World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

A comprehensive review of cryptographic techniques and emerging trends in modern cybersecurity

Debjit Banerjee [1,*] and Arnab Acharyya [2]

[1] *Department of Computer Science and Engineering, Elitte College of Engineering, West Bengal, India.*
[2] *Department of Computer Science and Engineering, Swami Vivekananda Group of Institutes, West Bengal, India.*

World Journal of Advanced Research and Reviews, 2026, 31(01), 1434–1460

Publication history: Received on 14 June 2026; revised on 21 July 2026; accepted on 23 July 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.31.1.1951

Abstract

Cryptography is a fundamental pillar of modern cybersecurity, ensuring confidentiality, integrity, authentication, and non-repudiation in digital communication systems. This paper presents a comprehensive review of classical and modern cryptographic techniques, including symmetric encryption, asymmetric encryption, and cryptographic hash functions. Widely adopted algorithms such as Advanced Encryption Standard (AES), Rivest -Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) are analyzed in terms of performance, security, and application domains. Recent advancements such as homomorphic encryption, blockchain-based cryptography, and post-quantum cryptography are also explored. Comparative analysis highlights trade-offs between computational efficiency, key size, and resistance to emerging threats such as quantum computing. Furthermore, challenges such as key management, scalability, and implementation vulnerabilities are discussed. The paper concludes by identifying future research directions focusing on lightweight, quantum-resistant, and privacy-preserving cryptographic systems for next-generation applications including IoT, cloud computing, and artificial intelligence-driven environments.

Keywords: Cryptography; AES; RSA; ECC; Post-Quantum Cryptography; IoT Security; Encryption**.**

2010 Mathematics subject classification: 47H10, 54H25.

1. Introduction

Cryptography has become one of the fundamental technologies underpinning modern cybersecurity, providing the essential mechanisms required to protect digital information against unauthorized access, modification, and misuse. The rapid expansion of digital communication networks, cloud computing, Internet of Things (IoT) devices, artificial intelligence (AI), mobile applications, and distributed computing environments has significantly increased the volume of sensitive data transmitted and stored across interconnected systems. Consequently, the need for robust cryptographic techniques has become more critical than ever to ensure confidentiality, integrity, authentication, and non-repudiation in both personal and enterprise-level applications.

Over the past several decades, cryptographic research has evolved from classical encryption methods to sophisticated mathematical frameworks capable of addressing increasingly complex security challenges. Traditional symmetric-key algorithms, such as the Advanced Encryption Standard (AES), continue to provide efficient solutions for high-speed data encryption, while asymmetric cryptographic techniques, including the Rivest–Shamir–Adleman (RSA) algorithm and Elliptic Curve Cryptography (ECC), have enabled secure key exchange, digital signatures, and public-key infrastructures. In parallel, cryptographic hash functions have become indispensable for ensuring data integrity and authentication across a wide range of security protocols.

* Corresponding author: Debjit Banerjee

Despite these remarkable advances, the cybersecurity landscape continues to evolve rapidly. Emerging technologies such as cloud computing, blockchain, artificial intelligence, and edge computing introduce new security requirements that extend beyond the capabilities of conventional cryptographic mechanisms. Furthermore, the anticipated emergence of large-scale quantum computers presents a significant threat to widely deployed public-key cryptographic algorithms, thereby motivating intensive research into post-quantum cryptography and other next-generation security solutions. At the same time, privacy-preserving technologies, including homomorphic encryption and zero-knowledge proofs, have gained considerable attention for enabling secure computation and data sharing without exposing sensitive information.

Given the continuous evolution of cryptographic research and the increasing diversity of application domains, a comprehensive review of existing cryptographic techniques is both timely and valuable. While numerous studies have examined individual algorithms or specific application areas, there remains a need for an integrated review that systematically compares classical and emerging cryptographic approaches, evaluates their strengths and limitations, and highlights their suitability for modern cybersecurity applications.

This review paper presents a comprehensive overview of contemporary cryptographic techniques by first introducing the fundamental concepts and security objectives of cryptography before examining the major categories of cryptographic algorithms, including symmetric-key, asymmetric-key, hash-based, and hybrid cryptographic systems. The paper further discusses advanced techniques such as Elliptic Curve Cryptography, homomorphic encryption, blockchain-based cryptography, zero-knowledge proofs, and post-quantum cryptography. A comparative analysis is provided to evaluate these techniques with respect to security strength, computational efficiency, scalability, resource requirements, and practical deployment considerations. The review also explores major application domains, identifies current implementation challenges and limitations, and discusses emerging research directions aimed at developing lightweight, privacy-preserving, and quantum-resistant cryptographic solutions.

The findings presented in this review are intended to provide researchers, academicians, cybersecurity professionals, and practitioners with a consolidated understanding of the current state of cryptographic technologies and their future evolution. By synthesizing existing knowledge and identifying emerging trends, this paper contributes to a broader understanding of how modern cryptography can address the security challenges of next-generation digital infrastructures.

2. Fundamentals of Cryptography

Cryptography provides the theoretical and practical foundation for securing digital communication. It involves mathematical techniques and algorithms to transform readable data (plaintext) into an unreadable form (ciphertext) and vice versa, ensuring that only authorized parties can access the information. Core Terminologies

- **Plaintext:** Original readable message or data.
- **Ciphertext:** Encrypted, unreadable form of data.
- **Encryption:** Process of converting plaintext into ciphertext using an algorithm and a key.
- **Decryption** Reverse process of converting ciphertext back into plaintext.
- **Key:** A secret value used by cryptographic algorithms to perform encryption and decryption.
- **Algorithm:** A mathematical function used for encryption/decryption (e.g., AES, RSA).

2.1. Basic Cryptographic Process

The cryptographic system works as follows:

