvertent actions.
Phishing / Social Engineering	4.0	4	Frequently exploited attack vector; ongoing employee training is essential.
Loss/Theft of Portable Media	2.0	2.5	Mitigation via encryption and physical security measures; risk increases with sensitive data.
Industrial Espionage	2.5	4.5	Low frequency but can have severe competitive and financial repercussions.

This table provides a concise overview of key risk factors, their relative likelihood, and potential impact, helping prioritize the focus areas for effective risk management and mitigation strategies.

Data Encryption in Cloud Environments

Pearson (2020), indicated that while data-in-transit encryption in the cloud was performed over virtual private networks (VPNs), this is not typically the case for data-at-rest encryption. Pearson noted that data can be at risk in the cloud because "the data at rest problem is different since the data, even when encrypted, is not solely under the enterprise's control." Vegesna (2019), stressed the importance of also encrypting data in cloud stores: "There are many new storage services that operate externally to cloud VM instances. Consider encrypting S3 objects with symmetric keys, and then protect the keys with HSMs in your on-premises data center. It can be done." In the interest of complete encryption, Vasconcelos Soares dos Santos (2024), also recommended: "Another method is to encrypt sensitive data in-memory using code compatible encryption, and keep the keys in a Hardware Security Module (HSM) on-premises. Some sensitive data will drop to disk and be written to unencrypted EBS volumes of snapshots while VMs are being written or saved and will need to be addressed separately (Gabriel et al., 2022). Temp files and TCP/IP spools add another dimension to the problem that complicates solving data-at-rest security by encryption" (Mei et al., 2022). These recommendations did not; however, seem to offer a clear solution to the problem of backup copies of files that will be unencrypted when decrypted for processing.

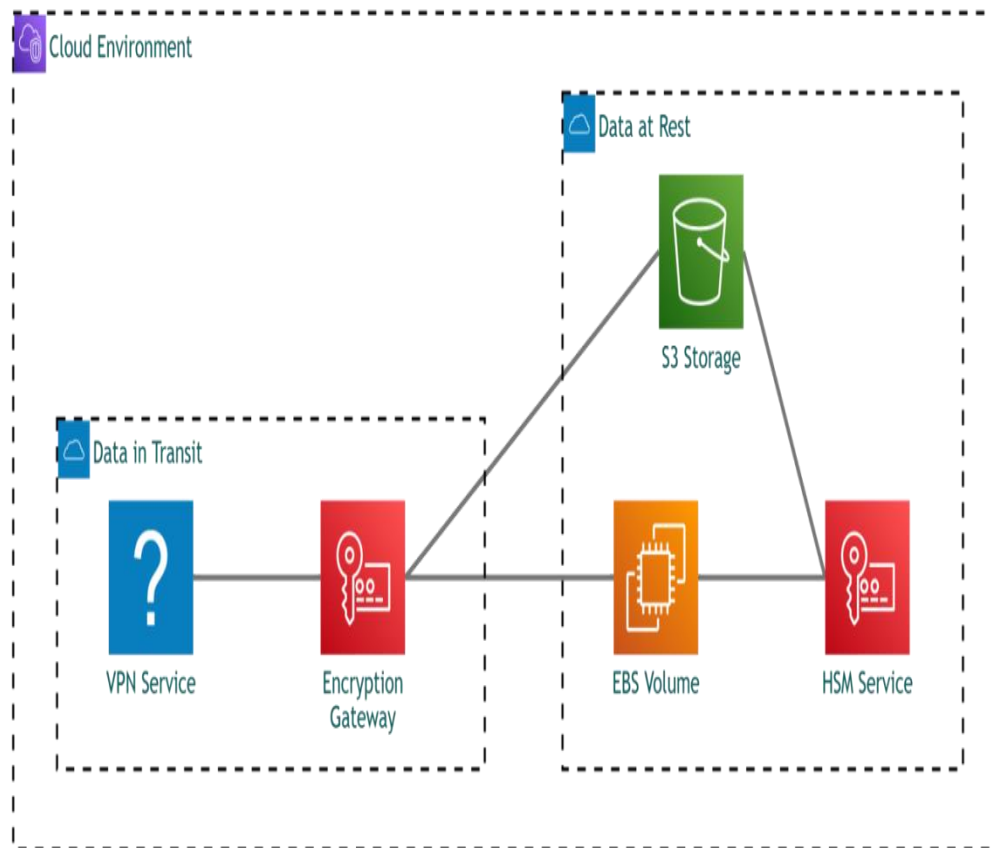


Figure 12: A cloud security architecture focusing on data encryption and secure storage.

This architecture ensures a multi-layered security approach by encrypting data at every stage—both in transit and at rest. By leveraging VPNs, encryption gateways, cloud storage security, and HSM services, organizations can protect sensitive data from unauthorized access and cyber threats.

Challenges and Best Practices

The first line of defense is passwords. Companies and users must create a complex password policy, enforcing the creation of complex passwords and encrypting these passwords (Lekkala & Gurijala, 2024; Abdel-Basset, Moustafa & Hawash, 2022). The second layer of defense is encryption, username, and password implementing an integrated one-time card. The third layer of security is an opportunity to connect by entering secured information such as social security number, date of birth, birth date, and mother's maiden name (Gautam, 2024). The feature is a response to the challenge created by production and visiting the users by asking three or four different questions about the user. Only when the questions are answered satisfactorily, mail is delivered (Lekkala & Gurijala, 2024). By this number, password, secret list, and username (as well as one-time card), authentic on communications dynamics are created (Dhillon, 2023). The need to authenticate channels is eliminated if the user decides for a VPN based on the company's internal network.

Only a corporate VPN connection through a wireless/Internet connection can provide secure data transfers based on the algorithms applied at the application level (Asija & Viral, 2025). Even if one has a secure connection over the corporate VPN, passwords and data files that are not encrypted can be grabbed when transmitted over the internal network. All of the servers used to secure data should be encrypted to provide a secure transmission of data (Obafemi & Ngeva, 2025). The encryption using a series of secure techniques provides a higher level of security, which translates to higher safety for users accessing the network (Hewage, Nawaf & Kesswani, 2024).

In a corporate environment, it is essential to have all transmissions through the network encrypted (Dhillon, 2023). This includes network card to network card communication, application to application communication, including transmissions through a wireless or an internet connection (Sharma et al., 2025). If wireless access points are exposed, transmitted or received encrypted data would be accessible

In this paper, we discussed well-known and widely accepted public key encryption algorithms. Note that encryption by itself does not provide full security when transmitting data from the sender to the receiver. This publicly available security method encrypts data using one of the described best algorithms, and it only applies to the ciphertext of the data. When a user wants to receive a message secured by the mentioned algorithm, keys exchanged using another public/private key method should be used. Otherwise, access points for unauthorized access are created.

Table 7: Cloud Encryption Best Practices

Best Practice/Recommendation	Challenge Addressed	Mitigation Strategy/Implementation
Encrypt Data-at-Rest	Data stored in the cloud is not solely under enterprise control and may be vulnerable even when encrypted	Encrypt cloud storage objects (e.g., S3) using symmetric keys, and protect these keys with on-premises Hardware Security Modules (HSMs)
In-Memory Encryption of Sensitive Data	Sensitive data may temporarily be written to unencrypted storage (e.g., EBS snapshots, temp files) during processing	Use code-compatible in-memory encryption for sensitive data, ensuring that encryption keys remain secured in an on-premises HSM
Enforce Strong Password Policies and Multi-Factor Authentication	Weak or compromised passwords can expose encrypted data, making unauthorized access possible	Mandate complex password policies and integrate multi-factor authentication (e.g., one-time cards, security questions) to strengthen user identity verification
Secure Data Transmissions via Corporate VPNs	Data transmitted over public networks is vulnerable to interception even if encrypted at the application level	Utilize corporate VPN connections for all data transfers, ensuring that even internal transmissions (wireless/Internet) are encapsulated within secure, encrypted tunnels
Encrypt All Server Communications	Unencrypted communications between servers, network cards, or applications may be intercepted or tampered with	Ensure that all internal communications, including network card-to-network card and application-to-application transfers, are encrypted using robust encryption protocols
Robust Key Management	Exposure of encryption keys can lead to complete system compromise if not properly managed	Maintain encryption keys separately from data, using on-premises HSMs and strict key lifecycle management to prevent unauthorized access and key misuse

This table provides a clear and concise summary of the best practices for securing data in cloud environments, highlighting both the challenges encountered and the recommended strategies for mitigating these risks.

Data Encryption in IoT Devices

Contemporary research focuses on the development of a new NIST lightweight standard (LWC-BEET) that should be considered for battery-operated devices, such as RFID, smart cards, and its future implementation in IoT devices (Goulart et al., 2022). The flexibility, customization, and cost-effective design of the lightweight cryptography standard make it the prime choice for IoT devices (Zeadally, Das & Sklavos, 2021). However, the challenge remains in preserving stringent information security properties, such as confidentiality, integrity, data validation, and privacy, in IoT devices. The integration of efficient and light symmetric data cryptographic algorithms, including quad-core parallel advanced encryption algorithm, and light forwarding search encryption algorithms, is applied with their optimized energy consumption as a new trend in this research area (Qashou, Hazzaa & Yousef, 2024). The paper explore the efficient lightweight encryption key permutation and design the light symmetric authenticated encryption algorithm with the light forward search algorithm and apply it to the heterogeneous IoT cloud. The designed system efficiently reduces and conserves the power source.

Encrypting data significantly preserves confidentiality, integrity, and privacy in the communication protocol in IoT architecture. The trade-off in encrypting data requires using a light encryption algorithm to save energy consumption (Figuerola-Hernandez Jr, 2019). The symmetric key algorithms, such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES), are the widely used light encryption algorithms. To enhance the light encryption algorithms and reduce energy consumption, the Parallel Light Advanced Encryption Standard (PLAES) algorithm and Efficient Advanced Encryption Standard (EffAES) algorithm employ a better forward search algorithm (Singh et al., 2024). The efficiency of these encrypting algorithms counteracts the main drawback in the lightweight encryption algorithms in the transmission protocols in the heterogeneous IoT cloud system (Zeadally, Das & Sklavos, 2021). The Light Forward Search Encryption (LFSE) is a more efficient and light encryption standard system that outperforms the forward search encryption algorithm. This LFSE algorithm saves a huge amount of power and reduces energy consumption during data transmission.

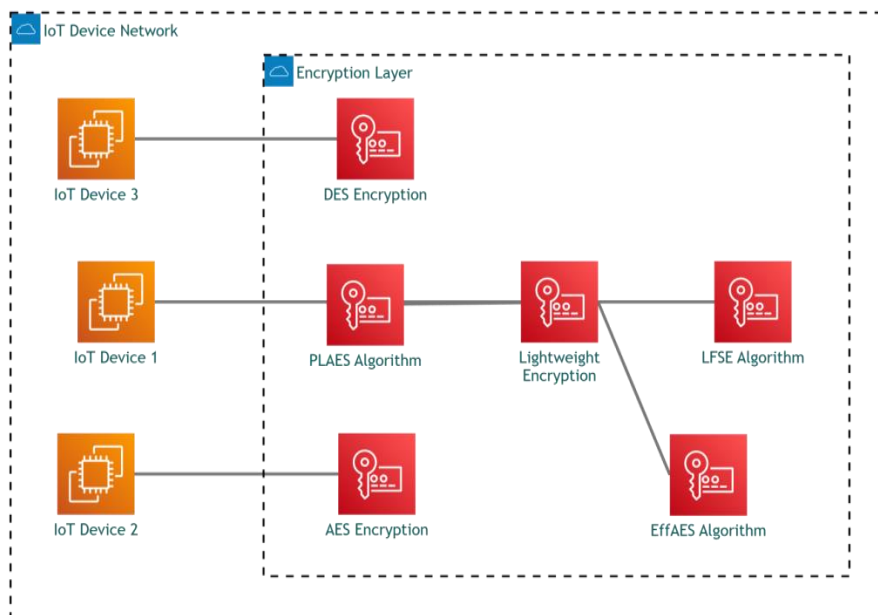


Figure 13: An IoT Device Network with encryption layer.

This encryption framework highlights the diverse encryption methods used in IoT security, balancing performance, power consumption, and security strength. While AES and lightweight encryption methods provide strong protection, DES is considered outdated. The adoption of lightweight encryption algorithms is particularly important in IoT networks, ensuring that devices remain secure without overloading their limited computational resources.

Security Concerns and Solutions

Cryptography is a science of encoding and decoding messages to secure the content from adversaries. Cryptography is a specialized domain of cryptology that concerns itself with encryption of messages (Shapiro et al., 2019). Various coding techniques are used to hide messages or transform messages utilizing various encryption methodologies. Information security is a critical issue in this computer and internet era, and it is of the companies' interest to protect valuable information. The reverse is true for the unethical hackers, crackers, intentional bugs, and malicious users with an intention to gain unauthorized access and steal or disparage sensitive, secret, confidential corporate information (Schwenk, 2022). Companies can employ different techniques to protect information from exposure to unauthorized access. One of the protective means is the simplest technique; for instance, the encryption process pads the hidden messages with gibberish, and only those who others are given deciphering the code or an important key. The approach is a mathematical practical method to make a message secure. Hash functions (MD5, AND SHA-1), symmetric key algorithms, and public-key algorithms are the basic cryptographic algorithms that protect data in transit, at rest, and in use (Portmann & Renner, 2022).