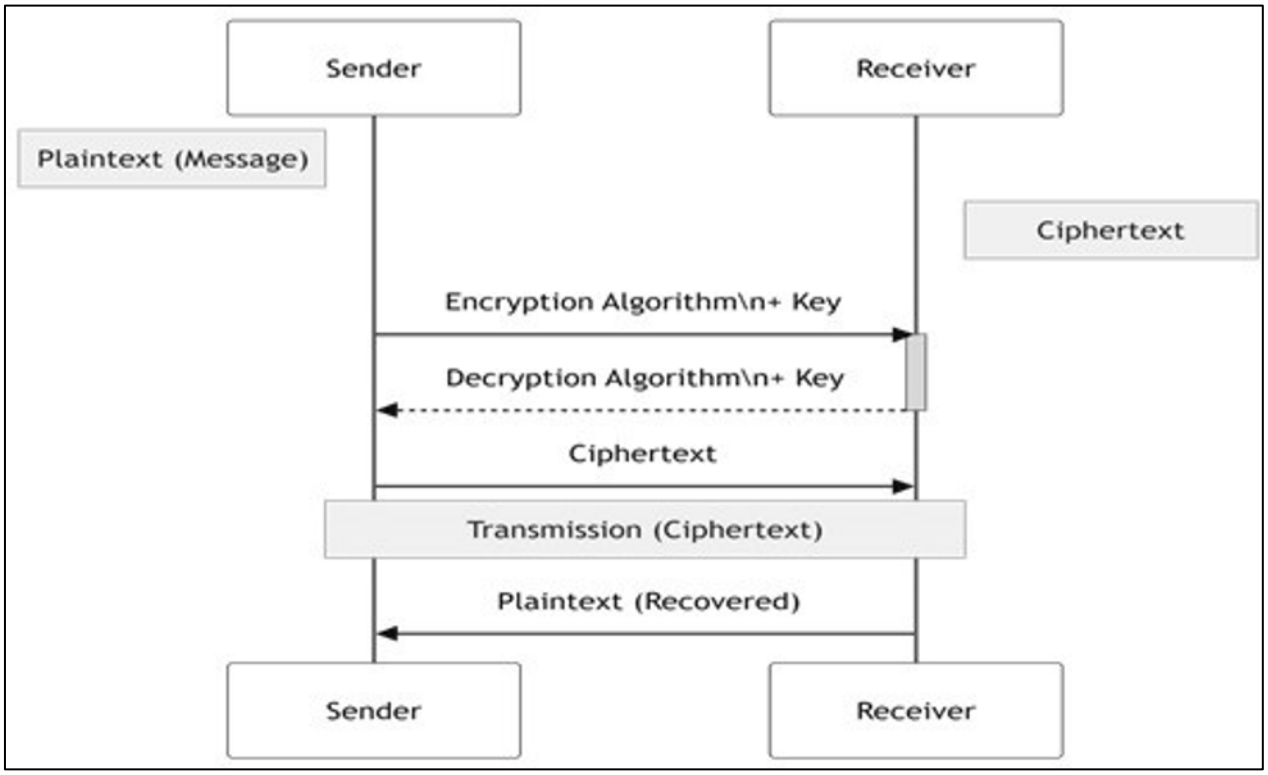

Figure 1 Basic Cryptographic Process

2.2. Types of Keys

- Symmetric Key
- Same key is used for encryption and decryption
- Faster but requires secure key sharing
- Asymmetric Key
- Uses a **public key** (encryption) and **private key** (decryption)
- More secure but computationally slower

2.3. Cryptographic Goals (Security Services)

Cryptography ensures four primary security objectives:

1. **Confidentiality**
    - Prevents unauthorized access to data
    - Achieved using encryption algorithms
2. **Integrity**
    - Ensures data is not altered during transmission
    - Achieved using hash functions
3. **Authentication**
    - Verifies the identity of users or systems
    - Implemented via digital signatures and certificates

4. **Non-Repudiation**

- Ensures that the sender cannot deny sending the message
- Achieved using digital signatures

2.4. Cryptographic Primitives

Cryptographic systems rely on fundamental building blocks:

Table 1 Cryptographic Primitives

Primitive	Function	Example
Encryption Algorithm	Secures data	AES, RSA
Hash Function	Ensures integrity	SHA-256
Digital Signature	Authentication	RSA Signature
Key Exchange	Secure key sharing	Diffie-Hellman

2.5. Encryption Models

Symmetric Encryption Model

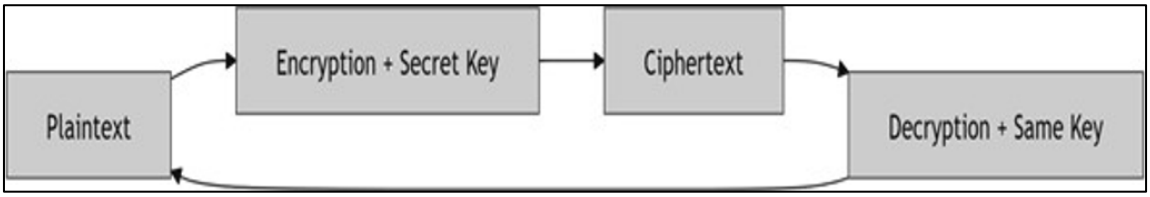

Figure 2 Encryption Models

2.6. Asymmetric Encryption Model

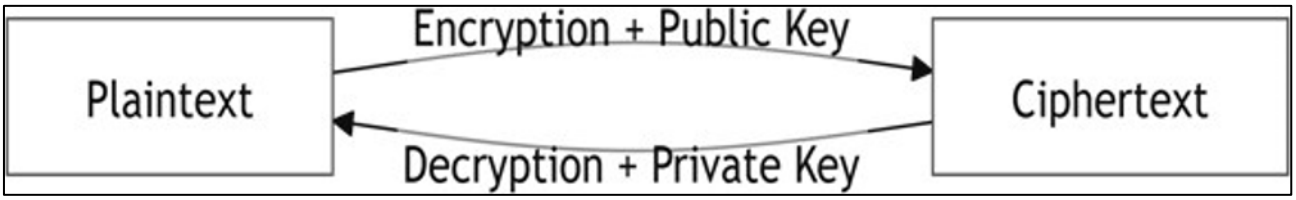

Figure 3 Asymmetric Encryption Model

2.7. Attack Models in Cryptography

Understanding threats is essential for designing secure systems:

- Ciphertext-Only Attack (COA)
- Known-Plaintext Attack (KPA)
- Chosen-Plaintext Attack (CPA)
- Man-in-the-Middle Attack (MITM)

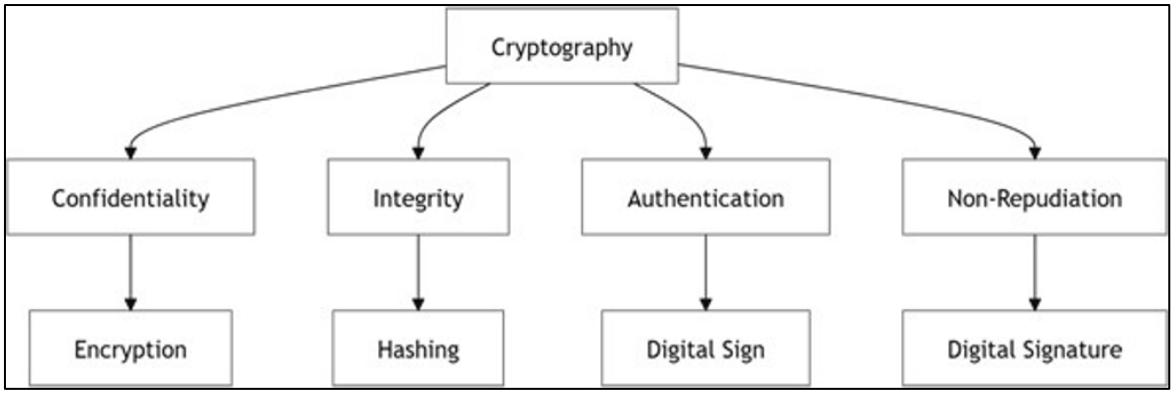

Figure 4 Cryptographic Security Services Overview

3. Classification of Cryptographic Techniques

Cryptographic techniques are broadly classified based on how keys are used and how data is processed. This classification helps in selecting appropriate algorithms for different security requirements such as speed, scalability, and level of protection.