We are living in an era of information explosion, and information, disinformation, and misinformation are constantly floating around us (Kizza, 2024; Abilimi et al., 2013). One of the primary concerns of this era is protecting confidential information from prying eyes (Portmann & Renner, 2022; Christopher, 2013). The majority of business organizations (banks, financial houses) including individuals carry out money transactions, banking over the internet, which is a risk-prone environment due to potential threats like cryptography, security threats, cyber terrors, eavesdropping, and theft of critical business information (Renner & Wolf, 2023; Abilimi & Yeboah, 2013). In this paper, the focus will be on financial enterprise information security using security management tools like computer science, cryptography, network security, and information safeguard, privacy technology, security engineering, and security risk management.

Table 8: Comparison of Lightweight Encryption Algorithms

Algorithm	Energy Consumption	Computational Requirements	Security Level	Additional Comments
PRESENT	Low	Minimal – optimized for low-resource hardware	Moderate (Suitable for IoT, but with 80-/128-bit key options)	Designed specifically for constrained devices with a small hardware footprint
SIMON	Very Low	Very Low – efficient	Moderate to High	Developed by NSA; widely adopted in

		hardware implementation	(Depends on configuration)	resource-constrained applications
SPECK	Very Low	Low – optimized for software implementation	Moderate to High (Comparable to SIMON)	Software-friendly cipher, ideal for devices with limited processing power
PRINCE	Low	Low – designed for low-latency environments	Moderate (Limited by its 64-bit block size)	Focuses on fast encryption with minimal delay, but block size may limit its use in high-security applications

This table provides a quick reference to help assess which lightweight encryption algorithm might best suit specific energy and performance constraints while balancing the required level of security.

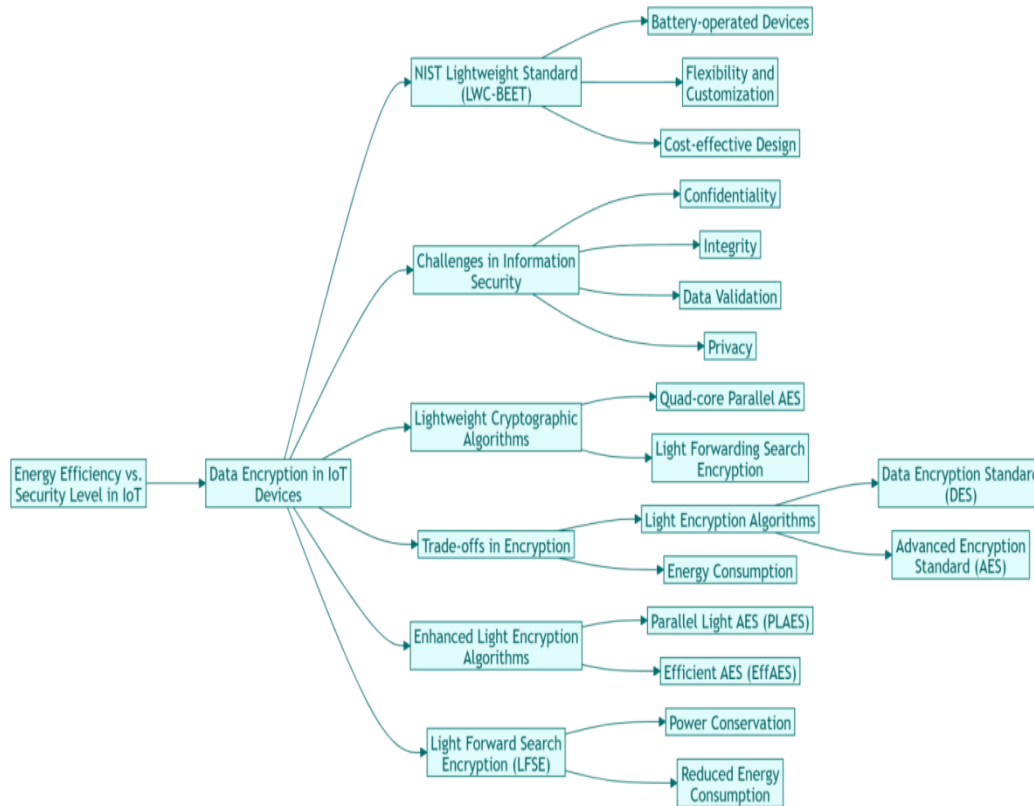


Figure 14: The relationship between energy efficiency and security levels in IoT devices.

This concept map highlights the need for balance between energy efficiency and security in IoT encryption. While lightweight cryptographic algorithms optimize performance, trade-offs must be considered to ensure strong encryption without excessive power consumption. New encryption techniques, such as PLAES, EffAES, and LFSE, provide efficient alternatives that meet the demands of IoT security.

Case Studies

In this paper, three major case studies are presented. Each case study represents an attempt by a single nation to control the export of encrypted products. Each instance is a failure, a view supported by the success in overcoming each government's restrictions with practically the same techniques favored by drug lords: the metaphorical speed boats and go-fast cars lead the real-life equivalent. These government policies led to strained international relationships, contributed to the development of the European Union's antitrust case against Microsoft, and drowned failing foreign companies attempting to develop US-style encryption products (Aoki, 2017). Also, these policy statements contributed to the formation of the American Civil Liberties Union's / Electronic Frontier Foundation Digital Privacy Act (ACLU/ EFF DPA); an act favorably supported by many countries and the UN's World Intellectual Property Organization (Jovanovic, 2020; ROSSI SILVANO, 2016).

Data Breaches and Encryption Failures

According to Reddy (2021), encryption does not assure privacy. For example, the Fact Corner illustrates how keys to more secure symmetric ciphers can be discovered by methodically testing every member of an enormous key space, thus revealing each unsent message. Moreover, despite their eminent security, cryptographic protocols can create financial crises or user distress. Therefore,

encryption is employed as part of a broader data safeguard structure that includes other safeguards and a means for adversarial detection and response (Krishnan, 2017).

Managers employ encryption to safeguard sensitive numerical and textual information from unauthorized use, particularly when the information is in storage or movement (Reddy et al., 2023; Abilimi et al., 2015). For example, the paper describes a simple substitution procedure whereby numerical amounts are encrypted into pseudo-random digits, then that result is distributed via a secured channel. Both of those steps rely on encryption that is solid only for sport. By contrast, the encryption of modern digital information is performed by sophisticated and complex computer algorithms based on scientific discoveries and mathematical theorems (Jaime et al., 2023; Abilimi & Adu-Manu, 2013; Burkhalter et al., 2021).

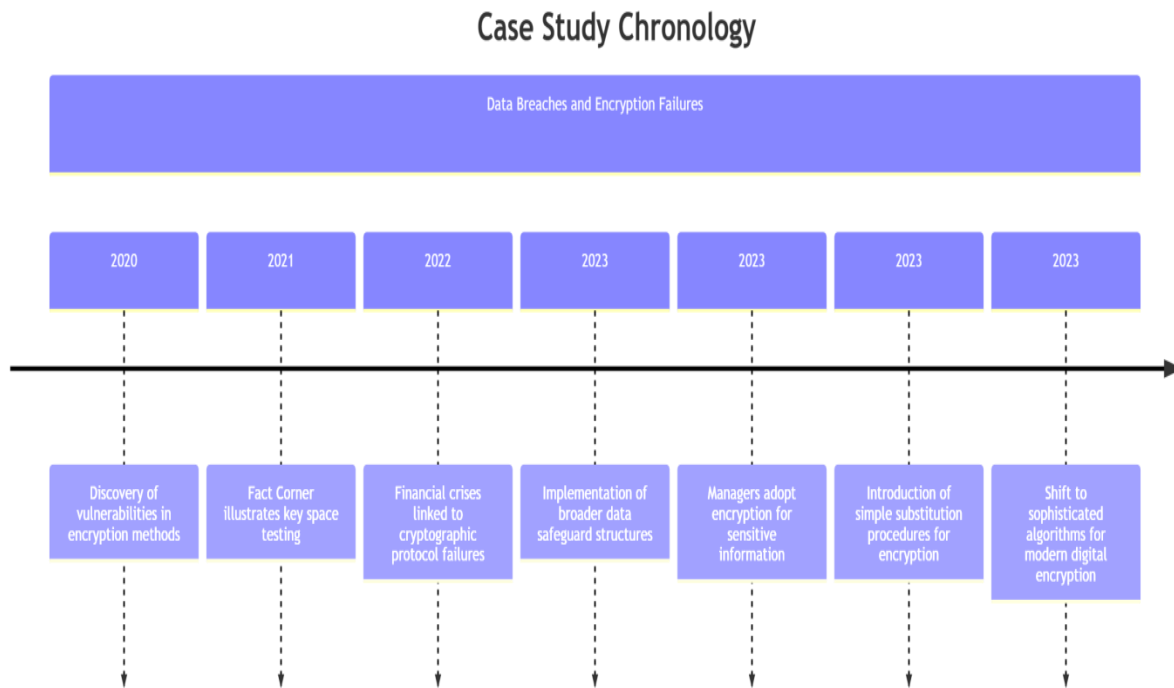


Figure 15: A case study chronology on data breaches and encryption failures.

This case study chronology illustrates how encryption practices have evolved in response to security breaches. Early vulnerabilities and financial crises forced organizations to strengthen encryption strategies, leading to the adoption of more advanced cryptographic solutions. The timeline highlights the constant need for innovation in encryption methods to stay ahead of cyber threats.

Table 9: Case Studies Overview

Case Study	Country	Encryption Failure Factors	Outcomes/Implications
Case Study 1	United States	Overly restrictive export controls; reliance on outdated enforcement mechanisms; circumvention via alternative methods	Strained international relationships; spurred digital privacy debates and contributed to the formation of acts such as the ACLU/EFF DPA
Case Study 2	European Union	Mismatches between regulatory frameworks and market practices; ineffective control over encryption product exports	Led to antitrust investigations (e.g., against Microsoft); increased scrutiny over technology export policies
Case Study 3	[Country X]*	Inadequate regulatory measures; failure to adapt policies to modern encryption technologies; market disruption by unauthorized export	Resulted in market failures for domestic encryption products and prompted policy reforms toward more flexible, innovation-friendly standards

*Note: "Country X" represents a nation where similar export control attempts have led to market disruptions and eventual policy changes, as observed in the case studies discussed.

This table provides a concise summary of the case studies, highlighting the key factors and consequences of attempts to control encryption exports across different regions.

Quantum Computing and Encryption

In mathematics and computer science, quantum computing, also called quantum computer science, is the study of extending computer technology to exploit the quantum state superposition to effectively solve computational challenges that might be challenging or unfeasible if approached by classical computer methods (Ajala et al., 2024). The power of quantum computing derives from one of the basic tenets of quantum mechanics that a particle can exist in more than one state at a time. In the binary system, only two parameters exist between 0 and 1, and the set of quantum state parameters ranges between 0 and 1. When particles pass through systems of qubits, they amplify and decrease the ability of calculations, thereby reducing data processing restrictions which would normally take an inordinate length of time (Azhari & Salsabila, 2024; Gilbert et al., 2025). The mysterious concept of qubits adds another quest, "if everything can be expressed in 1s and 0s, do those two entities equal everything?"

The exponential growth of data produced by the Internet of Things, social media, big data, and other advanced technologies needs secure, reliable, and private communication with computational speed and processing capabilities (Nkulenu, 2024). There are several public key encryption algorithms in existence today, for example, RSA, ElGamal, Elliptic Curve Cryptography (ECC), and Quantum Key Distribution (QKD) (Marella & Parisa, 2020). However, these encryption algorithms are not adequately prepared to deal with the threat of quantum computer attacks. Other effective public key encryption methods are Post-Quantum Cryptography (PQC) designed to resist cyber-attacks from quantum computers, such as McEliece, LATTICE, hash-based signature algorithms, and multivariate-quadratic-equations (Möller & Vuik, 2017). It is important to initiate measures and responses to evolve these new encryption systems because quantum computers have the potential to break conventional cryptography systems and are beginning to have a significant impact on a variety of industries where employing new information security solutions are an immediate necessity (Marella & Parisa, 2020).