3.1. Overview of Classification

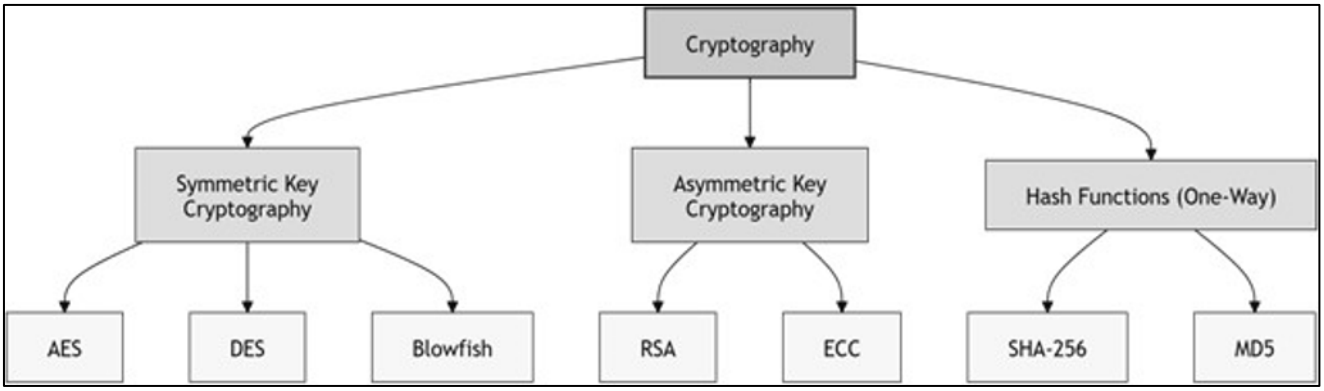

Figure 5 Classification of Cryptographic Techniques

3.2. Symmetric Key Cryptography

- Definition

Symmetric cryptography uses a **single secret key** for both encryption and decryption.

- Working Principle
  - Sender and receiver share the same key
  - Data is encrypted and decrypted using this shared key

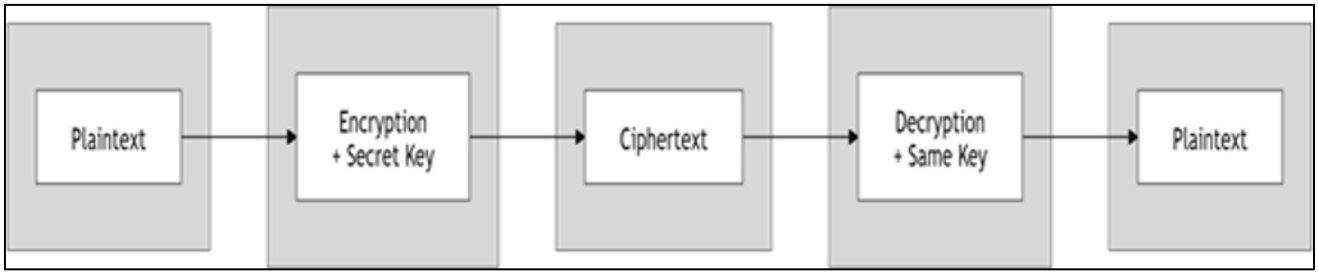

Figure 6 Symmetric Key Cryptography

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- Blowfish

2. **Advantages**
    - High speed and efficiency
    - Suitable for large data encryption
    - Low computational overhead
3. **Disadvantages**
    - Key distribution problem
    - Less secure if key is compromised

3.3. Asymmetric Key Cryptography

- Definition

Uses **a pair of keys:**

- Public Key (shared openly)
- Private Key (kept secret)

Working Principle

- Data encrypted with public key
- Only private key can decrypt

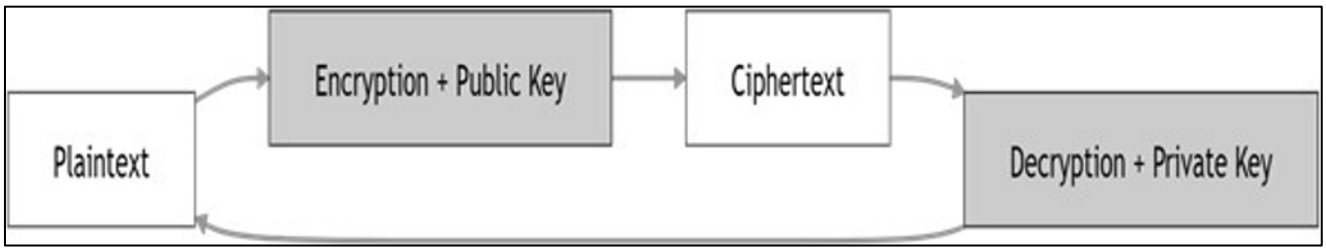

Figure 7 Asymmetric Key Cryptography

- **Common Algorithms**
    - RSA (Rivest-Shamir-Adleman)
    - ECC (Elliptic Curve Cryptography)
- **Advantages**
    - Secure key distribution
    - Enables digital signatures and authentication
- **Disadvantages**
    - Slower than symmetric cryptography
    - Computationally expensive

3.4. Hash Functions (One-Way Cryptography)

Definition:

Hash functions convert input data into a **fixed-length hash value**, and cannot be reversed.

Working Principle

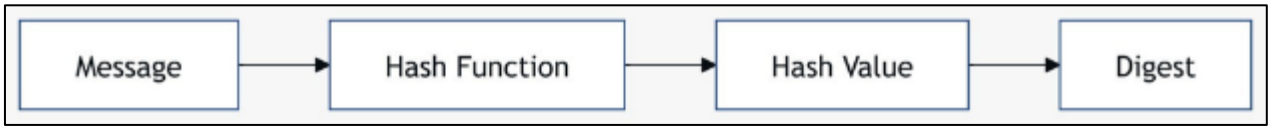

Figure 8 Hash Functions

Common Algorithms

- SHA-256
- SHA-3
- MD5 (now considered insecure)
- Advantages
- Ensures data integrity
- Fast computation
- No key required
- Disadvantages
- Cannot retrieve original data
- Vulnerable to collisions (in weak algorithms)

3.5. Hybrid Cryptography

Definition:

Combines **symmetric** and **asymmetric** cryptography to leverage the advantages of both.

Working Principle

- Asymmetric encryption used for key exchange
- Symmetric encryption used for data transmission
- Step 1: Public Key → Securely share symmetric key
- Step 2: Symmetric Key → Encrypt bulk data

Example

- SSL/TLS protocols
- Advantages
- Combines security + speed
- Widely used in real-world systems

3.6. Comparative Analysis

Table 2 Comparison of Cryptographic Techniques

Feature	Symmetric	Asymmetric	Hash Function
Keys Used	Single	Public + Private	No key
Speed	Fast	Slow	Very Fast
Security	Moderate	High	High
Use Case	Data encryption	Key exchange, authentication	Integrity verification
Example	AES	RSA, ECC	SHA-256

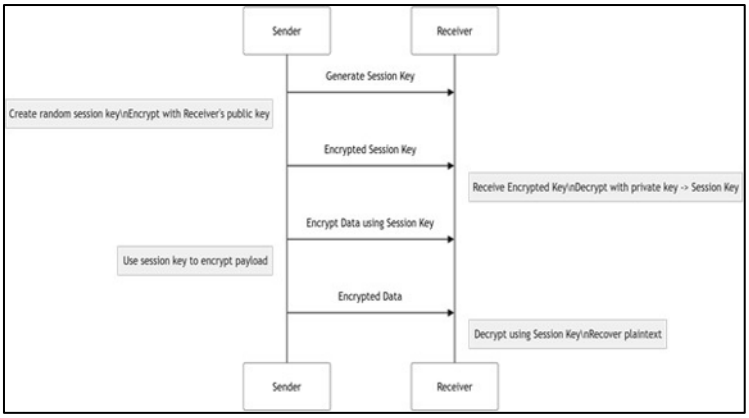

Figure 9 Hybrid Cryptographic System (Real-World Model)

4. Advanced Cryptographic Techniques

With the rapid evolution of cyber threats, traditional cryptographic methods are no longer sufficient on their own. Advanced cryptographic techniques have emerged to provide stronger security, enhanced privacy, and functionality in modern systems such as cloud computing, blockchain, IoT, and quantum environments.

4.1. Overview of Advanced Cryptography

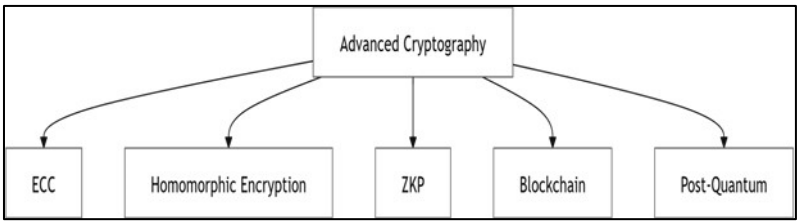

Figure 10 Overview of Advanced Cryptography

4.2. Elliptic Curve Cryptography (ECC)

- Definition

ECC is an asymmetric cryptographic technique based on the mathematics of elliptic curves over finite fields.

- Key Idea

Provides high security with **smaller key sizes**, making it ideal for resource-constrained devices.

- Working Principle

Uses points on an elliptic curve

Security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP)

- Curve Equation:

$y^2 = x^3 + ax + b$

- Key Representation

Public Key → Point on the curve

Private Key → Random number

- Advantages

Smaller key size (256-bit ECC ≈ 3072-bit RSA)

- Faster computation and lower power consumption

Applications

Mobile security

IoT devices

Digital signatures (ECDSA)

4.3. Homomorphic Encryption (HE)

- Definition

A form of encryption that allows computations to be performed directly on ciphertext without decrypting it.

- Working Principle / Types

Partial Homomorphic Encryption (PHE)

Fully Homomorphic Encryption (FHE)

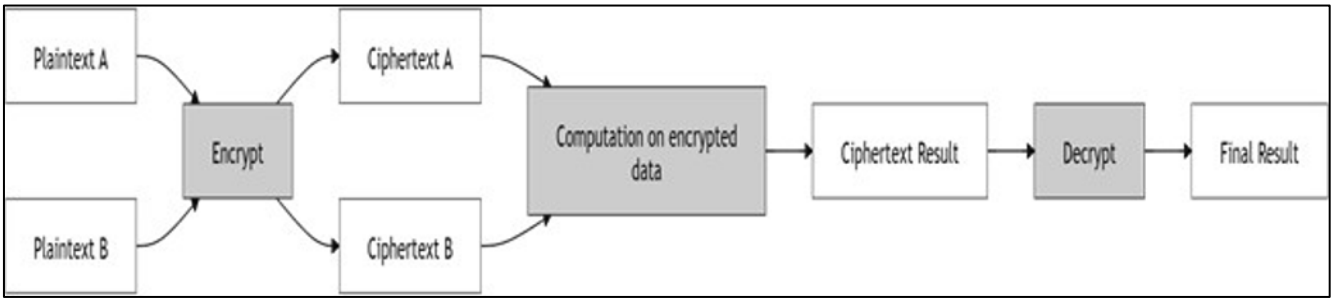

Figure 11 Homomorphic Encryption (HE)

- Advantages

Enables secure cloud computing

Preserves data privacy

- Applications

Secure data analytics

Privacy-preserving machine learning

4.4. Zero-Knowledge Proofs (ZKP)

- Definition

A cryptographic method where one party proves knowledge of information without revealing the information itself.

- Working Principle Prover → Verifier

“I know the secret”

Without revealing the secret

- Properties

Completeness

Soundness

Zero-knowledge

- Applications

Authentication systems

Blockchain privacy (e.g., zk-SNARKs)

4.5. Blockchain Cryptography

- Definition

Blockchain integrates cryptographic primitives such as hash functions and digital signatures to ensure secure, immutable transactions.

- Core Components

Block = Data + Hash + Previous Hash

- Working Principle

Block 1 → Block 2 → Block 3 → . . .

(Linked via cryptographic hashes)

- Advantages

Tamper-proof

Decentralized security

Transparency

Applications

Cryptocurrencies

Smart contracts

Supply chain

4.6. Post-Quantum Cryptography (PQC)

- Definition

Cryptographic algorithms designed to be secure against quantum computer attacks.

- Why Needed

Quantum algorithms (e.g., Shor's Algorithm) can break RSA and ECC.

- Types of PQC Algorithms

Lattice-based cryptography

Code-based cryptography

Hash-based cryptography

- Working Principle

Classical Crypto → Vulnerable to Quantum Attacks

Post-Quantum Crypto → Resistant to Quantum Attacks

- Applications

Future internet security

Government and defense systems

4.7. Comparative Overview of Advanced Techniques

Table 3 Comparison of Cryptographic Techniques

Technique	Key Feature	Strength	Use Case
ECC	Small key size	High efficiency	IoT, mobile
HE	Compute on encrypted data	High privacy	Cloud computing
ZKP	No data disclosure	Strong privacy	Authentication
Blockchain	Distributed ledger	Tamper-proof	Finance
PQC	Quantum resistance	Future-proof	Secure communication

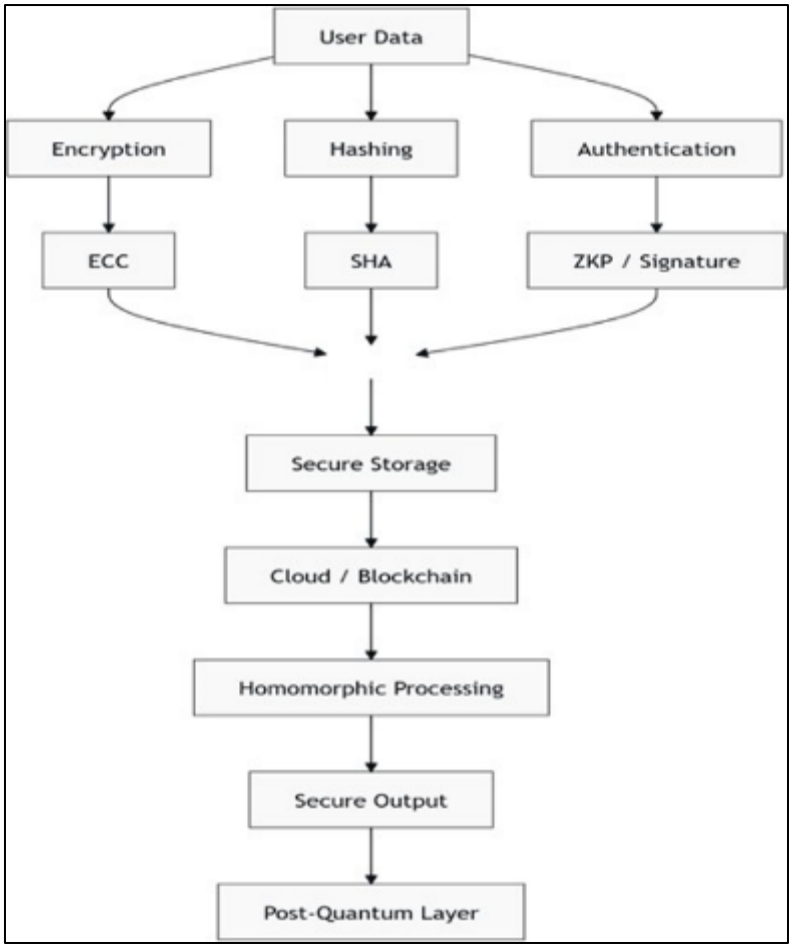

Figure 12 Integrated Advanced Cryptographic System

5. Comparative Analysis of Cryptographic Techniques

Comparative analysis is a crucial component of a review paper, as it evaluates different cryptographic techniques based on performance, security strength, computational cost, and suitability for real-world applications. This section provides a structured comparison of major cryptographic approaches to help identify the most appropriate technique for specific use cases.