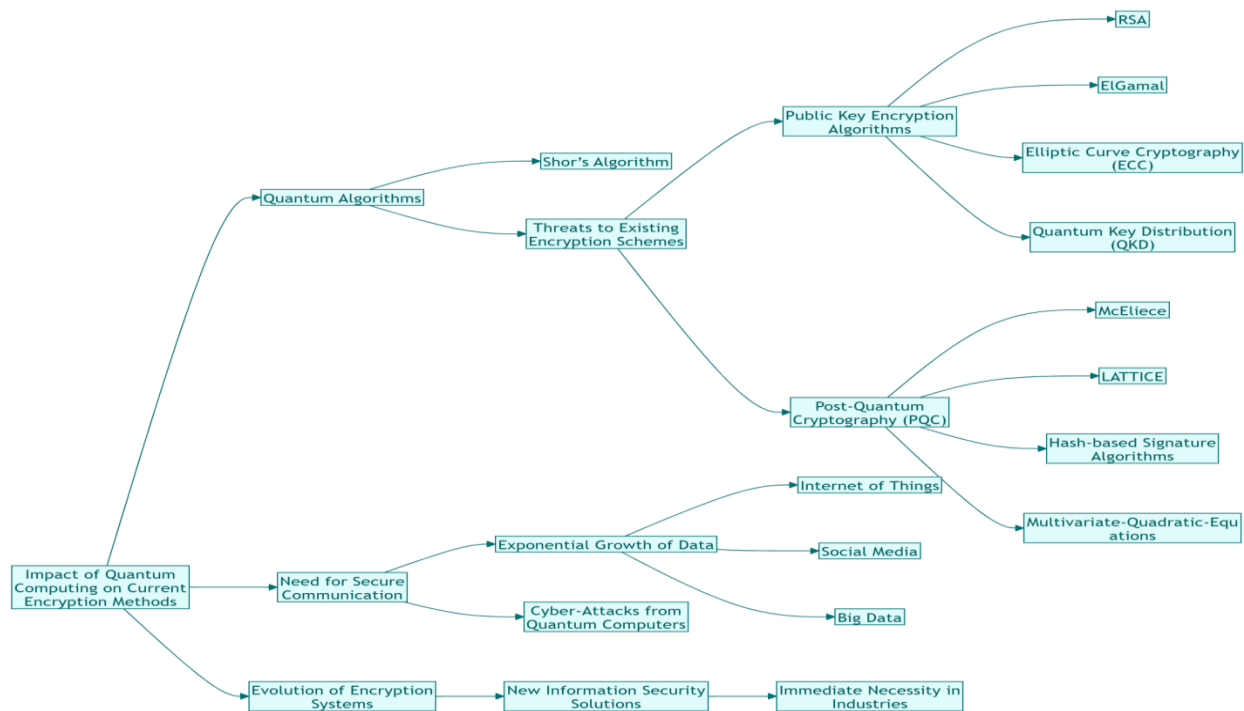


Figure 16: A concept map on the impact of quantum computing on encryption methods.

The rapid development of quantum computing poses an imminent threat to traditional encryption methods, especially public-key cryptography like RSA and ECC. This has driven the urgent need for post-quantum cryptography, ensuring that future encryption methods remain secure against quantum attacks. The shift toward quantum-safe cryptographic algorithms is critical for securing IoT, big data, and global communication networks.

VI. Findings, Conclusions and Recommendations

Findings

- **Critical Importance of Data Encryption:** The research confirms that encryption is vital in protecting sensitive data in modern digital environments. It highlights that in an era where data is often dubbed the "new green gold," organizations must carefully balance encryption speed with the level of security to safeguard their assets.

- **Performance vs. Security Trade-Offs:** A comparative analysis shows that symmetric encryption techniques, while fast and efficient, present challenges in secure key distribution. In contrast, asymmetric (public-key) encryption offers stronger security guarantees—by using a public/private key pair—but at the cost of higher computational overhead and slower performance.
- **Role and Limitations of Hash Functions:** Hash functions play a crucial role in ensuring data integrity and supporting non-repudiation. However, despite their relatively simpler design, no hash function is entirely immune to attacks, emphasizing the need for continuous improvement and monitoring.
- **Strengths and Weaknesses of Advanced Algorithms:** Detailed evaluations of algorithms such as Twofish, RC6, AES, RSA, and ECC revealed:
 - **Twofish** offers high speed and security due to its consistent block operations and robust key management.
 - **RC6** demonstrates flexibility through adjustable rounds and key sizes, making it secure against exhaustive key searches.
 - **AES** remains a widely adopted standard owing to its balance between performance and security.
 - **RSA** continues to provide strong public-key security, although its vulnerability to quantum computing poses future challenges.
 - **ECC** is emerging as a competitive alternative due to its ability to deliver high security with smaller key sizes.
- **Integrated Risk Management:** The study emphasizes the necessity of employing a comprehensive risk management framework that integrates multivariate risk analysis, threat identification, and layered security controls. This integration is critical to managing vulnerabilities such as unauthorized access and key interception.
- **Emerging Trends – Cloud, IoT, and Quantum Threats:** In cloud environments, data-at-rest remains at risk even when encryption is applied, while IoT devices demand lightweight, energy-efficient encryption. Furthermore, emerging quantum computing technologies may soon undermine current encryption methods, requiring a shift toward post-quantum cryptographic techniques.

Conclusions

- **Balanced Encryption Strategy is Essential:** The research concludes that no single encryption method meets all security and performance requirements. Instead, a balanced strategy that combines symmetric and asymmetric techniques—tailored to specific use cases—is essential for robust data protection.
- **Need for Comprehensive Risk Management:** Effective security is achieved not by encryption alone but through an integrated risk management approach. This includes regular risk assessments, continuous monitoring, and updating of security measures to keep pace with evolving threats.
- **Adaptability to Emerging Threats:** With the advent of quantum computing and the expansion of IoT and cloud technologies, existing encryption protocols face significant challenges. Organizations must be proactive in adopting next-generation cryptographic solutions and flexible risk management policies.
- **Holistic Approach to Data Security:** The study reinforces that ensuring data security involves more than just deploying encryption algorithms. It requires a layered security strategy that addresses technical vulnerabilities, human factors, and compliance with regulatory standards.

Recommendations

- **Implement a Multi-Layered Encryption Strategy:** Organizations should deploy both symmetric and asymmetric encryption methods as appropriate to their operational needs, ensuring that key management practices are robust and that encryption solutions are scalable.
- **Adopt Comprehensive Risk Management Practices:** It is recommended that companies integrate regular risk assessments, multivariate analysis of threat vectors, and proactive monitoring into their security frameworks. This holistic approach should include technical, administrative, and procedural controls.
- **Invest in Lightweight and Post-Quantum Cryptography:** For IoT and cloud environments, organizations should prioritize the development and adoption of lightweight encryption algorithms that conserve energy while maintaining high security. Additionally, preparation for quantum computing threats through the exploration of post-quantum cryptographic techniques is essential.
- **Continuous Review and Update of Security Measures:** Given the dynamic nature of cybersecurity threats, organizations should ensure that encryption and risk management strategies are regularly reviewed and updated to reflect current threats, technological advances, and regulatory requirements.

- Enhance Training and Awareness: Finally, alongside technical measures, organizations should invest in training for security personnel and employees to ensure that best practices in data encryption and risk management are consistently applied across the enterprise.

From a risk management perspective, we vindicated that often; two parallel cryptography techniques or more are implemented, causing greater complexity and greater security. We also explained that to strengthen public key cryptography, it may be applied to double the use of the modulus to be factored and more than some binary factors. These walls give a greater encrypted value of the RSA notation.

In this paper, we present many future trends, developments, and novelties regarding the world of data encryption. First of all, we highlighted that keys are at the fundamental base of data encryption algorithms, and we noticed that symmetric-key and public-key cryptographies are the two basic and mostly used data encryption mechanisms. After a comprehensive survey on public and private key encryption algorithms (including RSA, El Gamal, and ECC), we found several vulnerabilities, weaknesses, and fragilities in data protocols, specifically in the RSA protocol. We discovered that the success factor of an encryption algorithm may be given by the size of the key that the user configures as the encryption algorithm's parameter, and the quality of the prime number used. Until a key length parameter of almost 2048, 3072, or 4096, encryption mechanisms are certainly safe. However, as enumerated, and even when using advanced hardware material and/or software applications or both, there are currently some techniques that permit breaking a prime-number encryption system.

References

1. Abdel-Basset, M., Moustafa, N., & Hawash, H. (2022). Deep learning approaches for security threats in IoT environments. John Wiley & Sons.
2. Abilimi, C. A., Asante, M., Opoku-Mensah, E. & Boateng, F. O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application. Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015
3. Abilimi, C. A., & Adu-Manu, K. S. (2013). *Examining the impact of Information and Communication Technology capacity building in High School education in Ghana*. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 9, September – 2013
4. Abilimi, C. A., Amoako, L., Ayembillah, J. N., Yeboah, T. (2013). Assessing the Availability of Information and Communication Technologies in Teaching and Learning in High School Education in Ghana. *International Journal of Engineering Research and Technology*, 2(11), 50 - 59.
5. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 11, November - 2013
6. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications*, 119, 2603–2637.
7. Adenekan, T. K. (2024). Enhancing end-to-end VoIP security: A reliable privacy protection approach using elliptic-curve Diffie–Hellman and dynamic key changes.
8. Adeniyi, A. E., Jimoh, R. G., & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. *Computers and Electrical Engineering*, 118, 109330.
9. AKINTOYE, C. O. (2023). Evaluating information security threat in the supply chain: Human factor.
10. Aoki, K. (2017). Neocolonialism, anticommons property, and biopiracy in the (not-so-brave) new world order of international intellectual property protection. In *Globalization and Intellectual Property* (pp. 195–242). Routledge.
11. Aumasson, J. P. (2024). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press, Inc.
12. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
13. Aven, T. (2019). *The science of risk analysis: Foundation and practice*. Routledge.
14. Ayyasamy, S. (2024). Contemporary high-performance computing for big data applications. *Journal of Information Technology and Digital World*, 5(4), 375–384.
15. Azhari, R., & Salsabila, A. N. (2024). Analyzing the impact of quantum computing on current encryption techniques. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 5(2), 148–157.
16. Asija, D., & Viral, R. K. (2025). Cyber security: Emerging trends best practices. In *Cyber Security Solutions for Protecting and Building the Future Smart Grid* (pp. 161–187).
17. Bahig, H. M., Nassr, D. I., Bhery, A., & Nitaj, A. (2020). A unified method for private exponent attacks on RSA using lattices. *International Journal of Foundations of Computer Science*, 31(2), 207–231.
18. Bauskar, S. (2023). Advanced encryption techniques for enhancing data security in cloud computing environment. Available at SSRN 4987321.
19. Beierle, C., Biryukov, A., dos Santos, L. C., Großschädl, J., Perrin, L., Udovenko, A., ... & Biryukov, A. (2019). Schwaemm and esch: Lightweight authenticated encryption and hashing using the sparkle permutation family. *NIST round, 2*, 162893–162908.

20. Boura, C., & Naya-Plasencia, M. (Eds.). (2023). Symmetric cryptography, volume 1: Design and security proofs. John Wiley & Sons.
21. Bouleghlimat, I., Boudouda, S., & Hacini, S. (2024). PPSecS: Privacy-preserving secure big data storage in a cloud environment. *Arabian Journal for Science and Engineering*, 49(3), 3225–3239.
22. Burkhalter, L., Küchler, N., Viand, A., Shafagh, H., & Hithnawi, A. (2021). Zeph: Cryptographic enforcement of end-to-end data privacy. In *15th USENIX Symposium on Operating Systems Design and Implementation (OSDI 21)* (pp. 387–404).
23. Belcastro, L., Cantini, R., Marozzo, F., Orsino, A., Talia, D., & Trunfio, P. (2022). Programming big data analysis: Principles and solutions. *Journal of Big Data*, 9(1), 4.
24. Cannady, S. (2019). A study on the efficiency of encryption algorithms for wireless sensor networks (Doctoral dissertation, Pace University).
25. Candelario Burgoa, F. J. (2021). Addressing security and privacy issues by analyzing vulnerabilities in IoT applications.
26. Chairpoulou, S. (2024). Cybersecurity in industrial control systems: A roadmap for fortifying operations (Master's thesis, Πανεπιστήμιο Πειραιώς).
27. Christopher, A. A.(2013). Effective Information Security Management in Enterprise Software Application with the Revest-Shamir-Adleman (RSA) Cryptographic Algorithm. *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 2 Issue 8, August - 2013.
28. Corelli, A. (2014). Understanding financial risk management. Routledge.
29. Daemen, J., Rijmen, V., Daemen, J., & Rijmen, V. (2020). The advanced encryption standard process (pp. 1–8). Springer Berlin Heidelberg.
30. Dambra, S., Bilge, L., & Balzarotti, D. (2020, May). SoK: Cyber insurance—technical challenges and a system security roadmap. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1367–1383). IEEE.
31. Datta, N., Dutta, A., Nandi, M., & Yasuda, K. (2018). Encrypt or decrypt? To make a single-key beyond birthday secure nonce-based MAC. In *Advances in Cryptology—CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38* (pp. 631–661). Springer International Publishing.
32. Dhillon, G. (2023). Cybersecurity challenges in an AI enabled world. *Journal of Information Systems Security*, 19(3), 165–168.
33. Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34, 1–42.
34. Dwivedee, S., & Singh, A. K. (2015). Efficient implementation of Advanced Encryption Standard.
35. Easttom, W. (2022). Modern cryptography: Applied mathematics for encryption and information security. Springer Nature.
36. Ermoshina, K., & Musiani, F. (2022). Concealing for freedom: The making of encryption, secure messaging and digital liberties (p. 274). Mattering Press.
37. Fagade, T. (2018). A multi-domain approach for security compliance, insider threat modelling and risk management (Doctoral dissertation, University of Bristol).
38. Figueroa-Hernandez Jr, J. (2019). A comparison of lightweight ciphers meeting NIST lightweight cryptography requirements to the advanced encryption standard.
39. Franco, M. F., Künzler, F., Von der Assen, J., Feng, C., & Stiller, B. (2024). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. *Computers & Security*, 139, 103737.
40. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1), 183–199.
41. Gautam, A. (2024). Enhancing security and usability in password-based web systems through standardized authentication interactions.
42. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's *The Road*. [English Journal, Volume 102, Issue Characters and Character](https://doi.org/10.58680/ej201220821), p. 40 - 47. <https://doi.org/10.58680/ej201220821>.
43. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. *The Educational Forum*, 83(1), 60–74. <https://doi.org/10.1080/00131725.2018.1505017>.
44. Gilbert, C. (2021). Walking the popular education spiral - an account and analysis of participatory action research with teacher activists. *Educational Action Research*, 30(5), 881–901. <https://doi.org/10.1080/09650792.2021.1875856>
45. Gilbert, C. (2022). Making the Invisible Visible: Professional Development to Support Teacher Activism. *Kappa Delta Pi Record*, 58(1), 14–19. <https://doi.org/10.1080/00228958.2022.2005426>
46. Gilbert, C. & Gilbert, M.A.(2024a). Unraveling Blockchain Technology: A Comprehensive Conceptual Review. *International Journal of Emerging Technologies and Innovative Research* (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : <http://www.jetir.org/papers/JETIR2409066.pdf>
47. Gilbert, C. & Gilbert, M.A.(2024b). Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. *International Journal of Latest Technology in Engineering Management & Applied Science*, 13(8), 132-141. <https://doi.org/10.51583/IJLTEMAS.2024.130816>