5.1. Evaluation Criteria

To compare cryptographic techniques effectively, the following parameters are considered:

- Security Strength

Resistance against attacks (brute force, cryptanalysis, quantum threats)

- Key Size

Length of the cryptographic key (affects security level)

- Computational Efficiency

Speed of encryption/decryption

- Scalability

Suitability for large-scale systems

- Resource Consumption

CPU, memory, and power usage

- Application Suitability

Domain where the technique performs best

5.2. Comparative Table of Core Techniques

Table 4 Comparison of Cryptographic Algorithms

Algorithm	Type	Key Size	Speed	Security Level	Resource Usage	Best Use Case
AES	Symmetric	128–256 bits	Very Fast	Very High	Low	Bulk data encryption
DES	Symmetric	56 bits	Fast	Low	Low	Legacy systems
RSA	Asymmetric	2048–4096 bits	Slow	High	High	Key exchange
ECC	Asymmetric	256–521 bits	Medium	Very High	Low	IoT, mobile
SHA-256	Hash	—	Very Fast	High	Very Low	Data integrity

5.3. Advanced Techniques Comparison

Table 5 Comparison of Advanced Cryptographic Techniques

Technique	Security	Efficiency	Complexity	Quantum Resistance	Application
ECC	Very High	High	Medium	No	Mobile, IoT
Homomorphic Encryption	Very High	Low	Very High	Partial	Cloud computing
Zero-Knowledge Proof	High	Medium	High	Yes	Authentication
Blockchain Cryptography	High	Medium	High	Partial	Finance
Post-Quantum Cryptography	Very High	Medium	High	Yes	Future systems

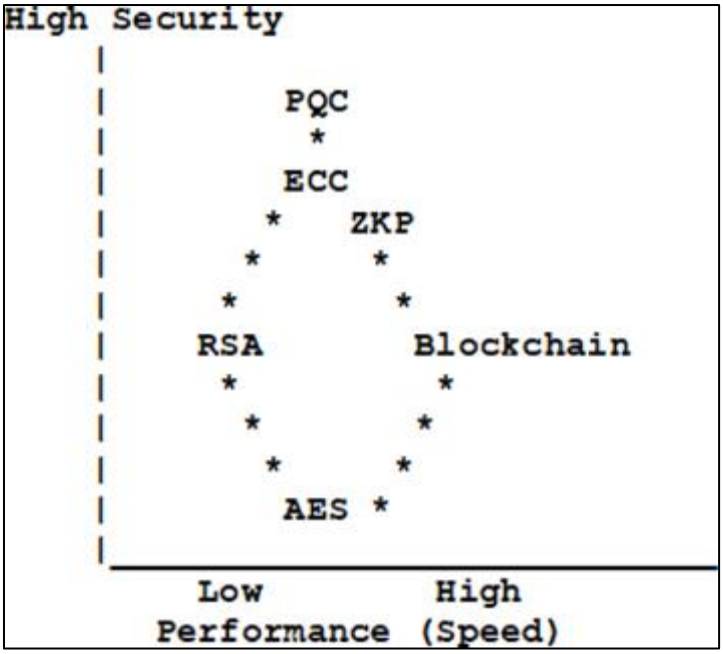

Figure 13 Graphical Comparison (Performance vs Security Trade-off)

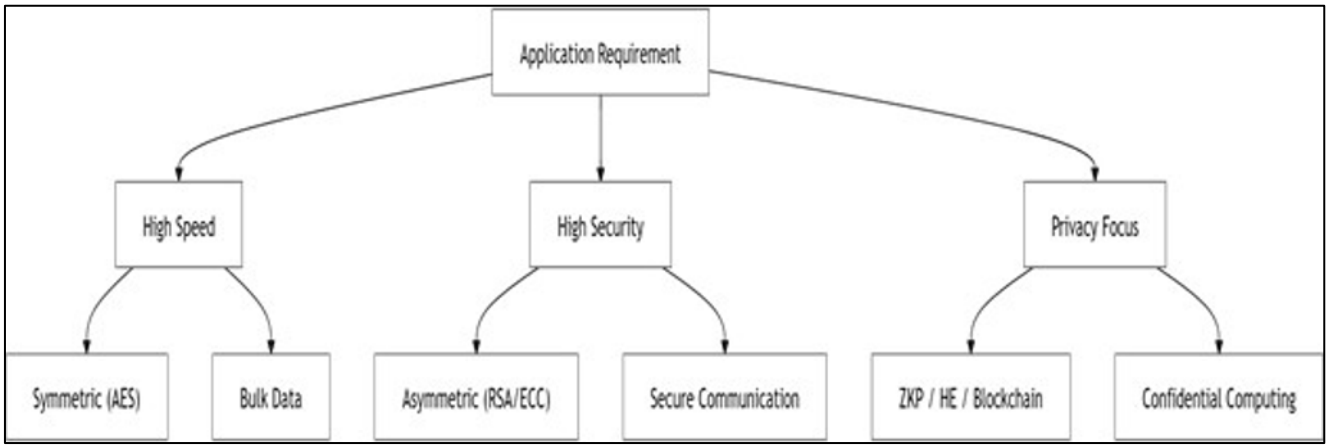

Figure 14 Cryptographic Selection Framework

5.4. Key Observations

- AES (Symmetric)

Best for high-speed encryption

Widely used in real-time systems

- RSA (Asymmetric)

Strong security but slower

Suitable for secure key exchange

- ECC

Provides strong security with smaller keys

Ideal for IoT and mobile environments

- Hash Functions

Essential for data integrity and authentication

Used in blockchain and digital signatures

- Homomorphic Encryption & ZKP

Enable advanced privacy-preserving applications

Computationally expensive but highly secure

- Post-Quantum Cryptography

Future-proof solution against quantum attacks

Still under development and standardization

5.5. Trade-off Analysis

Table 6 Best Cryptographic Choices Based on Factors

Factor	Best Choice
Speed	AES
Security	ECC / PQC
Low Power Devices	ECC
Privacy-Preserving Computing	Homomorphic Encryption
Future Security	PQC

6. Applications of Cryptography

Cryptography is widely applied across modern digital systems to ensure secure communication, protect sensitive data, and enable trust in distributed environments. Its applications span multiple domains including networking, finance, healthcare, cloud computing, and emerging technologies such as blockchain and artificial intelligence.