48. Gilbert, C. & Gilbert, M.A.(2024c). The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441.
https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.
49. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, 3(9), 9-9.
50. Gilbert, C. & Gilbert, M.A.(2024e). Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. *International Journal of Emerging Technologies and Innovative Research* (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available <http://www.jetir.org/papers/JETIR2410134.pdf>
51. Gilbert, C. & Gilbert, M.A. (2024f). [Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy](#). *International Journal of Advanced Engineering Research and Science*, ISSN (Online): 2455-9024, Volume 9, Issue 4, pp. 95-106.
52. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, 3(10). <https://doi.org/10.38124/ijrsmt.v3i10.54>
53. Gilbert, C., & Gilbert, M. A. (2024h). [Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness](#). *International Journal of Latest Technology in Engineering, Management & Applied Science*, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.
54. Gilbert, C. & Gilbert, M.A. (2024i). [Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques](#). *Global Scientific Journal* (ISSN 2320-9186) 12 (10), 1368-1392.
55. Gilbert, C. & Gilbert, M.A. (2024j). The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation.*International Research Journal of Advanced Engineering and Science* (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.
56. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. *International Journal of Research Publication and Reviews*, Vol 5, no 11, pp 219-236.
57. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, 9(4), 205–219.
58. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, 5(11), 889–907. <https://www.ijrpr.com>
59. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, 9(10), 131–137. <https://doi.org/10.51584/IJRIAS.2024.910013>
60. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, 5(11), 3235-3256. <https://www.ijrpr.com>.
61. Gilbert, C., & Gilbert, M. A. (2024p). CRYPTOGRAPHIC FOUNDATIONS AND CYBERSECURITY IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY.*Global Scientific Journals*,ISSN 2320-9186,12(11),464-487. <https://www.globalscientificjournal.com>
62. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science*, 9(4), 238–251.
63. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology*, 3(11). <https://doi.org/10.38124/ijrsmt.v3i11.76>
64. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology*, 3(11). <https://doi.org/10.38124/ijrsmt.v3i11.77>
65. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews*, 5(12), 507–533. <https://www.ijrpr.com/>
66. Gilbert, C., & Gilbert, M. A. (2024u). Organizational and leadership aspects of cybersecurity governance. *International Journal of Research Publication and Reviews*, 5(12), 1174–1191. Retrieved from www.ijrpr.com
67. Gilbert, C., & Gilbert, M. A. (2024v). The development and evolution of cryptographic algorithms in response to cyber threats. *International Journal of Research Publication and Reviews*, 5(12), 1149–1173. Retrieved from www.ijrpr.com
68. Gilbert, C., & Gilbert, M. A. (2024w). Privacy-preserving data mining and analytics in big data environments. *Global Scientific Journal*, 12(12). Retrieved from www.globalscientificjournal.com
69. Gilbert, C., & Gilbert, M. A. (2024x). Investigating the challenges and solutions in cybersecurity using quantum computing and cryptography. *International Research Journal of Advanced Engineering and Science*, 9(4), 291–315.
70. Gilbert, C., & Gilbert, M. A. (2024y). The integration of blockchain technology into database management systems for enhanced security and transparency. *International Research Journal of Advanced Engineering and Science*, 9(4), 316–334.

71. Gilbert, C., & Gilbert, M. A. (2025a). *Artificial intelligence (AI) and machine learning (ML) for predictive cyber threat intelligence (CTI)*. International Journal of Research Publication and Reviews, 6(3), 584–617. <http://www.ijrpr.com>
72. Gilbert, C., & Gilbert, M. A. (2025b). Continuous user authentication on mobile devices. International Research Journal of Advanced Engineering and Science, 10(1), 158–173.
73. Gilbert, C., & Gilbert, M. A. (2025c). *Patterns and vulnerabilities of cryptocurrency-related cybercrimes*. Global Scientific Journal, 13(3), 1950–1981. <https://www.globalscientificjournal.com>
74. Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025). Enhancing detection and response using artificial intelligence in cybersecurity. *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, 7(10), 87–104.
75. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.
76. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.
77. Goulart, A., Chennamaneni, A., Torre, D., Hur, B., & Al-Aboosi, F. Y. (2022). On wide-area IoT networks, lightweight security and their applications—a practical review. *Electronics*, 11(11), 1762.
78. Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. *Journal of Information Security*, 11(3), 138–148.
79. He, Y., Ye, N., & Zhang, R. (2021). Analysis of data encryption algorithms for telecommunication network-computer network communication security. *Wireless Communications and Mobile Computing*, 2021(1), 2295130.
80. Hewage, C., Nawaf, L., & Kesswani, N. (2024). AI applications in cyber security and communication networks.
81. Huang, Y. T., Chiang, D. L., Chen, T. S., Wang, S. D., Lai, F. P., & Lin, Y. D. (2022). Lagrange interpolation-driven access control mechanism: Towards secure and privacy-preserving fusion of personal health records. *Knowledge-Based Systems*, 236, 107679.
82. Ince, M. N., Günay, M., & Ledet, J. (2022). Lightweight distributed computing framework for orchestrating high performance computing and big data. *Turkish Journal of Electrical Engineering and Computer Sciences*, 30(4), 1571–1585.
83. Jaiswal, A., Dwivedi, P., & Dewang, R. K. (2024). Machine learning approaches to detect, prevent and mitigate malicious insider threats: State-of-the-art review. *Multimedia Tools and Applications*, 1–41.
84. Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, 23(21), 8944.
85. Javadpour, A., Ja'fari, F., Taleb, T., Zhao, Y., Yang, B., & Benzaïd, C. (2023). Encryption as a service for IoT: Opportunities, challenges, and solutions. *IEEE Internet of Things Journal*, 11(5), 7525–7558.
86. Jovanovic, S. (2020). Governing the internet: The extraterritorial effects of the general data protection regulation.
87. Kizza, J. M. (2024). Computer network security protocols. In *Guide to Computer Network Security* (pp. 409–441). Cham: Springer International Publishing.
88. Koukoulopoulos, D. (2019). The distribution of prime numbers (Vol. 203). American Mathematical Soc.
89. Kultinov, K., Liu, M., & Wang, C. (2024). The implementations and optimizations of elliptic curve cryptography based applications. *INTERNATIONAL JOURNAL OF COMPUTERS AND THEIR APPLICATIONS*, 254.
90. Kurdi, H., & Thayananthan, V. (2021). Authentication mechanisms for IoT system based on distributed MQTT brokers: Review and challenges. *Procedia Computer Science*, 194, 132–139.
91. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, 7(7), 8-13.
92. Lahraoui, Y., Lazaar, S., Amal, Y., & Nitaj, A. (2024). Securing data exchange with elliptic curve cryptography: A novel hash-based method for message mapping and integrity assurance. *Cryptography*, 8(2), 23.
93. Lekkala, S., & Gurijala, P. (2024). Leveraging AI and machine learning for cyber defense. In *Security and Privacy for Modern Networks: Strategies and Insights for Safeguarding Digital Infrastructures* (pp. 167–179). Berkeley, CA: Apress.
94. Lekkala, S., & Gurijala, P. (2024). Security and privacy for modern networks.
95. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659–671.
96. Logunleko, K. B., Adeniji, O. D., & Logunleko, A. M. (2020). A comparative study of symmetric cryptography mechanism on DES, AES, and EB64 for information security. *International Journal of Science Research in Computer Science and Engineering*, 8(1).
97. Mahalle, V. S., & Shahade, A. K. (2014, October). Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm. In *2014 International Conference on Power, Automation and Communication (INPAC)* (pp. 146–149). IEEE.
98. Marcu, O. C., & Bouvry, P. (2024). Big data stream processing (Doctoral dissertation, University of Luxembourg).
99. Marella, S. T., & Parisa, H. S. K. (2020). Introduction to quantum computing. *Quantum Computing and Communications*, 61.

100. Möller, M., & Vuik, C. (2017). On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and Information Technology*, 19, 253–269.
101. Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: A survey. *Wireless Networks*, 27(2), 1515–1555.
102. Moch, A., & List, E. (2019). Parallelizable MACs based on the sum of PRPs with security beyond the birthday bound. In *Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17* (pp. 131–151). Springer International Publishing.
103. Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, 21, 997–1018.
104. Mezrag, F., Bitam, S., & Mellouk, A. (2022). An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. *Journal of Network and Computer Applications*, 200, 103282.
105. Mäntysaari, P., & Mäntysaari, P. (2010). Corporate risk management. In *The Law of Corporate Finance: General Principles and EU Law: Volume I: Cash Flow, Risk, Agency, Information* (pp. 115–157).
106. Nkulenu, G. (2024). Quantum computing: The impending revolution in cryptographic security.
107. Obafemi, O. A., & Ngeva, T. M. (2025). Cyber security: Emerging threats, challenges, and future directions.
108. Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, 9(2), 44.
109. Oladipupo, E. T., Abikoye, O. C., Imoize, A. L., Awotunde, J. B., Chang, T. Y., Lee, C. C., & Do, D. T. (2023). An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks. *IEEE Access*, 11, 1306–1323.
110. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst.*, 4, 50–57.
111. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760–769.
112. Palsson, K., Gudmundsson, S., & Shetty, S. (2020). Analysis of the impact of cyber events for cyber insurance. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 45(4), 564–579.
113. Pearson, S. D. (2020). Encryption methods in protecting cloud data when adopting cloud solutions: A Delphi study (Doctoral dissertation, Capella University).
114. Portmann, C., & Renner, R. (2022). Security in quantum cryptography. *Reviews of Modern Physics*, 94(2), 025008.
115. Pratt, K. (2020). Primes from sums of two squares and missing digits. *Proceedings of the London Mathematical Society*, 120(6), 770–830.
116. Qashou, A., Hazzaa, F., & Yousef, S. (2024). Wireless IoT networks security and lightweight encryption schemes-survey. *International Journal of Emerging Technology and Advanced Engineering*, 14(1), 28–36.
117. Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 12, 547–566.
118. Rane, S. V. (2020). Quantitative model of a facility-level radiological security risk index (Doctoral dissertation, Purdue University).
119. Reddy, J., Elsayed, N., ElSayed, Z., & Ozer, M. (2023). A review on data breaches in healthcare security systems. *International Journal of Computer Applications*, 184(45), 1–7.
120. Reddy, J. (2021). Data breaches in healthcare security systems (Master's thesis, University of Cincinnati).
121. Renner, R., & Wolf, R. (2023). Quantum advantage in cryptography. *AIAA Journal*, 61(5), 1895–1910.
122. Raj, K. (2019). Foundations of blockchain: The pathway to cryptocurrencies and decentralized blockchain applications. Packt Publishing Ltd.
123. ROSSI SILVANO, A. (2016). Internet privacy in the European Union and the United States: Three essays on privacy, the internet, politics, implementation, business power, and surveillance in the European Union and the United States (Doctoral dissertation, European University Institute).
124. Schwenk, J. (2022). Guide to internet cryptography: Security protocols and real-world attack implications. Springer Nature.
125. Sharma, A., Bhatia, R., Sharma, D., & Kalra, A. (2025). Exploring AI's prowess in advancing cybersecurity. In *Smart Systems: Engineering and Managing Information for Future Success: Navigating the Landscape of Intelligent Technologies* (pp. 77–98). Cham: Springer Nature Switzerland.
126. Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 43, 224–238.
127. 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.

128. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access*.
129. Sood, R., & Kaur, H. (2023). A literature review on RSA, DES and AES encryption algorithms. *Emerging Trends in Engineering and Management*, 57–63.
130. 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.
131. Tovkun, Y. (2023). Personal data protection in context of cyberwarfare.
132. Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: State of the art, trends and future directions. *International Journal of Information Security*, 22(3), 737–748.
133. Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, 23(8), 4117.
134. Urooj, S., Lata, S., Ahmad, S., Mehruz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. *Alexandria Engineering Journal*, 72, 37–50.
135. Vasconcelos Soares dos Santos, N. (2024). Data security and user authentication in public cloud computing environments.
136. Vegesna, V. V. (2019). Investigations on different security techniques for data protection in cloud computing using cryptography schemes. *Indo-Iranian Journal of Scientific Research (IIJSR)*, 3, 69–84.
137. Wong, D. (2021). *Real-world cryptography*. Simon and Schuster.
138. Khaferi, A. J. B. Z. G., & Jusufi, A. (2024). The use of functions $f: D \times D \times D \rightarrow \mathbb{R}$ for encrypting and decrypting data in space.
139. Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management*, 22(2), 369–387.
140. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A. (2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, 2(7).
141. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.
142. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b). Automatic Biometric Student Attendance System: A Case Study Christian Service University College. *Journal of Engineering Computers & Applied Sciences*, 2(6), 117-121.
143. Yeboah T. & Abilimi C.A. (2013). *Using Adobe Captivate to create Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, www.ijert.org, “2(11).
144. Yin, F., & Shi, F. (2022). A comparative survey of big data computing and HPC: From a parallel programming model to a cluster architecture. *International Journal of Parallel Programming*, 50(1), 27–64.
145. Zeadally, S., Das, A. K., & Sklavos, N. (2021). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*, 14, 100075.
146. Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE Access*, 6, 18209–18237.
147. Zekaj, B., Jusufi, A., & Imeri-Jusufi, B. (2022). Using incomplete polynomial functions of the odd degree n and their inverses for data encryption and decryption. *IFAC-PapersOnLine*, 55(39), 241–246.
148. Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, 177, 176–190.
149. Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., & Muyeen, S. M. (2024). Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, 101357.