6.1. Overview of Cryptographic Applications

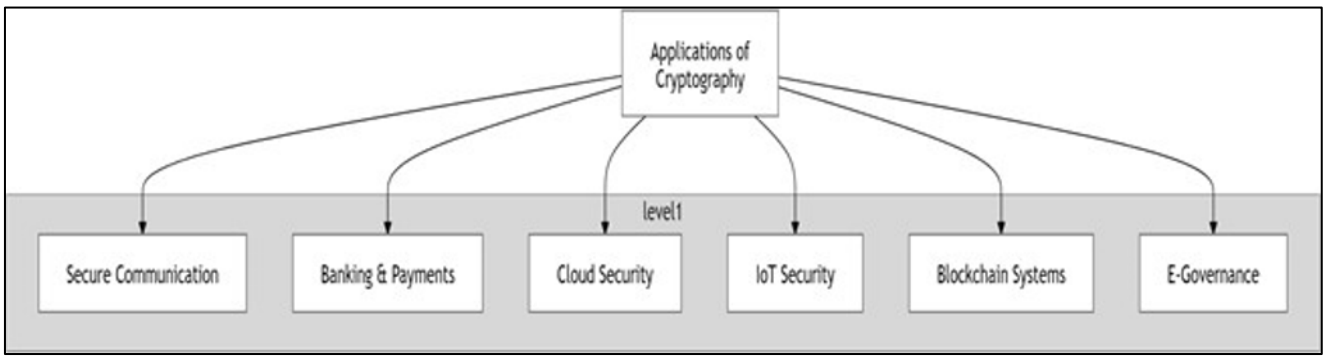

Figure 15 Overview of Cryptographic Applications

6.2. Secure Communication (SSL/TLS)

- Description

Cryptography ensures secure data transmission over networks using protocols such as **SSL/TLS**.

How it Works

Asymmetric encryption → Key exchange

Symmetric encryption → Data transmission

Hash functions → Data integrity

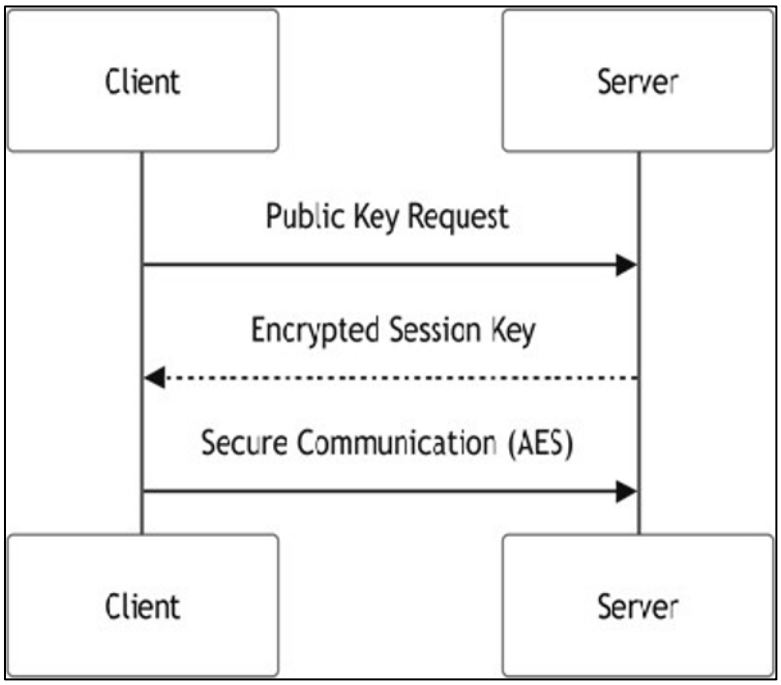

Figure 16 Secure Communication (SSL/TLS)

- Applications

Web browsing (HTTPS)

Email security

Messaging systems

6.3. Banking and Digital Payments

- Description

Cryptography secures financial transactions and protects user credentials.

- Technologies Used

AES (data encryption)

RSA/ECC (secure key exchange)

Digital signatures

- Working Flow

User → Encrypt Transaction → Bank Server → Authentication → Secure Payment Processing

- Applications

Online banking

Credit/debit card transactions

Mobile wallets

6.4. Cloud Computing Security

- Description

Cryptography protects data stored and processed in cloud environments.

- Key Techniques

Encryption of stored data (data-at-rest)

Encryption during transmission (data-in-transit)

Homomorphic encryption for secure computation

- Working Flow

User Data → Encrypt → Cloud Storage

↓

Encrypted Processing

↓

Secure Output

6.5. Internet of Things (IoT) Security

- Description

IoT devices require lightweight cryptography due to limited resources.

- Key Techniques

Lightweight encryption algorithms

ECC for low-power devices

- Working Flow

Sensor → Encrypt Data → Gateway → Cloud

- Applications

Smart homes

Healthcare devices

Industrial automation

6.6. Blockchain and Cryptocurrencies

- Description

Cryptography ensures security, transparency, and immutability in blockchain systems.

- Key Components

Hash functions → Block integrity

Digital signatures → Transaction authentication

- Structure

Block = Data + Hash + Previous Hash

Chain: Block1 → Block2 → Block3 → . . .

- Applications

Cryptocurrencies

Smart contracts

Supply chain management

6.7. E-Governance and Digital Identity

- Description

Governments use cryptography for secure digital services and identity verification.

- Applications

Digital signatures for documents

Secure voting systems

Aadhaar-based authentication (India context)

- Working Flow

Citizen → Submit Data → Encrypt → Government Server

6.8. Healthcare Data Security

- Description

Cryptography ensures confidentiality of sensitive medical data.

- Applications

Electronic Health Records (EHR)

Telemedicine

Medical device security

- Working Flow

Patient Data → Encrypt → Hospital Database

6.9. Artificial Intelligence and Privacy

- Description

Cryptography enables privacy-preserving AI systems.

- Key Techniques

Homomorphic encryption

Secure multiparty computation

- Working Flow

Encrypted Data → AI Model → Encrypted Results → Decrypt Output

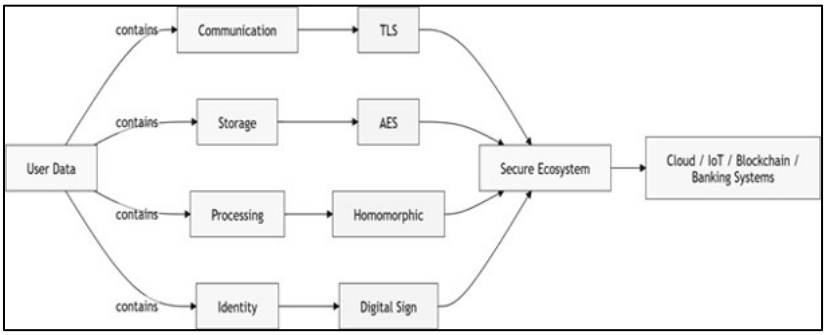

Figure 17 Integrated Cryptographic Application Framework

7. Challenges and Limitations of Cryptography

Despite its critical role in securing digital systems, cryptography faces several challenges and limitations that affect its effectiveness, scalability, and real-world implementation. These issues arise from computational constraints, evolving attack techniques, and practical deployment complexities.

7.1. Overview of Challenges

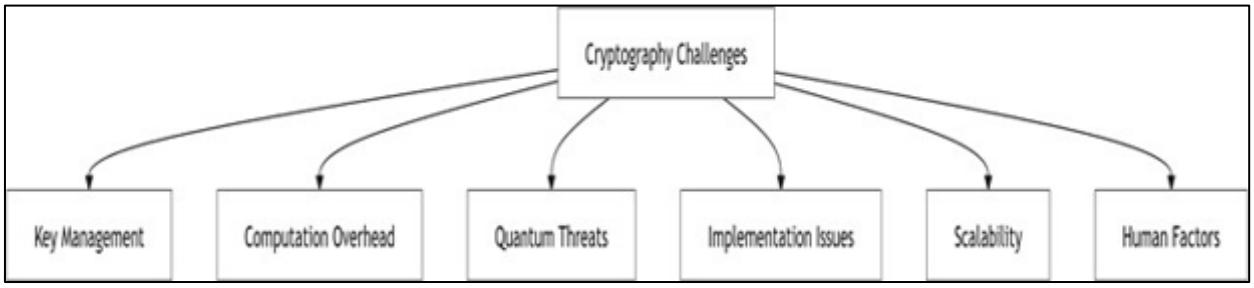

Figure 18 Challenges and Limitations of Cryptography

7.2. Key Management Issues

- Problem

Secure generation, distribution, storage, and rotation of cryptographic keys is one of the most difficult aspects of cryptography.

- Challenges

Secure key exchange in symmetric systems

Storage of private keys in asymmetric systems

- Key leakage or theft

Frequent key updates in large systems

- Impact

Even strong encryption algorithms become useless if keys are compromised.

7.3. Computational Overhead

- Problem

Advanced cryptographic algorithms require significant computational resources.

- Examples

RSA is slow for large data encryption

Homomorphic encryption is extremely resource-intensive

- Impact

Increased latency

Higher energy consumption

Not suitable for real-time or low-power systems

7.4. Quantum Computing Threats

- Problem

Emerging quantum computers can break widely used cryptographic algorithms. Key Risks

Shors algorithm can break RSA and ECC

Grovers algorithm reduces symmetric key security

- Comparison

Classical Cryptography → Vulnerable

Post-Quantum Cryptography → Resistant

- Impact

Existing infrastructure may become insecure

Urgent need for quantum-resistant algorithms

7.5. Implementation Vulnerabilities

- Problem

Even secure algorithms can fail due to poor implementation.

- Types of Attacks

Side-channel attacks (timing, power analysis)

Fault injection attacks

Software bugs and misconfigurations

- Impact

Leakage of secret keys

System compromise without breaking encryption

7.6. Scalability Issues

- Problem

Cryptographic systems struggle to scale efficiently in large networks.

- Examples

Managing keys in cloud systems

Certificate management in PKI systems

- Impact

Increased complexity

Higher operational cost

7.7. Human Factors and Usability

- Problem

Users often misuse or misunderstand cryptographic systems.

- Examples

Weak passwords

Poor key storage practices

Falling victim to phishing attacks

- Impact

Human error remains one of the weakest links in security systems.

Regulatory and Compliance Challenges

- Problem

Different countries impose varying regulations on cryptographic usage.

- Issues

Export restrictions

Legal requirements for encryption standards

Data privacy laws

- Impact

Limits global deployment

Adds compliance complexity

7.8. Interoperability Issues

- Problem

Different systems and standards may not work seamlessly together.

- Examples

Compatibility issues between cryptographic protocols

Legacy systems using outdated algorithms

- Impact

Reduced efficiency

7.9. Increased integration effort

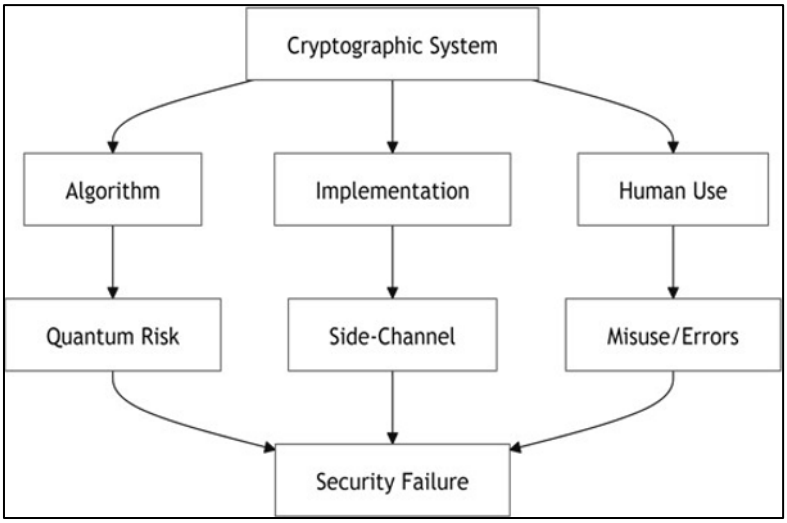

Figure 19 Cryptographic Risk Landscape

7.10. Key Insights

- **Key management** is the most critical and weakest component
- **Performance vs security trade-off** is unavoidable
- **Quantum computing** poses a major future threat
- **Implementation flaws** are more common than algorithm weaknesses
- **Human error** significantly impacts security

7.11. Mitigation Strategies (Important for Review Paper)

Table 7 Challenges and Possible Solutions in Cryptography

Challenge	Possible Solution
Key Management	Use PKI, Hardware Security Modules (HSM)
Computational Overhead	Use hybrid cryptography
Quantum Threats	Adopt Post-Quantum Cryptography
Implementation Issues	Secure coding + audits
Human Errors	User awareness & training

8. Future Research Directions in Cryptography

As digital ecosystems expand and cyber threats become more sophisticated, cryptography must continuously evolve. Future research focuses on developing secure, efficient, and scalable solutions that can withstand emerging challenges such as quantum computing, massive data processing, and privacy concerns in AI-driven systems.

8.1. Overview of Future Directions

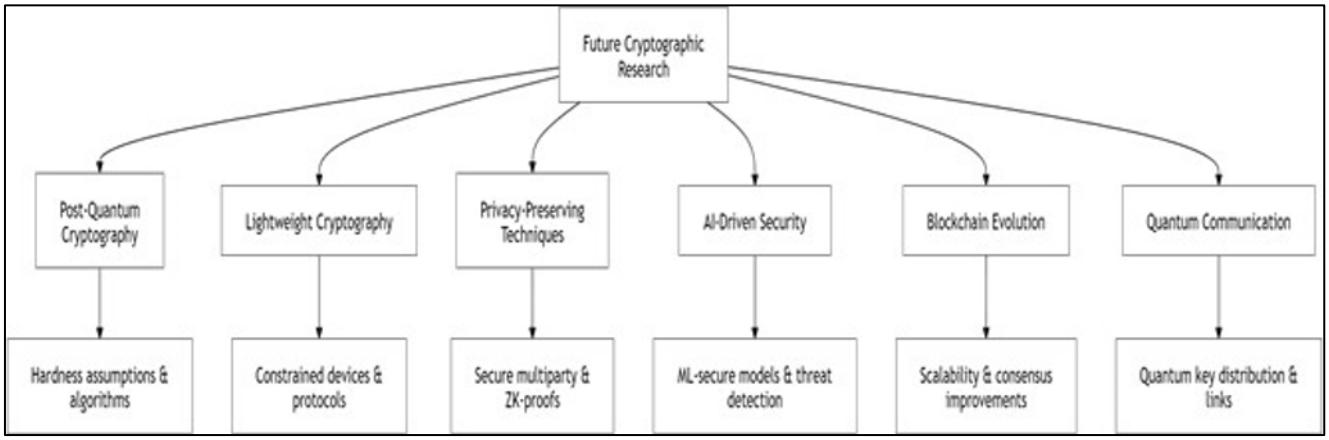

Figure 20 Future Research Directions in Cryptography

8.2. Post-Quantum Cryptography (PQC)

- Motivation

Quantum computers threaten current cryptographic algorithms such as RSA and ECC.

- Research Focus

Lattice-based cryptography

Code-based cryptography

Hash-based signatures

- Goal

Develop algorithms that are **secure against quantum attacks** and suitable for real-world deployment.

Classical Crypto → Breakable by Quantum PQC Algorithms → Quantum-Resistant

8.3. Lightweight Cryptography for IoT

- Motivation

IoT devices have limited processing power, memory, and energy.

- Research Focus

Low-power encryption algorithms

Efficient key management

Hardware-friendly designs

- Goal Ensure secure communication with minimal resource usage.

8.4. Privacy-Preserving Cryptography

- Motivation:

Growing concerns about data privacy in cloud computing and AI systems.

- Key Techniques:

Homomorphic Encryption

Secure Multiparty Computation (SMC)

Zero-Knowledge Proofs (ZKP)

- Goal:

Enable computation and data sharing **without exposing sensitive information.**

Workflow:

Encrypted Data → Compute → Encrypted Output → Decrypt Result

8.5. AI-Driven Cryptography and Cryptanalysis

- Motivation:

Artificial Intelligence can both enhance and attack cryptographic systems.

- Research Focus:

AI-based cryptanalysis

Intelligent key generation

Adaptive security systems

- Goal:

Use AI to **strengthen cryptographic resilience** and detect vulnerabilities.

8.6. Blockchain and Decentralized Security

- Motivation:

Need for trustless and decentralized systems.

- Research Focus:

Scalable consensus algorithms

Secure smart contracts

Integration with cryptographic primitives

- Goal:

Improve **security, scalability, and efficiency** of blockchain systems.

8.7. Quantum Cryptography and Quantum Key Distribution (QKD)

- Motivation:

Leverage quantum mechanics for ultra-secure communication.

- Key Concept:

Quantum Key Distribution ensures **unbreakable key exchange**

- **Goal:**

Develop **physically secure communication systems**.

- Communication Model:

Sender → Quantum Channel → Receiver (Any interception is detectable)

8.8. Cryptography for Cloud and Edge Computing

- Motivation:

Data is increasingly processed in distributed environments.

- Research Focus:

Secure data sharing

Encrypted computation

Edge device security

- **Goal:**

Ensure **end-to-end security in distributed systems**.

8.9. Standardization and Interoperability

- Motivation

Need for global cryptographic standards.

- Research Focus

Standardizing PQC algorithms

Protocol compatibility

Regulatory compliance

Goal Enable **universal and secure adoption** of cryptographic systems.

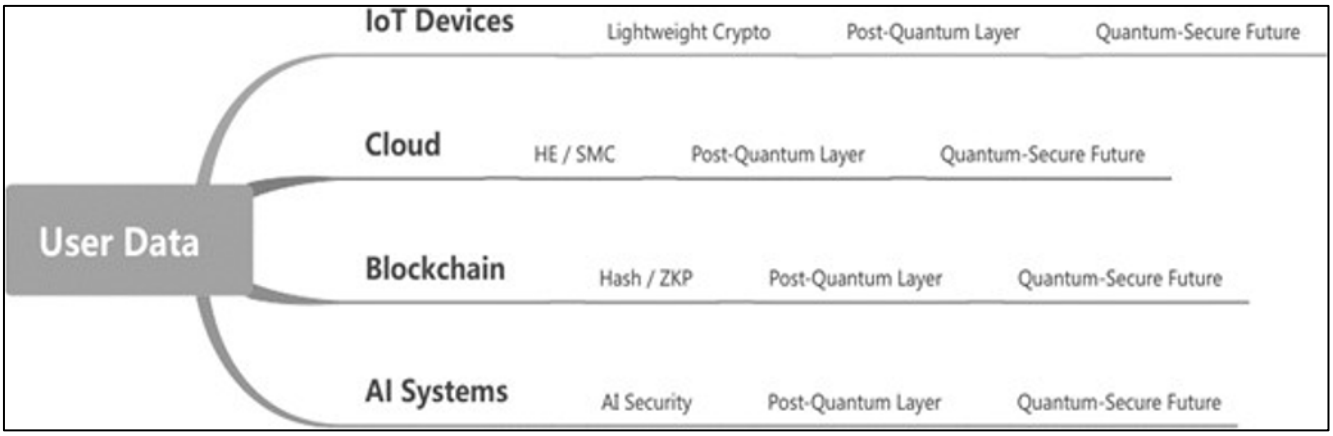

Figure 21 Future Cryptographic Ecosystem

9. Conclusion

Cryptography remains a fundamental pillar of modern cybersecurity, enabling secure communication, data protection, and trust in digital systems. This review has presented a comprehensive analysis of cryptographic techniques, beginning with foundational concepts and progressing through classical classifications such as symmetric, asymmetric, and hash-based methods. Widely adopted algorithms like AES, RSA, and ECC continue to play a vital role in securing contemporary applications, while hybrid approaches effectively combine their strengths to address real-world requirements. The study further examined advanced cryptographic techniques, including homo-morphic encryption, zero-knowledge proofs, blockchain-based cryptography, and post-quantum cryptography, highlighting their potential to address emerging challenges in privacy, scalability, and computational security. A comparative analysis demonstrated that no single cryptographic method is universally optimal; instead, each technique involves trade-offs between security, efficiency, and resource utilization. Additionally, key challenges such as key management, computational over-head, implementation vulnerabilities, and quantum threats emphasize the need for continuous innovation. Looking ahead, future research must prioritize the development of quantum-resistant algorithms, lightweight cryptographic solutions for IoT, and privacy-preserving mechanisms for AI and cloud environments. In conclusion, the evolution of cryptography will be critical in ensuring secure, scalable, and resilient systems in an increasingly interconnected and data-driven world.

Compliance with ethical standards

Acknowledgments

Authors are very grateful to the reviewer for suggesting some improvements to increase its readability.

Disclosure of conflict of interest

The authors declare that they have no known financial interests, personal relationships, institutional affiliations, or competing interests that could have appeared to influence the work reported in this review article. The authors confirm that the manuscript was prepared independently and that there are no conflicts of interest associated with its publication.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017. Covers fundamentals, AES, RSA, and security models.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. Strong base for cryptographic primitives and algorithms.

[4] C. Gentry, "A Fully Homomorphic Encryption Scheme," Stanford University, 2009. Key ref-erence for homomorphic encryption.

[5] P. Nutalapati, "Advanced Data Encryption Techniques for Secure Cloud Storage in Fintech Applications."

[6] N. Tayal, R. Bansal, S. Gupta, and S. Dhall, "Analysis of Various Cryptography Techniques: A Survey," *International Journal*, 2016. Discusses Section 2.

[7] F. Maqsood, M. Ahmed, M. M. Ali, et al., "Cryptography: A Comparative Analysis for Modern Techniques," *International Journal*, 2017. Discusses Section 2.

[8] B. Gobinathan, M. A. Mukunthan, et al., "A Novel Method to Solve Real-Time Security Issues in Software Industry Using Advanced Cryptographic Techniques," *Scientific Journal*, Wiley, 2021. Discusses Section 4 (ECC).

[9] M. Abudalou, "Enhancing Data Security Through Advanced Cryptographic Techniques," *International Journal of Computer Science and Mobile Computing*, 2024. Discusses Section 4.

[10] S. Ahmed and T. Ahmed, "Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review," *International Journal of Scientific Research*, 2022. Covers comparison of all algorithms.